



# Product Documentation

# PAM

## Administrators Guide

---



# Contents

---

<b>Contents</b>	<b>3</b>
<b>Getting Started</b>	<b>32</b>
Privileged Access Management	32
Privileged Account Management	32
Privileged Session Management	32
Privileged Job Management	32
Architecture	32
Understanding the Privileged Access Management Architecture	32
Privileged Access Management's server blocks	33
Typical deployment architecture scenarios	34
Remote or Isolated Nodes	35
The Concept and Architecture	35
Session Manager	36
Job Engine	36
Additional Nodes	37
Number of simultaneous sessions for each PAM Node	37
Privileged Access Management Deployment Architecture	37
Architecture	38
Scalability	40
Importance of your Master Password	40
Break Glass Procedure	42
Scenario #1	43
Scenario #2	43
Extract a list of records	46
Best Practices	47
Planning your Build Out	47
Using Folders for Organization and Inheritance	48
Example of a common IT scenario	48
Understanding Record Types	49
Managing Assets with PAM Records	50
Sharing and Permissions	50
Tasks, Policies, Execution and Automation	51
Workflows	51
Alerts and Notifications	51
Administrative Responsibilities	52
Conclusion	53
<b>Installation</b>	<b>54</b>
System Requirements	54
Software Requirements	54
External Database	54
Trial and POC Prerequisite	55
System Requirements	55
Minimum requirements for basic deployments and trials	55
Recommended requirements for Production deployments	55
Hardware Requirements	55
Software Requirements	56
Application Server	56
Database Server	56
Installation Guides	56
Test Accounts	57
Ports in Use	57
Open Ports required	57
Ports used	57
Saving master password during installation	58
Certificates	58
Generate a Certificate Request for your PAM Server	58

Using Self-Signed Certificates .....	61
Changing PAM from a basic login prompt authentication to a login page .....	61
Generating a Self-signed Certificate .....	62
Troubleshooting: Key Store Password Incorrect .....	65
Checking of my Self-signed Certificate .....	65
Importing a self-signed certificate for Federated Sign-In .....	66
Replacing Self-signed Certificate with Trusted Certificate .....	66
Error 500 Troubleshooting .....	67
Self-signed certificate in DER format .....	68
Self-signed certificate in JKS format .....	68
Self-signed certificate in something other than DER or JKS .....	70
SSL Certificate Web Browser Security Warning .....	70
Sync Session Manager Certificates .....	71
Windows Deployment .....	72
Linux Deployment .....	73
Create or renew the PAM Web server certificate .....	74
Federated Sign-in Module .....	76
Federated Sign-In .....	76
Deploying Federated Sign-In During Installation .....	77
Deploying PAM Federated Sign-In Post Installation .....	79
Pre-requisites .....	79
Deploying PAM Federated Sign-In Post Installation .....	79
Migration to Federated Sign-In Module v6.5 .....	80
Pre-requisites .....	80
Considerations .....	81
Migration from version 5.2x to version 6.5 .....	82
Testing .....	84
Rollback from version 6.5 to version 5.2 .....	84
Troubleshooting .....	85
Application not Authorized error message .....	85
FAQs .....	85
Federated Sign-In: Certificate Errors .....	86
Federated Sign-In Module Timeout Errors .....	86
Encrypting Properties of Federated Sign-In Module .....	87
Integrations .....	88
Active Directory .....	88
Active Directory Integration .....	88
Active Directory binding During Installation .....	89
Active Directory binding After Installation .....	90
Multiple Domain Configuration .....	91
AD or LDAP connections .....	91
Disabling .....	93
Troubleshooting .....	93
Multi Domain Forests with AD Trust Configuration .....	93
Integration for UPN Accounts .....	94
Secure Connectivity to an Active Directory Domain Controller .....	95
Troubleshooting .....	95
AD Authentication is Slow .....	96
The first method .....	96
The second method .....	97
The third method .....	97
Integration with Active Directory in HA mode .....	98
LDAP .....	101
Configuring JumpCloud LDAP Integration .....	101
Pre-requisites .....	101
JumpCloud LDAP Integration .....	101
Configuring NetIQ eDirectory Integration .....	102
Configuring NetIQ eDirectory connections .....	102
Disabling an Existing Connection .....	104

Azure and ADFS .....	104
Azure (Office 365) SSO SAML Integration .....	104
Requirements .....	104
Step 1: Create and Configure your Azure AD Enterprise Application .....	104
Step 2: Begin Configuration of PAM .....	106
Step 3: Test the Integration .....	109
ADFS Integration .....	113
Requirements .....	113
Step 1: Download your ADFS Federation Metadata File to PAM .....	113
Step 2: Import your ADFS Self-Signed Certificate to PAM .....	114
Step 3: PAM Configuration .....	115
Step 4: Generate an PAM Certificate .....	117
Step 5: Create an ADFS Relying Party Trust for PAM .....	119
Step 6: Create your ADFS Relying Party Trust Claim Rules .....	130
Step 7: Add the PAM Certificate to your RPT .....	134
Imprivata EAM .....	139
Integration with Imprivata Confirm ID for MFA .....	139
Requirements .....	139
Step 1: Begin the Imprivata Confirm ID Configuration .....	139
Step 2: Configuring PAM for Confirm ID .....	140
Step 3: Configure RADIUS MFA Requirements in PAM .....	141
Step 4: Test your Login Integration .....	143
Integration with Imprivata Enterprise Access Management (formerly OneSign) .....	144
Requirements .....	144
Step 1: Begin the Imprivata EAM Configuration .....	144
Step 2: Configuring PAM for EAM .....	146
Step 3: Complete the EAM Configuration .....	148
Step 4: Test your Login Integration .....	149
Imprivata Manage EAM Admin AD .....	151
Requirements .....	151
Step 1: Retrieve the AD account from Imprivata EAM .....	152
Step 2: Configuring PAM record to rotate AD account on EAM .....	152
AD Password Reset task .....	154
Integration with Microsoft Azure AD .....	157
Prerequisites .....	157
Steps to configure Azure .....	157
Azure MSI .....	166
Requirements .....	166
PAM Configuration .....	167
Steps for Implementation .....	168
Output .....	168
Integration with Duo Security .....	170
Adding Additional Duo Integrations .....	171
Integration with Okta SSO .....	172
Pre-requisites .....	172
Add to Okta Application .....	172
Configuring PAM for your Okta SSO .....	173
Integration with Shibboleth SSO .....	177
Requirements .....	177
Step 1: Generate Service Provider Metadata file for PAM .....	178
Step 2. Configure your Shibboleth Identity Provider for Integration .....	178
Testing the integration .....	179
Integration with PingIdentity SSO .....	180
Requirements .....	180
Step 1: Configure your PingIdentity SAML Application for Integration .....	180
Step 2: Configure PAM for PingIdentity Integration .....	184
Considerations for SSO Users .....	186
Integration with Microsoft Azure AD Authenticator Push and OTP .....	186
Functionality .....	186

Requirements .....	186
To enable Azure AD MFA for a specific user or group perform the following steps .....	187
Configuring Azure .....	187
Register a New App .....	187
Create an Access Policy .....	191
Configuring your PAM System Properties: .....	197
Azure MFA Number Matching .....	197
To test the integration .....	199
Integration with OneLogin authentication .....	199
Requirements .....	199
Step 1: Begin the OneLogin Configuration .....	200
Step 2: Perform the PAM Configuration .....	201
Step 3: Complete the OneLogin Configuration .....	202
Integration with RADIUS based Providers .....	205
Integration with ServiceNow .....	206
Configuring your ServiceNow Integration .....	207
Testing PAM and ServiceNow Integration .....	207
Integration with TOTP (MFA) Authentication .....	211
Integration with WatchGuard AuthPoint .....	212
Requirements .....	212
Step 1: Begin the AuthPoint Configuration .....	213
Step 2: Perform the Configuration .....	214
Step 3: Complete the AuthPoint Configuration .....	217
Integration with YubiKey .....	223
Step 1. Register your YubiKey to get Yubico API Keys .....	224
Step 2. Configure Integration with YubiKey .....	226
Advanced Deployments .....	227
Changing Web GUI Port Number .....	227
Windows .....	227
Linux with root account .....	228
Linux with a non-root user account .....	228
Deployment Architecture to Scale Session Manager .....	229
Component Architecture .....	229
Session Manager Deployment .....	230
Configuring .....	231
Double-Hop SSH and RDP Proxy Configuration .....	232
Configuring components .....	232
Troubleshooting Steps .....	233
Front-End Server Architecture .....	233
Front-end Architecture for Production Deployment .....	234
Front-end Architecture for Test or Trial Deployment .....	234
Additional Considerations .....	235
High Availability Configuration for PAM Deployments .....	236
High Availability Option Concepts .....	236
High Availability Option Setup .....	238
1. Database Server .....	238
2. Load Balancer .....	238
3. PAM node A .....	238
4. PAM node B .....	239
5. Setup Federated Sign-In Component in Multi-Node configuration .....	240
6. Configure MFA for a Multi-Node Deployment .....	240
7. Setup Local User Directory Replication .....	240
Saving to a Shared Network Drive .....	241
Load Balancer Configuration .....	242
Load Balancer Configuration .....	242
Pre-requisites .....	242
Apache HTTP Server with Sticky Sessions .....	242
Debian and Ubuntu Linux Load Balancer .....	244
Objective .....	244

Pre-requisites .....	244
Configuration .....	244
HTTPS Load Balancer in a Linux deployment of PAM .....	246
Red Hat and CentOS Linux Load Balancer .....	246
Objective .....	246
Pre-requisites .....	246
Configuration .....	246
NGINX Configuration .....	248
Nginx config for reverse proxy: .....	248
Nginx config for web load balancer .....	249
Nginx additional config for tcp load balancer for proxies: .....	250
Securing Traffic Between a Load Balancer and PAM .....	252
Pre-requisites .....	252
Configuring your PAM Web Container(s) to accept HTTPS Traffic .....	253
PAM Health Check Page .....	254
Multi-Replication of Directory Services Nodes (3+) .....	255
Troubleshooting .....	257
Transparent Perimeter deployment .....	257
Remote Worker Nodes for multiple Master Nodes .....	258
Transparent Perimeter .....	258
Silent Installer for Linux Platforms .....	260
Silent Installer for Windows Platforms .....	261
Deploying OpenSSH Service on Windows 10+ Hosts .....	263
Pre-requisites .....	263
Deploying OpenSSH Service .....	264
Update Local Directory to TLS 1.2 .....	267
Session Connection Failed Error 519 .....	268
Login Connection Failed Error 404 .....	268
Troubleshooting .....	268
Switch PAM from IP to Name URL Access .....	268
Session Manager Not Connecting .....	270
IIS Buffer configuration .....	270
Session Connection Errors Codes .....	271
0 (SUCCESS) .....	271
256 (UNSUPPORTED) .....	271
512 (SERVER_ERROR) .....	271
513 (SERVER_BUSY) .....	271
514 (UPSTREAM_TIMEOUT) .....	271
515 (UPSTREAM_ERROR) .....	271
516 (RESOURCE_NOT_FOUND) .....	271
517 (RESOURCE_CONFLICT) .....	271
518 (RESOURCE_CLOSED) .....	272
519 (UPSTREAM_NOT_FOUND) .....	272
520 (UPSTREAM_UNAVAILABLE) .....	272
521 (SESSION_CONFLICT) .....	272
522 (SESSION_TIMEOUT) .....	272
523 (SESSION_CLOSED) .....	272
768 (CLIENT_BAD_REQUEST) .....	272
769 (CLIENT_UNAUTHORIZED) .....	272
771 (CLIENT_FORBIDDEN) .....	272
776 (CLIENT_TIMEOUT) .....	272
781 (CLIENT_OVERRUN) .....	272
783 (CLIENT_BAD_TYPE) .....	272
797 (CLIENT_TOO_MANY) .....	273
Hardening Protocols and Ciphers .....	273
Configuring the SSH Proxy Security Algorithms .....	274
Session Relay Node Architecture and Deployment .....	274
Considerations .....	276
Configuration .....	276

New Relay Node Deployment .....	276
PAM Web Configuration .....	277
Relay Node Configuration .....	277
Testing .....	279
SSH Proxy with Relay Node .....	281
Requirements .....	281
Relay Node Configuration .....	281
Testing SSH Proxy connection with Relay node .....	282
RDP Proxy with Relay Node .....	282
Requirements .....	282
Relay Node Configuration .....	282
Testing RDP Proxy connection with Relay node .....	283
Command Line Secure Shell Interface (SSH) with Relay Node .....	284
Requirements .....	284
Testing SSH connection with relay node .....	284
Limit Relay Node option to specific containers or records .....	284
Requirements .....	284
Additional Configuration .....	284
Storing Master Password on Separate Server .....	284
Pre-requisites .....	285
Configuration .....	285
External Database Connection Strings .....	286
Apache Derby .....	286
Microsoft SQL Server .....	286
MySQL .....	286
Oracle .....	287
PostgreSQL .....	287
PostgreSQL database account management .....	287
Configure HTTP to HTTPS Redirect .....	287
To Configure HTTP (8080) to HTTPS (443/6443) Redirection .....	287
Changing the PAM Database .....	288
Enabling JMX Monitoring .....	290
JMX Support for PAM Instances .....	290
JMX Security Considerations .....	290
Checking JMX Support for PAM Framework Component (Java JRE) .....	291
Enabling and Configuring .....	291
JMX for Apache Tomcat on Linux .....	291
JMX for Apache Tomcat on Windows .....	292
How to increase the amount of memory a PAM server can use .....	293
Information .....	293
Linux .....	294
Windows .....	294
To verify the max memory has changed .....	295
Generate and Replace the SSL Certificate for PAM WEB Session Manager .....	295
Generate and Replace the SSL Certificate for PAM Local Directory Service .....	296
Integration with HSM device .....	298
Integration with Smart Cards .....	299
PAM Internal Database Tables .....	301
Linux Installation Guide .....	302
Introduction .....	302
Technical Support .....	302
Privileged Access Management .....	302
Privileged Account Management .....	303
Privileged Session Management .....	303
Privileged Job Management .....	303
Software Components .....	303
Architectural Diagram .....	304
Services .....	305
Active Directory or LDAP Integration .....	305

Planning your Installation and Deployment .....	305
Getting Started Guidelines .....	305
Installing Privileged Access Management .....	306
System Requirements .....	306
Software Requirements .....	307
External Database .....	307
Installation .....	308
License Agreement .....	308
Components .....	309
Internal Database .....	309
Directory Service .....	309
Application GUI .....	310
Job Engine .....	310
Session Manager .....	310
Federated Sign-In .....	311
Component v.6.5 or 5.2 .....	311
System Administrator .....	312
SSO Connect .....	312
External Database .....	312
Active Directory Integration .....	314
Installation Complete .....	314
Linux deployment of HA and DR nodes .....	315
PAM Centralized Deployment Manager .....	315
Supported Scope of Operations .....	315
System Requirements .....	316
Operating System Requirements .....	316
Getting Started .....	317
Logging into Privileged Access Management .....	317
Browser SSL Certificate .....	317
Initialize .....	318
License Registration .....	320
Manual Registration .....	320
Uninstalling Privileged Access Management .....	320
Uninstaller .....	320
Database Cleanup .....	321
Appendix .....	321
Remote Session Manager Configuration .....	321
Web Server .....	322
Windows Installation Guide .....	322
Introduction .....	322
Technical Support .....	322
Privileged Access Management .....	323
Privileged Account Management .....	323
Privileged Session Management .....	323
Privileged Job Management .....	323
Software Components .....	323
Architectural Diagram .....	323
Services .....	325
Active Directory or LDAP Integration .....	325
Planning your Installation and Deployment .....	325
Getting Started Guidelines .....	325
Installing Privileged Access Management .....	326
System Requirements .....	326
Software Requirements .....	326
External Database .....	326
Installation .....	328
License Agreement .....	329
Components .....	330
Internal Database .....	330

Directory Service .....	331
Application GUI .....	331
Job Engine .....	331
Session Manager .....	332
Federated Sign-In .....	332
Installation Location .....	333
System Administrator .....	334
SSO Connect .....	335
External Database .....	336
Active Directory Integration .....	338
Summary .....	339
Completing the Installation .....	341
Logging into Privileged Access Management .....	341
Browser SSL Certificate .....	342
Initialize .....	342
License Registration .....	343
Manual Registration .....	343
Uninstalling Privileged Access Management .....	344
Uninstaller .....	344
Database Cleanup .....	345
Appendix .....	345
Remote Session Manager Configuration .....	345
Offline Installation .....	347
Downgrade PAM to an earlier version .....	348
For the Federated Sign-in Module users .....	349
Connection to your own external database .....	349
Security Hardening Guide .....	349
Introduction .....	349
Technical Support .....	350
Implementation .....	350
General .....	350
Database .....	350
Application Server .....	350
Application Settings .....	351
Maintenance .....	351
Web Browser .....	351
Permissions and Authentication .....	352
<b>Users .....</b>	<b>353</b>
Privileged Access Management .....	353
Privileged Account Management .....	353
Privileged Session Management .....	353
Privileged Job Management .....	353
Software Components .....	353
Architectural Diagram .....	353
Navigating the User Interface .....	354
The Record List contains the following sections: .....	354
Left Menu Navigation .....	355
Top Menu .....	357
Search Records .....	357
Action Menu .....	358
Object List .....	359
Personal Vault .....	359
Benefits .....	361
Personal Vault Role .....	361
Personal Vault Recording .....	362
Disabling .....	362
Working with Folders .....	363
Creating Folders .....	363
Folder Options .....	364



Creating Records .....	366
Your First Record .....	366
Connecting to Sessions .....	368
Connecting to Sessions .....	368
Establishing your First Secure Session .....	368
Record's Session History .....	369
Secure Session with Recording .....	370
Setting your Preferred Session Window Size .....	373
"Global" Session Start Mode .....	374
"User" Session Start Mode .....	374
Transferring Files .....	375
In a Windows Remote Sessions .....	375
Out of Windows Remote host .....	378
In a Unix Remote Sessions .....	379
Out of the Unix remote host .....	381
File Copy Session Events .....	382
Disable Session .....	383
Overwrite Session .....	383
Troubleshooting: File transfer folder "G on Access Manager" (\\TSCIENT\G) is not available .....	384
Troubleshooting .....	384
File Transfer - Change Access Manager File Drive Letter and name .....	385
Coping Files and Clipboard Text To and From Remote Sessions .....	385
Clipboard text .....	385
Copy a file: local to remote .....	388
Copy a file: remote to local .....	391
Disable Session .....	392
Overwrite Session .....	392
Connecting to a Windows Host .....	393
Resetting Privileged Passwords .....	393
Password Formulas .....	394
Record Tasks .....	396
Record Policies .....	397
Password Resetting .....	399
Password Unlocking .....	401
Securing Objects with Permissions and Sharing .....	403
User and Groups .....	403
To create a new user in PAM: .....	403
If you also want to organize local users into local groups: .....	404
Grant Permissions .....	405
Permissions in Action .....	408
Revoke Permissions .....	410
System Administrators .....	411
Search Query Options .....	413
Records Visibility .....	413
PAM Manual Search Criteria Options .....	413
Multiple Search Criteria Options .....	417
Reviewing the Audit Log .....	418
Notifications and Alerts .....	419
Unsubscribe to Alerts .....	420
Managing my User Profile .....	421
Update your User Profile .....	421
Configure your PAM Preferences .....	421
Logging Out .....	421
Appendix .....	422
Inheritance .....	422
Wrapping Up .....	423
Technical Support .....	423
Web Browser Extension .....	423
What is the Browser Extension .....	423

Using the Browser Extension .....	424
Extension supported in Opera browser .....	426
Extension records for Viewer only .....	428
Using the Browser Extension with Viewer Permissions .....	429
My input fields are not auto-populating .....	429
Configure Web Form Input Fields .....	429
Additional functionality of the Browser Extension .....	431
Broker extension only [Deprecated] .....	431
Global parameter for Plugin for HTTP Proxy [Deprecated] .....	432
Adding a Placeholder to the Record .....	432
Submit button .....	433
Records in the Extension for Users .....	433
Records in Extension .....	435
PAM Browser Extension does not login when logging onto PAM .....	435
Troubleshooting .....	435
Recover a Lost System Administrator Account Password .....	436
Method #1 .....	436
Method #2 .....	436
Method #3 .....	437
Locked System Administrator Account .....	439
Licensing Guidelines .....	440
Application Node License .....	440
Remote Session Manager Node License .....	441
User Count License .....	442
Record Count License .....	442
Expired License .....	443
<b>Administrators and Power Users .....</b>	<b>444</b>
Getting Started .....	444
Technical Support .....	444
Other Documentation .....	444
Navigating the User Interface .....	444
Navigation menu .....	445
User Settings .....	445
Records .....	445
All Records .....	445
Shared With Me .....	445
Personal Vault .....	446
Favorites .....	446
<Favorite Folders> .....	446
Administration .....	446
Global Permissions .....	446
Global Roles .....	446
Local Users .....	446
Local Groups .....	446
Discovery .....	447
Scripts .....	447
Record Types .....	447
Tokens .....	447
Workflows .....	447
Command Control .....	447
MFA .....	447
Behavior Profiles .....	447
Settings .....	447
Updates .....	447
Reports .....	448
Searches .....	449
Management .....	449
My Sessions .....	450
My Profile .....	450

Profile .....	450
Subscriptions .....	450
Anonymous Links .....	450
Preferences .....	450
My Alerts .....	450
My Workflows .....	450
About .....	450
Application Toolbar .....	451
Login and Logout .....	451
Record List .....	451
Go to Parent .....	452
Bulk Actions .....	452
Manage .....	453
Import .....	453
Permissions .....	453
Workflows .....	453
Local Users .....	453
Local Groups .....	454
Tokens .....	454
Reports .....	454
Paste .....	454
Add Container / Add Folder .....	454
Add Record .....	454
Refresh .....	454
Subscribe to Alerts .....	454
Add / Remove from Favorites .....	454
Application Settings .....	454
Global Parameters: Access .....	454
Aggregated Email Notifications .....	454
Alert Notification Attempts .....	455
Anonymous Links .....	455
Create Audit Log for CAS Login Events .....	455
Date Format .....	455
Delegation of User Management .....	455
Group Cache TTL .....	455
Health Check Process .....	456
Managed Path .....	456
Password Expiration Warning .....	456
Proxy Server .....	456
Record Cache TTL .....	456
Restrict Scripts View .....	456
Split View Role .....	456
User Input Validation .....	456
Visible Unlock .....	457
Window Title .....	457
Other System Settings .....	457
Global Parameters: Browser Extension .....	457
Access Request Scope .....	457
Plugin Fields .....	458
Plugin for HTTP Proxy .....	458
Plugin Level .....	458
Other System Settings .....	458
Global Parameters: Discovery .....	459
Discovery Query Execution Frequency .....	459
Other Global Parameters .....	459
Global Parameters: Drivers .....	459
Azure AD MFA Domain .....	459
Azure App Id .....	459
JWT Signing Key .....	459

WS-Management Delay .....	460
WS-Management Timeout .....	460
Other Global Parameters .....	460
Global Parameters: Jobs .....	460
Password Reset LDAP Validation .....	460
Periodic Jobs Execution When Checkout .....	460
Rerun Failed Job Interval .....	461
Rerun Failed Job Window .....	461
SSH Connector Type .....	462
Other Global Parameters .....	462
Global Parameters: Preference .....	462
Access Sessions Events .....	462
Days for License Expiration Warning .....	462
Display License Expiration Warning to Administrators .....	463
Debug Mode .....	463
Display Full Administrator Menu for Auditors .....	463
Display Full Path For Objects In Reports .....	463
Email Override .....	463
Initial Query Type .....	463
Language .....	463
Search Scope .....	463
Session Clipboard Hotkeys .....	464
Session Heartbeat Interval .....	464
Session RDP Font Smoothing .....	464
Session RDP Resize Method .....	464
Session RDP Screen Size .....	464
Session RDP Server Layout .....	464
Session Start Mode .....	465
Skin .....	465
Starting View .....	465
Window Close Confirmation .....	465
Other Global Parameters .....	465
Global Parameters: Proxy .....	465
HTTP Proxy [Deprecated] .....	465
HTTP Proxy Connect Timeout .....	465
HTTP Proxy Domains .....	466
HTTP Proxy Idle Connection Timeout .....	466
HTTP Proxy Port .....	466
HTTP User Placeholder .....	466
HTTP Password Placeholder .....	466
Proxy Key Password .....	466
RDP Proxy .....	466
RDP Proxy Idle Timeout .....	467
RDP Proxy Ciphers Deny List .....	467
RDP Proxy Idle Timeout .....	467
RDP Proxy Port .....	467
RDP Proxy Protocol Level .....	467
SSH Proxy .....	467
SSH Proxy Allowed Channels .....	468
SSH Proxy Banner .....	468
SSH Proxy Ciphers .....	468
SSH Proxy Idle Timeout .....	468
SSH Proxy Keep Alive Count .....	469
SSH Proxy Keep Alive Interval .....	469
SSH Proxy Key Exchange Algorithms .....	469
SSH Proxy Macs .....	469
SSH Proxy Port .....	469
SSH Proxy Public Key Expiration (in days) .....	469
Throttle SSH Proxy Automation Connections .....	470

Universal Proxy HTTP Forwarding .....	470
Universal Proxy HTTP Forwarding Host .....	470
Universal Proxy HTTP Forwarding Use SSL .....	470
Universal Proxy Session Manager Forwarding .....	470
Universal Proxy Session Manager Forwarding Host .....	470
Universal Proxy Session Manager Forwarding Use SSL .....	470
Other Global Parameters .....	471
Global Parameters: Sessions .....	471
AS400 Screen Size .....	471
Exclusive Session .....	471
Password Detection Entropy .....	471
Personal Vault Event Recording .....	471
Personal Vault Session Recording .....	471
Resize Tolerance .....	472
Session Clipboard Transfer .....	472
Session Connect And Record Message .....	472
Session Connect Message .....	472
Session Expiration Warning Threshold .....	473
Session File Transfer .....	473
Session Idle Activity Timeout .....	473
Session Idle Timeout .....	473
Session Recording Metadata .....	473
Session Recording Rendering Bitrate .....	473
Session Recording Rendering Resolution .....	473
Session Request Enforcement .....	474
Session WebSockets .....	474
Support Relayed Sessions .....	474
URI Handler RDP .....	474
URI Handler SSH .....	474
Use Proximity Groups to Resolve Relays .....	475
Web Session Idle Timeout .....	475
Other Global Parameters .....	475
Global Parameters: Storage .....	475
Archived Objects Retention .....	475
Audit Logs Retention .....	475
Content Location .....	476
Content Storage .....	476
Encrypt Content .....	476
Export Location .....	476
Export Schedule .....	476
Export Time Window .....	476
Personal Vault .....	476
Personal Vault Role .....	476
Report Folder .....	477
Report Title Prefix .....	477
Session Recording Retention .....	477
Session Transfers Retention .....	477
System Export Retention .....	477
System Log Session Events .....	477
System Logs Retention .....	477
Temp Folder Retention .....	478
Temporary Location .....	478
Other Global Parameters .....	478
Global Parameters: Workflow .....	478
Approve by Mail .....	478
Approve by Mail Enforce JWT .....	478
Approve by Mail Filter .....	479
Approve by Mail Keywords .....	479
Default Requested Time .....	479

Minimum Requested Time .....	479
Maximum Requested Time .....	479
Minimum Reason Length .....	479
Reason Selection Helper .....	479
Holidays .....	479
Weekend .....	480
Work Hours .....	480
Other Global Parameters .....	480
Records .....	480
Records .....	480
Create a New Record .....	480
Create New Record Page .....	481
Viewing a Record .....	481
Split View .....	482
Editing a Record .....	483
Sharing a Record .....	483
Deleting a Record .....	485
Managing a Record .....	485
Archive/Restore Records .....	486
Working with Multiple Records (Bulk Actions) .....	486
Clipboard Actions (Copy, Cut, Paste, Link) .....	486
Finding Objects .....	487
Anonymous Links .....	487
Link for Records .....	488
Link with a Generic Message .....	491
Disable the Link .....	493
Design of the Link .....	493
Expired or Restricted Link .....	494
Archiving Records .....	495
Functionality of an Archived record .....	496
Archive or Restore record .....	496
Mass archive or multiple records restore .....	497
Tracking Archived Objects .....	498
Generating Strong Passwords .....	499
Object Export (Export to CSV) .....	500
Considerations for CSV Object Export .....	500
To Export a Parent Container to a CSV file: .....	501
To Export Selective Objects to a CSV file: .....	502
Importing Records from Third Party Systems .....	503
CSV file .....	504
RDC Manager save file .....	505
PuTTY export file .....	505
Import a KeePass v2 Export .....	505
Import Overwrite Behavior .....	506
Dry Run for CSV, KeePass, RDG and PuTTY files .....	506
Import from KeePass .....	509
Record Field Options and Types .....	510
Field Types .....	512
Reference Record .....	513
Using of reference record .....	513
Saving a File to a Record .....	515
Split View and Secret Co-ownership .....	518
Configure .....	518
Test .....	519
Consideration .....	520
Creating a SSH session record .....	520
Containers .....	521
Containers (Folders and Vaults) .....	521
Create a New Container .....	521

Opening or Editing a Container .....	521
Sharing a Container .....	521
Deleting a Container .....	524
Managing a Container .....	524
Container Scoped Objects .....	524
Container Scoped Local Users .....	525
Container Scoped Local Groups .....	525
Container Scoped API Tokens .....	525
Difference between Container Types .....	525
Sharing Records or Containers .....	527
Editing Permissions .....	528
Inheriting Permission .....	529
Creating Permissions .....	529
Revoking Permissions .....	531
Record Types .....	532
Record Types .....	532
Working with Record Types .....	532
Creating Record Types .....	532
Fields .....	533
Formula .....	534
Tasks .....	534
Commands .....	534
Editing Record Types .....	534
Deleting Record Types .....	534
Inheritance .....	534
Default Record Types .....	535
Creating Custom Record Types .....	554
Available Fields for Additional Functionality .....	556
AD Query .....	557
Agent Forwarding (SSH) .....	557
Allowed Hosts .....	557
Allowed Resolved Hosts .....	557
Audio .....	558
Clipboard Transfer Control .....	558
Command .....	558
Command Password .....	558
Connection .....	559
Console .....	559
Enable Level .....	559
Enable Password .....	559
Enabled .....	559
Enable WinRM SSL .....	560
Exclusive Session .....	560
File Transfer Control .....	560
File Transfer Disabled .....	560
Filter .....	560
Font Smoothing .....	561
Glyph Caching .....	561
Host Name DNS .....	561
Hosts .....	561
Key Size .....	562
Minimum Password Age .....	562
Override Session Manager .....	562
Password Attribute .....	562
Platform .....	563
Prologue .....	563
Remote App .....	563
Remote App Arguments .....	563
Remote App Directory .....	563

Resize On Connect Delay .....	564
Screen Size .....	564
Self Check Status .....	564
Service .....	564
Service Port .....	565
SFTP .....	565
SSH Channels .....	565
SSH Connector Type .....	566
Telnet Login Prompt Detection Regular Expression .....	566
Telnet Password Prompt Detection Regular Expression .....	566
Terminal .....	566
Traffic Interceptor Hints .....	567
Transport Security .....	567
Trust WinRM Server certificate .....	567
Trust WinRM Server host .....	567
VNC Password .....	567
Windows Theme (RDP in-browser sessions) .....	568
Windows Wallpaper (RDP in-browser sessions) .....	568
Record types Security policy report .....	568
Permissions Roles and Security .....	569
Permissions .....	569
Global Roles .....	569
Record Control .....	570
Session Control .....	571
Task Control .....	571
Permission, Roles and Security .....	573
Object Permissions .....	573
Record Control .....	573
Session Control .....	573
Task Control .....	574
Inheritance .....	574
Global Permissions .....	575
Global Roles .....	575
Auditor .....	575
System Administrator .....	576
Split View .....	576
Service .....	576
Blocked .....	576
Automation .....	576
Local Users and Groups .....	576
Create a Local User .....	576
Local User Password Formula .....	577
Managing Local Users .....	577
Create a Local Group .....	577
Manager Permissions .....	578
Object Permissions .....	578
Record Control .....	578
Session Control .....	579
Task Control .....	579
Inheritance .....	580
Global Permissions .....	580
Assigning Global Permissions .....	581
Global Permissions .....	581
Global Roles .....	581
Auditor .....	582
System Administrator .....	582
Split View .....	582
Service .....	583
Blocked .....	583



Automation .....	583
Local Users and Groups .....	583
Create a Local User .....	583
Local User Password Formula .....	584
Managing Local Users .....	584
Create a Local Group .....	584
Secure IDs .....	585
Enabling secure IDs .....	585
Secure ID Examples .....	586
Auditor Role .....	587
"Auditor" can .....	588
"Auditor" cannot .....	588
Folder Level Users .....	589
Preventing Users Access to PAM or its Objects (Deny Login and Block Access) .....	589
Deny Login of a User or Group .....	589
Deny Login Required Configuration .....	590
Deny Login to a Specific Users or Groups .....	591
Deny Login to Everyone with Allowed Exceptions .....	591
Customizing the Deny Login Message .....	593
Blocked Users or Groups .....	593
To Block a User or Group .....	593
Privileged-Elevation-Management .....	595
Ephemeral Accounts .....	595
Creating Ephemeral Account Records .....	596
The Ephemeral Account Process .....	597
Just-In-Time Permission Elevation .....	597
Prerequisites: .....	597
Create Just-In-Time Permission Elevation Record Type .....	597
Step 1. Create a new PAM record .....	597
Step 2. Add Just-In-Time (JIT) Record type .....	598
Step 3. Add Tasks .....	600
Step 4. Create your record .....	600
Step 5. Configure the Task .....	601
Step 6. Configure the Workflow .....	601
The Just-In-Time Permission Elevation Process .....	602
Secure Remote Sessions (Connect) .....	603
Connect .....	603
In-Session Menu .....	604
Join .....	605
Terminate .....	605
Automatically terminate .....	605
Windows Logoff Disconnection .....	605
Recording .....	606
Video Recording .....	606
Session Event Recording .....	607
RDP Client Proxy Sessions .....	607
Connecting to a Managed Windows Endpoint using an RDP Client .....	607
SSH Client Proxy Sessions .....	608
Connecting to the SSH Proxy Interface .....	609
Connecting Directly to a Managed Endpoint .....	610
Connecting with an SSH Tunnel .....	610
Windows Remote PowerShell access .....	611
Joining an Active Web Session .....	611
To Join from the Record View .....	611
To Join from the Record's Session Report .....	611
To Request to Join from the Record View .....	612
Session Joining as Request approver .....	614
Video Recording .....	616
Session Recordings .....	616

Session Recordings with Event Overlay .....	617
PAM Permissions .....	618
Session Recording Retention .....	619
Session Event Recording .....	619
Locating and reviewing a session's Session Events .....	620
Recording enforcement for Personal Vaults .....	621
Session Event Masking .....	621
Masking Conditions .....	622
Password Detection Entropy Configuration .....	622
To configure Password Detection Entropy: .....	622
Entropy Value Description .....	623
Password Detection Entropy Example .....	624
SQL Traffic Recording .....	625
RDP Client Proxy Sessions .....	626
Enabling RDP Proxy .....	627
Session record .....	627
RDP session record in a native Client .....	627
Example: Remote Desktop .....	635
Example: mRemoteNG .....	636
Example: generic RDP Mobile App .....	637
Troubleshooting .....	638
AWS Command Line Utility Proxy .....	639
Instructions .....	639
SSH-Client-Proxy-Sessions .....	640
SSH Client Proxy Sessions .....	640
Example using Command or Terminal Prompt .....	645
Example using SecureCRT .....	646
Example using WinSCP .....	647
Enabling SSH Proxy .....	647
Controlling the list of channels .....	648
PKCS#8 private key format support .....	648
Public Key Authentication for SSH Clients .....	649
To enable using your existing Public/Private Key Pair .....	649
To enable using generated Public/Private Key Pair .....	650
To disable using any Public/Private Key Pair .....	651
System Administrator Key Management Options .....	652
To Expire Keys .....	652
Blocking .....	652
Unblocking .....	652
Managing Local User SSH Keys .....	652
Additional Information .....	653
SSH Tunnels for Privileged Access .....	653
Creating SSH Tunnels for Secure Access .....	653
Allowed Hosts .....	654
Command Line Secure Shell Interface (SSH) .....	655
Overview .....	655
help, ? or help<commandName> .....	657
records or rec .....	658
connect or conn .....	659
view or v .....	660
unlock or u .....	661
request or q .....	662
request status .....	663
filter or filt .....	664
less .....	665
records .....	666
exit .....	667
Oracle-SQL-Proxy-Sessions .....	667
Oracle SQL Proxy Configuration .....	667

Enabling Oracle SQL Proxy .....	668
Creating Oracle SQL Proxy Records in Vault .....	668
Monitoring Oracle Client Connection .....	669
SSL support for SQL Proxy connections .....	669
Connecting to Oracle RDBMS through Oracle SQL Proxy .....	670
Remote-Apps .....	671
Remote Apps Getting Started Guide .....	671
Pre-requisites .....	671
Topic guide .....	672
1: Deploying and publishing .....	673
2. Configuring Remote Apps record types .....	673
3. Creating your Remote App Host record .....	674
4. Creating Remote App Launcher record .....	674
5. Verifying or Updating Remote App Script .....	674
6. Testing your Remote App connection .....	675
Imprivata Enterprise Access Management (formerly OneSign) Web Console Session using PAM RemoteApps .....	675
Pre-requisites .....	676
Deploy and Publish the PAM App Launcher .....	676
Modifying the PAM RemoteApp Script .....	677
Enabling Record Types .....	677
Creating Records to Support EAM RemoteApp Sessions .....	678
Testing your Session Connections .....	678
Troubleshooting and Tips .....	679
Remote Apps with TSPlus .....	682
Guide topics: .....	682
Deploying and publishing .....	682
Configuring Remote Apps record .....	683
3. Remote App Host record .....	683
4. Remote App Launcher record .....	684
5. Testing your connection .....	684
Windows RDS RemoteApp Launcher .....	685
Cases and scenarios .....	685
Remote App Launcher Work .....	685
Pre-requisites .....	686
1. Configure System to RemoteApps .....	686
2. Create a record .....	687
3. Testing Record .....	688
Troubleshooting .....	689
Windows RDS MMC Snap-in Launcher (MSC) .....	690
Cases and scenarios .....	690
MMC Launcher .....	690
Pre-requisites .....	691
1. System Configuration to Launch MMC Snap-ins .....	691
2. Create a record .....	692
3. Testing Record .....	694
Launching MMC snap-ins .....	695
Troubleshooting .....	695
Additional-Topics .....	696
Command Execution During SSH Login .....	696
To configure Automatic Command Execution for Browser-based or Native SSH Client Use: .....	696
Custom Remote App Launcher Record Types .....	698
Autolt Record .....	698
PAM Autolt Script Examples .....	699
Dynamic Login Credentials .....	700
Example .....	700
To create Dynamically Loaded Login Records .....	701
Pass-Through Login Credentials .....	703
Prompt for Credentials .....	705
Prompting Host or Port .....	706

Prompting for User and Password credentials .....	707
Prompting for All parameters .....	708
To prompt a user for a port using the SSH Proxy (dynamic port) .....	710
To prompt a user to select from a list of available Hosts .....	711
Setup SSH Tunnel Access .....	713
Application SSH Tunnel Configuration Examples .....	716
PuTTY .....	716
Oracle SQL Developer .....	717
SSH Sudo Execution or SU Utility Execution .....	717
Sudo Session Persistence Control .....	719
Cisco Devices .....	721
Manage your Cisco device .....	722
Password for Cisco device .....	722
Juniper Devices .....	723
Manage Juniper device .....	723
Password for Juniper network device .....	724
Palo Alto Devices .....	724
Manage Palo Alto device .....	724
Password for Palo Alto Networks device .....	724
MacOS Endpoints .....	725
Tasks .....	728
Creating Tasks .....	728
Edit or Remove Tasks .....	728
Target Record .....	729
Policy Events .....	729
Shadow Account .....	730
Time Window .....	731
Reviewing Job Results .....	731
Fallback Jobs .....	731
Configuration .....	732
To configure and execute a script associated to a record .....	732
Task Policy Events .....	736
Task Control .....	736
Shadow Account .....	738
Additional topics .....	739
Generate, Save and Share Virtual MFA TOTP Tokens .....	739
To Generate Virtual TOTP MFA Tokens in PAM .....	739
Heartbeat Checks .....	740
Job Details Error Responses .....	741
Response error: 401 .....	742
To troubleshoot a 401 response error, consider trying the following: .....	742
Response error: Cannot perform this operation at this time .....	743
Response error: The user or administrator has not consented to use the application with ID .....	743
Response error: Verification Error: Exception calling "ChangePassword" .....	743
Exception calling "SetPassword" ... "Access is denied." .....	744
Task: Password Reset LDAP, State: error, Message: StrategyDirectory: Error resetting password. PamException: Failure to update AD certificate .....	744
Task: Password Reset LDAP, State: error, Message: StrategyDirectory: Error resetting password. PamException: Cannot find user domain\user or cannot connect to AD ldaps://yourADServer:3269. ....	745
(Partial) Message: StrategyDirectory: Error resetting password. PamException: The WS-Management service cannot process the request. The maximum number of concurrent shells for this user has been exceeded. ....	745
Reconciliation Account .....	746
Rerun Failed Jobs (Fallback) .....	747
To configure these rerun options .....	748
SSH Key Management .....	748
Dual Account Control .....	750
Enable Dual Account Control .....	750
Creating Dual Account Control Records .....	750
Configuring Dual Password Rest Policies .....	751

Using the API to Retrieve Valid Credentials .....	752
Reports .....	752
Alternate Dual Account Control Configuration .....	753
Verification API .....	753
Performance Optimization .....	753
Host Queries for Mass Script Execution .....	754
Using PAM Host Query Records .....	755
Windows Local Admin Group Cleanup .....	757
Bulk Task Execution .....	760
Modifying the task .....	761
Setting Windows Passwords .....	762
Bulk Task Execution .....	764
Rotating Domain Passwords used for Services .....	765
Setup .....	766
Step by Step Configuration Example .....	767
Process Flow .....	770
Rotating Local Passwords used by Services .....	771
Autologon Domain Account Management (Windows Kiosk Mode) .....	774
Pre-requisites .....	775
Configuration .....	775
Step 1. Create a new Script .....	775
Step 2. Create a new Record Type .....	776
Step 3. Create new Fields .....	776
First Field: .....	776
Second Field: .....	776
Third field: .....	777
Step 4. Set the Password Complexity formula .....	777
Step 5. Set the Tasks configuration .....	777
Step 6. Create a record .....	778
Step 7. Associate a new Record with the Task as a Shadow Account .....	778
Testing .....	779
How it Works .....	779
Script configuration to enable the restart command .....	780
Rotating Domain Service Account Passwords in Additional Domains using LDAP Server and LDAP User Records .....	780
Hostname DNS Verification .....	784
To implement hostname verification .....	784
Automated Password Rotation for Multiple AD Servers .....	786
Assumptions .....	787
Concepts .....	787
Prerequisites .....	788
Configuration .....	788
Configuring Automation using Record Types .....	789
Password Reset Remote SSH .....	790
OpenLDAP Compliant Server Password Change .....	790
Recreating Database Links after Password Rotation .....	795
Concepts .....	795
Configuration .....	795
Operations .....	801
Generate Temporary AWS API Keys .....	801
Generate an AWS API Key Pair for Temporary Access .....	801
Additional Configuration Options .....	802
Job Execution Strategy Groovy .....	803
Groovy script specification .....	804
PAM job execution workflow .....	804
Methods of the record and shadow record objects .....	805
Script access to record and shadow record custom field values .....	806
Job Execution Strategy Interactive SSH .....	806
Interactive SSH script specification .....	806
EXPECTED-PROMPT .....	807

OUTPUT .....	807
ERROR-CONDITION .....	808
Return Result .....	808
Privileged SSH Sessions: .....	808
Imprivata Privileged Access Management .....	808
Use PAM .....	809
PAM Accomplishing .....	810
Workflows .....	811
Components .....	812
Managing Templates .....	813
Create a New Template .....	813
Edit a Template .....	813
Delete a Template .....	814
Manage Bindings .....	815
Create a New Binding .....	815
Check Instance Status .....	819
Terminate Requests Before Approval .....	820
Requestor .....	820
System Administrator .....	820
Terminate Requests After Approval .....	821
Requestor .....	821
Approver .....	821
System Administrator .....	821
Approve or Reject Requests .....	822
Interactive Approval .....	822
Email Approval .....	822
Getting Started with Workflows .....	824
Stage 1: Design an Approval Workflow .....	824
Stage 2: Request an Action that requires Approval .....	827
Stage 3: Review the Workflow Request .....	828
Stage 4: Approve the Request .....	829
Stage 5: Gain Access to the Approved Action .....	830
Designing Workflow Templates .....	831
Template Planning .....	832
Alternative Configurations .....	835
IP Based Restrictions .....	836
Associate a Client IP .....	837
IP Filter Configuration Example Scenarios .....	837
Workflow Binding Actions .....	838
Workflow Time Selectors .....	838
Workflow Binding Duration .....	839
Check Out Option .....	843
Configuring the Check Out Feature .....	844
Configuring Check Out with a Password Reset Policy .....	845
The User Experience of the Check Out Feature .....	845
MFA Requirements .....	846
Request and Approval Workflows .....	847
Cases and scenarios .....	847
Approval Workflows .....	848
Generating a Workflow Request .....	849
To request access or actions using a workflow .....	850
Approving and Rejecting Requests .....	851
To approve a request using a workflow: .....	852
Additional options available to Workflow Approvers .....	853
Using Email to Approve or Reject Requests .....	853
Enable the Approval by Email Feature .....	853
Email Responding to Access Requests .....	854
Access Request Email Response .....	855
Access Request Email Process .....	855

Troubleshooting: Emails not Coming .....	856
Granting Approved Access to Others .....	856
To Grant Access on behalf of another User .....	856
Canceling Your Request .....	858
To cancel your Access Request .....	858
Canceling Another User's Request .....	859
To cancel an Approved Access Request .....	859
Auto-Approved Workflows .....	861
To create an auto-approved workflow .....	861
Workflow Time Expiration .....	863
Modifying Workflows .....	866
Conditions .....	866
Update workflow template .....	866
Update workflow binding .....	866
Delete workflow template .....	866
Delete workflow binding .....	867
Workflow Template Types .....	867
Automatic Approval .....	867
Interactive Approval .....	867
Delegated Approval .....	868
Restrict Access .....	868
Formulas .....	868
Password Formula .....	868
XKCD generator to password formula .....	871
Formula Options .....	871
Local Users Password Formula .....	872
Random Password Generator Screen .....	872
Script Library .....	876
The Script library columns .....	877
Creating a new script .....	877
Editing an existing script .....	878
Deleting an existing script .....	878
Script for task to trigger another task .....	878
Scripts Library .....	878
Creating Custom Scripts .....	879
Editing Existing Scripts .....	879
Deleting Existing Scripts .....	879
Using Variables or Placeholders .....	879
To restart a service in a Unix or Linux host: .....	881
To create a new user in Active Directory and add them to a group: .....	882
To list the members of a Windows local group: .....	883
Discovery .....	883
Discovery Query .....	883
Creating a New Query .....	884
Managing Existing Queries .....	884
Viewing a Query Report .....	885
Deleting Queries .....	885
Scheduling Queries .....	885
Privileged Discovery Query .....	885
Discover Queries .....	886
Creating a Discovery Query .....	886
Discovery Query Reports .....	889
Discovery Query Report Actions .....	890
Discovery Query Schedule .....	890
AWS EC2 Discovery .....	891
Command Control .....	893
Command Control Policies .....	893
Create Command Control Policies .....	894
Edit or Delete Command Control Policies .....	894

Apply Command Control Policies .....	895
Apply Policies to Record Types .....	895
Apply Policies to Records .....	895
Getting Started with Command Control Policies .....	895
Whitelist Command Policy .....	896
Stage 1: Creating a Command Control Policy .....	896
Stage 2: Applying the Policy to a Record .....	897
Stage 3: Executing Commands in a Policy Controlled Session .....	898
Blacklist Command Policy .....	900
Stage 1: Creating a Command Control Policy .....	900
Stage 2: Applying the Policy to a Record .....	901
Stage 3: Executing Commands in a Policy Controlled Session .....	902
MFA Configuration .....	904
Defining MFA per User or Group .....	906
Reset a User's GAuth MFA Token .....	907
Google Authenticator .....	908
MFA Configuration Options .....	913
Integration .....	913
Configuration Options .....	913
MFA Grace Period .....	915
MFA Login as a User .....	916
YubiKey MFA Login as a User .....	925
Behavior Profiles and Event Analytics .....	927
Create Behavior Profiles .....	928
Apply Behavior Profiles to User or Records .....	930
Edit Behavior Profiles and their Rules .....	931
Delete Behavior Profiles and their Rule .....	931
Calendar style weekly access analytics report .....	931
Behavior Profiles .....	932
Create Behavior Profiles .....	932
Edit or Delete Behavior Profiles .....	934
Edit or Delete Behavior Profiles Rules .....	934
Applying Behavior Profiles .....	934
Settings and Configurations .....	935
Application Nodes .....	935
Proximity Groups .....	935
Database .....	935
Registration .....	935
Parameters .....	936
Mail Server .....	936
AD .....	936
Syslog .....	936
System Properties Reference Guide .....	936
Backend Database .....	936
LDAP Authentication .....	937
MFA .....	938
CAS .....	940
CAS Authentication .....	943
XTAM .....	945
Command Line Utility Reference Guide .....	953
Configuration Commands .....	955
Tool Commands .....	965
Break Glass Commands .....	968
Database Configuration Commands .....	969
Appendix A: Summary of commands .....	970
Administrative Messages .....	971
Create or Manage Administrative Messages .....	972
View Administrative Messages .....	972



Mail Server .....	973
Configuration to Send Emails .....	974
Configuration to Read Emails .....	974
Configure OAuth2 Setup for SMTP and IMAP in Microsoft Azure AD .....	974
Register a new application in the Azure portal .....	974
Locate Tenant ID and Client ID .....	976
Locate Application Secret Value .....	977
Configure Required Application Permissions .....	979
Complete the PAM Mail Server OAuth2 Setup .....	983
Customizing the Email Templates .....	983
Email Template Placeholders .....	984
General Placeholders .....	984
Report Placeholders .....	985
Workflow Placeholders .....	985
Proximity Groups .....	986
Disabling Proximity Groups .....	987
To Disable a Proximity Group .....	988
Example scenario with two Proximity groups .....	988
Disabling Servers .....	989
To Disable a Server within a Proximity Group .....	989
Export and Import .....	990
Automatically export of PAM Database .....	991
On-Demand export of PAM Database .....	991
System Export Retention .....	992
Import back into the same PAM deployment .....	993
Import into a new deployment with Encrypted Export .....	993
Import into a new deployment with Decrypted Export .....	994
Multi Language Support .....	995
"Global" Language .....	995
"User" Language .....	996
Registration .....	996
Online Registration .....	996
Offline Registration .....	997
Active Directory Integration .....	998
Active Directory binding During Installation .....	998
Active Directory binding After Installation .....	999
Unable to Connect to AD services .....	1000
Several ways to move forward .....	1001
Can't add any new AD users .....	1001
Here are some other reasons for error 49 .....	1001
Syslog .....	1002
Syslog server .....	1002
Message Filtering .....	1003
Audit Log Events .....	1004
Event Levels .....	1004
Event Categories .....	1004
Migration to Log4j version 2 .....	1005
Migration Guide .....	1005
Roll back to Log4j version 1 .....	1008
Adding Syslog configuration to log4j2 .....	1009
Alert and Report Subscriptions .....	1010
Alert and Report Subscriptions .....	1010
In-application and Email Alerts .....	1010
Subscribe/Unsubscribe from Alerts .....	1010
Emailed Reports .....	1011
Subscribe / Unsubscribe from Reports .....	1011
Subscribe and Unsubscribe to Alerts and Notifications .....	1011
To subscribe to an alert for a Record or Folder: .....	1012
Subscribe alert .....	1012

Subscribe report .....	1013
View and unsubscribe .....	1014
Software Updates .....	1014
Check and Update PAM Online .....	1015
Check and Update PAM Offline .....	1016
Performing PAM software update manually .....	1016
PAM and OS upgrade .....	1017
Roll Back Update .....	1017
To restore the previously backed up version of PAM: .....	1017
Recovering From Post Update Errors .....	1018
Updating the Framework .....	1018
Prerequisites .....	1018
Considerations .....	1018
Step 1. Download and Extract Framework Components .....	1019
Step 2. Stop the PAM Services .....	1019
Step 3. Updating the OpenJDK Framework .....	1019
Step 4. Start the PAM Services .....	1021
Step 5. Test and Verify .....	1021
Rollback .....	1021
Step 6. Cleanup .....	1022
Updating the Session Manager Component .....	1022
Windows Server .....	1022
Linux Server (x86 or ARM) .....	1023
Updating the WEB Container .....	1023
Prerequisites .....	1024
Considerations .....	1024
Step 1. Download and Extract WEB container Components .....	1024
Step 2. Stop the PAM Services .....	1024
Step 3. Updating the WEB Container .....	1025
Step 4. Start the PAM Services .....	1025
Step 5. Test and Verify .....	1025
Rollback .....	1025
Step 6. Cleanup .....	1025
Disable WEB GUI check for the update .....	1026
Updating the Federated Sign-in Module .....	1026
Considerations .....	1026
Step 1. Download and Extract Federated Sign-in Module .....	1026
Step 2. Stop the Pam Services .....	1027
Step 3. Updating the Federated Sign-in Module .....	1027
Step 4. Start the Pam Services .....	1027
Step 5. Test and Verify .....	1027
Rollback .....	1028
Step 6. Cleanup .....	1028
Reports .....	1028
Reports .....	1028
Working with reports .....	1029
Access Report .....	1030
Access report options .....	1030
Provided Information .....	1030
Audit Log Report .....	1031
Options .....	1031
Provided Information .....	1031
Saved Filters .....	1032
Bindings Report .....	1032
Options .....	1033
Provided Information .....	1033
Inventory Report .....	1034
Options .....	1034
Provided Information .....	1034

Matrix Export .....	1035
Saved Filters .....	1035
Change History Report .....	1036
Custom Queries .....	1037
Creating a New Custom Query .....	1039
Record View screen .....	1040
Example of custom query with Id filter .....	1041
Job History Report .....	1042
Options .....	1042
Provided Information .....	1042
Saved Filters .....	1042
Job Summary Report .....	1043
Options .....	1043
Information Provided .....	1043
Local Group Membership Report .....	1044
Options .....	1044
Provided Information .....	1044
Requests Report .....	1045
Options .....	1045
Provided Information .....	1045
Saved Filters .....	1046
Sessions Report .....	1046
Options .....	1047
Provided Information .....	1047
Saved Filters .....	1048
Session Events Report .....	1048
Options .....	1048
Provided Information .....	1049
Saved Filters .....	1049
Statistics Report .....	1050
Available graphs .....	1050
Subscriptions (Reports) .....	1051
Options .....	1051
Provided Information .....	1051
Subscriptions (Alerts) .....	1052
Options .....	1052
Information .....	1052
Tasks Report .....	1053
Options .....	1053
Provided Information .....	1053
Users Report .....	1054
Options .....	1054
Provided Information .....	1054
Saved Filters .....	1055
Workflow Report .....	1056
Options .....	1056
Provided Information .....	1056
Report Center .....	1057
Options .....	1058
Provided Information .....	1058
<b>Developers .....</b>	<b>1059</b>
Working with the API .....	1059
Authentication Tokens .....	1059
Managing Tokens .....	1059
Token Authentication .....	1060
Generate API Authentication Tokens .....	1061
Perform the actions .....	1063
Provided Information .....	1063
API Parameters Details .....	1064

Connect Permissions .....	1064
API Examples .....	1064
PowerShell .....	1064
Create a Record .....	1065
Create a Folder .....	1065
Retrieve Root Folder .....	1066
List Folder Content .....	1066
Retrieve a Record .....	1066
Retrieve a Record with Password Unlock .....	1067
Retrieve a Record Field Unlock .....	1067
Update a Record .....	1067
Download a File .....	1068
Share a Record or Folder .....	1069
Delete a Record .....	1069
Look up for Objects .....	1069
List Record Types .....	1070
Database Export Decrypted .....	1070
Database Export Encrypted .....	1070
Database Import .....	1071
API Token .....	1071
Secure Authentication .....	1072
REST API Shell Scripts .....	1077
Create a Record .....	1078
Create a Folder .....	1078
Retrieve Root Folder .....	1079
List Folder Content .....	1079
Retrieve a Record .....	1079
Retrieve a Record with Password Unlock .....	1080
Retrieve a Record Field Unlock .....	1080
Update a Record .....	1080
Update One Record Field .....	1081
Download a File .....	1081
Share a Record or Folder .....	1081
Delete a Record .....	1082
Look up for Objects .....	1082
List Record Types .....	1082
Database Export Decrypted .....	1083
Database Export Encrypted .....	1083
Database Import .....	1083
API Token .....	1083
Secure Authentication .....	1084
Python .....	1090
VBScript .....	1095
Ansible Integration .....	1102
Connection Brokering Integration .....	1103
Data Lookup Integration .....	1104
Best Practices .....	1105
Using the API with Cross-Site Scripting Protection .....	1105
Using the API with Federated Sign-in Module .....	1106
Using the API with MFA Enabled .....	1106
Customization of Federated Sign-In Page text .....	1107
Page Title .....	1107
Bottom Security message .....	1108
Export your Data from PAM .....	1109
Automatically .....	1109
On-Demand .....	1109
System Export Retention .....	1110
Import Data into PAM from Exported File .....	1110
Import back into the same PAM deployment .....	1111

Import into a new deployment with Encrypted Export .....	1111
Import into a new deployment with Decrypted Export .....	1112
Java 8 to OpenJDK 11 Migration .....	1113
Prerequisites .....	1113
Considerations .....	1114
Step 1. Download Migration Components .....	1114
Step 2. Stop the PAM Services .....	1114
Step 3. JRE to OpenJDK Migration .....	1115
Step 4. Start the PAM Services .....	1117
Step 5. Test and Verify .....	1117
Rollback .....	1117
Step 6. Cleanup .....	1118
FAQs .....	1118
Updating Original PAM Deployment to Latest Framework and WEB Container .....	1118
Prerequisites .....	1119
Considerations .....	1119
Step 1. Download Migration Components .....	1119
Step 2. Stop the PAM Services .....	1119
Step 3. Updating Framework and WEB Container Version .....	1120
Step 4. Start the PAM Services .....	1122
Step 5. Test and Verify .....	1122
Rollback .....	1122
Step 6. Cleanup .....	1122
PAM Software Binary Distribution and Signatures .....	1123
PAM Binary Components with MD5, SHA512 and PGP signatures .....	1123
PAM Component Integrity .....	1123
Windows Integrity Check .....	1123
Linux Integrity Check .....	1124
PDF Downloads .....	1125
Company Information .....	1125
Technical Support .....	1125
Imprivata Contact Support .....	1126
Support: Americas .....	1126
Support: EMEA .....	1126
Support: APAC .....	1126
Imprivata Headquarters .....	1126
Imprivata Worldwide headquarters .....	1126
Imprivata European headquarters .....	1126
Imprivata Germany .....	1127
Imprivata BENELUX .....	1127
Imprivata Australia .....	1127

# Getting Started

---

## Privileged Access Management

Privileged Access Management (PAM) is an agentless solution that provides a secured database to manage privileged accounts and secrets, establishes secure sessions for users through a standard web browser and automates the execution of jobs or tasks without disclosing or sharing access, passwords or secrets.

PAM contains the following core components:

### Privileged Account Management

A secure AES 256-bit encrypted database that contains records which can be stored, shared and used without disclosing the actual privileged account or its secrets (passwords, certificates or keys).

### Privileged Session Management

The ability to establish a privileged session to an underlying system (Windows, Unix, Linux, Mac, or Network Device) through a standard web browser or native clients (such as PuTTY, Secure CRT, mstcs, and many others) while providing the means to monitor, join, record or terminate this session.

### Privileged Job Management

Schedule, automate or execute on demand jobs to privileged systems without embedding the secrets in scripts or sharing them with untrusted users.

## Architecture

### Understanding the Privileged Access Management Architecture

Privileged Access Management server is installed on a single or multiple physical or virtual computers.

We call each computer a node.

Single node setup is very easy and quick.

However, administrators might decide to use multiple nodes for the server installation to increase performance, to improve availability (in case when one of the nodes malfunctions) or to improve security (to separate master password and encrypted data).

Privileged Access Management server is constructed from several types of blocks.

Administrators can install all these blocks on one single node (remember, a node is just a physical computer or a virtual machine).

This is what we recommend for trial or a light system use to simplify the installation process. We call such virtual or physical computer – a node.

Note that each node might contain multiple blocks or different type.

Moreover, an administrator can install more blocks of the same type on different nodes to increase system performance, to improve PAM availability or to improve internal PAM security.

The diagram illustrates a Zero Trust Architecture (ZTA) implementation. At the center is the **Access Manager (PAM)**, which is **SSL Secured**. It acts as the central hub for authentication and session management. External components include **Desktop and Mobile Web Browsers**, **AD, MFA, TOTP, SAML Authentication**, **RDP, SSH and HTTPS Proxies**, and **Secure Access Tokens**. The Access Manager interacts with an **Identity Vault** and a **Session Manager**. The Identity Vault is connected to **Automated Password Rotation** and **Cloud Infrastructure**. The Session Manager is connected to **RDP, SSH, HTTPS, VNC, Telnet** protocols. The diagram is enclosed in a blue border with a brick wall pattern, representing a secure perimeter.

- **Application GUI or WEB Front End** is the block that interacts with users using WEB GUI or with scripts using API. The server may contain multiple Application GUI blocks installed on different nodes to make the system serve users faster. Each Application GUI block might serve many users or script requests.
  - However, as more users access the system more Application GUI blocks might be installed. When the server uses multiple Application GUI nodes, the administrators should install a **Load Balancer** block (on one of the nodes or on a separate node) to balance the use of WEB Front Ends.
- **Job Engine** is the block that executes background processes like password reset or discovery. The server might contain multiple Job Engine blocks installed on different nodes. Each Job Engine block can handle many password resets or discovery queries.
  - However, adding more Job Engine nodes increases the speed of these tasks because more of them will be executed at the same time. The system includes flexible configuration of Job Engines on each node.

This allows for some processes to be disabled on some nodes and adding more threads (parallel tasks) for certain nodes.

- **Session Manager** is the Jump Server gateway. This block displays remote computer screens in the users browsers. The server might contain multiple Session Managers. Each session manager can handle multiple simultaneous sessions.
  - However, when the server has to support too many sessions, an administrator can add more Session Manager nodes. Moreover, Session Manager node might be installed at a strategic location that can access certain computers on the network. The server includes flexible configuration that allows selection of session manager depending of the location of the destination computer.
- **Directory Service** is a block that contains local system users and also a master password. The server might contain only one Directory Service.
  - However, an administrator may decide to host this block on a separate node to separate physical master password location from the encrypted data in the database.
- **RDBMS** is a block that stores all internal system data (with the exception of local users and master password stored in the Directory Service). The server may contain only one RDBMS node. The server is shipped with the internal database that should be installed on one of the nodes with either Application GUI or Job Engine.
  - However, an administrator might decide to use one of several external supported RDBMS. We do not count RDBMS node in our licensing model.
- **Federated Sign-In** is a block that performs user authentication. The server might include only one [Federated Sign-In](#) block.

## Typical deployment architecture scenarios

To illustrate the use of the nodes we will describe several typical deployment architecture scenarios:

- **Trial.** All blocks could be installed on a single node using default installation options.
- **Light Use.** All PAM components could be installed on a single node like during the Trial but exposed to the outside world using Load Balancer with secured SSL HTTPS connection through the standard https port 443. Clients will need to install their own certificate for the known host name. The Federated Sign-In service might or might not be installed in this case depending on whether basic authentication through the secure channel could be enough for the system operations. This is our primary recommendation for the initial or light use in a typical SMB organization.
- **Enterprise Database.** While the internal RDBMS shipped with the system is a reliable database, it is possible to connect all components (Application GUI and Job Engines) to external database scheme supplied by the user. PAM will create and populate the data tables automatically during the first run or data import. The database could be a Derby database installed as a part of different computer node or it could be any other certified RDBMS supplied by the user.



- **High Availability** scenario is achieved when Application GUI, Job Engine and Session Manager components deployed to two different nodes connected to the single RDBMS accessed through the single [Load Balancer](#) and using a single Directory Service possibly offloaded to a third node. This three-node setup is a minimal configuration for highly available, moderate performance deployment with the inclusion of the improved security option.
- **Many Users** scenario addresses the situation of many users accessing PAM Application GUI simultaneously mostly for the data managed by the system without accessing many remote computers. In this case Application GUI could be deployed to several nodes accessed through the load balancer connected to the same RDBMS and Directory Service to improve PAM reaction time.
- **Many Sessions** scenario addresses the case of many simultaneous sessions to remote computers established by system users at the same time. The sessions might include multiple users attached to the same computer (session sharing) or users accessing different computers. In this situation Session Manager could be installed on multiple different nodes to reduce the load to each individual Session Manager. Application GUI will load balance Session Manager selected to access specific computer group based on the number of sessions currently opened on an Session Manager. In addition to that some Session Manager components could be installed at the strategic network locations to provide (better) access to certain network resources. IT creates Session Manager proximity groups that define groups of Session Manager services that access certain computers selected by IP addresses or by name pattern.
- **Many Jobs** scenario covers the case when there are many parallel password resets, script executions, notifications, or discovery jobs running in the background. In this case the Job Engine component could be installed on multiple computers connected through the single RDBMS to reduce the load on any particular node. The Job Engine component could be configured to increase or decrease the thread load for every particular process or to disable certain processes on some nodes completely. For example, some computers might only handle password reset jobs while other computers might only handle notifications. In addition to that some Job Engine components could be installed at the strategic network locations to provide (better) access to certain network resources.
- **Combination** scenario allows use of any previous deployment configuration. The complete PAM application farm might contain multiple nodes distributed across multiple network locations accessed through a single HTTPS entry point.

## Remote or Isolated Nodes

### *The Concept and Architecture*

You install an PAM node in an isolated network to provide access to assets in this network and to execute jobs such as password resets on the assets in the isolated network.

One node in the isolated network will serve all assets it can access within this network. In this scenario, users gain access to all assets from this isolated network through the main PAM node, while the isolated node works transparently behind the scenes to serve these assets.

This is not a high availability setup because both nodes have access to different assets (one in the main network and the other one in the isolated network) so you need both of them to operate.

When the main node is down, no access is possible to anything.

The following is a description of the architecture to design an isolated Session Manager (for sessions) and isolated Job Engine (for task execution like password resets) deployment.

This is a conceptual description to illustrate the architecture to help with design decisions.

For details and configuration options, please read the appropriate guide linked below.

- [Isolated Session Manager Nodes](#)
- [Isolated Job Engine Nodes](#)

The isolated node should be installed using its internal database and then configured to serve as an isolated node.

It does not need to connect to the same database the main PAM node is connected as this deployment scenario assumes that the back end database of the main PAM node is not accessible by the isolated node from inside of its network.

## *Session Manager*

To provide remote access to assets in the isolated network, the main node needs to connect to the Session Manager in the isolated network using the proprietary PAM protocol, which it does using port 4822.

This port should be opened in the isolated network firewall to the PAM isolated node for the main node to connect.

The Session Manager traffic between the main node and the isolated node is secured by the certificates exchanged between the nodes.

To configure this you will need to bring this certificate from the main PAM node to this isolated node during configuration.

Lastly, the main node should have a configuration in the Administration > Settings > **Proximity Groups** screen instructing the main node to route traffic for certain assets to the isolated node. There are several criteria you can choose from:

1. route all traffic to certain IP addresses to the isolated node and all other assets will be served by the main node
2. route all traffic to certain computer names (by DNS name masks) to the isolated node and all other assets will be served by the main node
3. route all traffic for all assets located in certain PAM Vault (folder) to the isolated node and all other assets will be served by the main node

Use Case #2, Network Isolation, in the article provides additional details [here](#).

## *Job Engine*

To make the isolated node for task executions like password reset jobs on the assets inside the isolated network, you need to create a Service user in the main node using the Administration > Local Users screen.

After that, you need to designate this user account as a Service using Administration > Global Roles screen. Lastly, you need to grant this user permissions (Owner with Execute rights) for the assets the isolated node should serve.

This permission could be granted for the Vault, Folder or for individual Records.

The isolated node, when configured, will execute jobs only for the assets with this user in permission sets.

The main PAM node will not execute jobs for the assets designated for the isolated node.

After the service user is created, connect the isolated node to the main node by using the **XTConnect** command, providing the https URL of the main node and credentials of the service user created earlier.

After this command, the isolated node will communicate with the main node using HTTPS traffic from inside of the isolated network.

The main node should be available for the isolated node to connect using the regular URL (port 443 should be opened in the main node firewall, you can check this by browsing main node from the isolated node).

When properly configured, the isolated node will poll the main node for the jobs to execute for the assets designated for the isolated node by means of the permissions granted for the service account, execute those jobs for the local assets and send results back to the main PAM node.

Use Case #2, Remote Job Engines operating in isolated networks, in the article provides additional details [here](#).

## *Additional Nodes*

More isolated network nodes could be added in a similar fashion by using additional proximity groups for session managers and additional service accounts to designate assets for task execution by these remote nodes.

One of the design decisions in content organization is how to group assets for the isolated nodes to simplify management.

The simplest solution is to put all assets related to the isolated network into a corresponding PAM Vault to set up Session Manager proximity group to this vault and to grant permissions to the service account on the vault level.

There are other solutions for this designation too.

## Number of simultaneous sessions for each PAM Node

Depending on CPU and RAM, the typical recommendation for simultaneous sessions is between 100-200 sessions per node. If need be, an additional node(s) can be added to maintain a healthy Node active session count balance.

To check the number of active sessions per hour, the [Dashboard](#) graph **Number of active sessions in selected hour** can be used. This will show statistics for how many Active sessions there are for each 1 hour block of the last 7 days. Hovering over each block will show the actual number.

## Privileged Access Management Deployment Architecture

The article discusses a typical mid-size deployment architecture of a Privileged Access Management system.

# Architecture

The diagram below illustrates typical High-Availability (HA) setup of an PAM Privileged Access Management system with Disaster Recovery (DR) option.

2 nodes deployed in the “Primary Site” in a High Availability configuration with the third node as a single deployment in the “DR site”.

Data replication (outside of PAM) would be enabled for both the database as well as the file share where objects like [Video Recordings](#) are stored.

This replication could be extended to the DR site if possible.

Alternatively, use PAM [export/import](#) commands to provide data to the DR node.



# Scalability

The diagram also includes a depiction of additional nodes in the Primary Site (“Additional Scaling Options”). Additional PAM nodes can quickly be setup and included in the Primary deployment even during production use of the system.

Configure these additional nodes (PAM Nodes 3+) like the first two acting to expand the HA options.

Alternatively, they could act as independent Session Manager or Job Engine nodes.

If and/or how these nodes would be deployed depends entirely on the circumstances that may arise when PAM is deployed.

Additional nodes could be used to address concerns like performance issues, increasing number of PAM users, isolated networks and others.

Read about details of High Availability configuration in the following [article](#).

## Importance of your Master Password

Why is my Master Password so important?

During PAM installation, it is stressed that the master password generated and displayed be saved to a file and stored in a safe location. Here we will explain the importance of your Master Password.

```
Administrator Account: pamadmin / leveled-revoke-powders?  
Directory Password: R7HmHmyreTdQX8  
Master Password: TAIQBo2ZY9eRuvIPcmxOM0uK0DDMfRZJ  
Database Password: EAn7HP959Xrrs4
```

```
System Admin: pamadmin/Mq7bL6  
Master Password: Ok: uiCvb6UBAQGa83AYvPHtEBc2YAYmKcAu  
DB Password: Ok: 0L4yEBTDpIr3Y3  
Directory Admin Password: Ok: SU8QwtPn4qDpKl
```

Master Passwords are generated and displayed during installation.

Above, you will see a Windows installation on the left and Unix on the right.

Privileged Access Management encrypts sensitive data stored in its backend database using an AES-256 algorithm.

This algorithm is based on the master password that system uses to lock and unlock encrypted data.

Without the master password nothing can decrypt sensitive data in your system database which is a good thing because there is no backdoor to circumnavigate this algorithm.

However, in the unfortunate event when the master password is lost it would be helpful to have it available for restoration to make sure that encrypted data could be decrypted by the trusted password holder.

This is why it is important to **save your master password in a safe place during system installation**.

PAM secures your master password in its *Directory Service* component.

The Directory Service component could be hosted on a separate computer to increase overall system security by keeping encrypted data and the master password on different physical machines.

PAM generates a master password for each farm during installation of the Directory Service component of this farm.

It is vitally important to save the master password to a safe place after installing Directory Service.

Please note that encrypted export file does not include a master password for the security purposes.

The **only** way to access a lost master password is to save it during installation.

Unfortunately, if the password is lost then your data cannot be decrypted by anyone, so please do save it to a file and store it in a safe location.

It only takes a minute to do and can potentially save a lot of pain and heartache in the future.

When configuring PAM in a High Availability (HA) deployment then all system nodes must have the same Master Password.

Additional information about HA deployments can be found [here](#).

If a node in this kind of configuration is using a different master password, then it will be unable to read secrets that were created in one of the other nodes and vice versa.

The usual indication of this type of misconfiguration between nodes is when you click the **Unlock** button, the secured value fails to load and you receive a decryption error in the log.

To resolve this issue with mismatched Master Passwords, you will need to set the Master Password of the new node to that of the current node.

That will ensure that all future records created in either node will be read by both. If you have existing records that were encrypted with the previous Master Password, then those will need to be re-encrypted with the new password.

To do this, navigate to Administration > Settings > Database and *click* the **Change Master Password** button. In the dialog, supply the *Current Master Password* and the *New Master Password* to start the process.

This option will re-encrypt all records in the system encrypted with the provided old master password using the new provided master password. This option is useful when repairing the records created by the incorrect master password.

Note that the same master password should be used to view these records after re-encryption.

When it begins, the system will traverse the entire Identity Vault and for every record, it will attempt to decrypt each using your Current Master Password.

For those that decrypt, it will then re-encrypt them with your new Master Password.

For records that fail to decrypt with the current, they will not be re-encrypted.

When the re-encryption process begins and completes, an Audit Event will be generated for each.

```
1 | Category: Operation
2 | Level: INFO
3 | Event: Re-Encrypt Records
4 | Message: Records re-encrypting started
```

```
1 | Category: Operation
2 | Level: INFO
3 | Event: Re-Encrypt Records
4 | Message: Records re-encrypting completed
```

When a record is re-encrypted, an Audit Event will be generated for each that was updated.

```
1 | Object: {Name of Record}
2 | Category: Data
3 | Level: INFO
4 | Event: Update
5 | Message: Re-encrypt
```

If a record is not re-encrypted, then no Audit Event for that object will be generated.

## Break Glass Procedure

A break glass procedure refers to a quick method for a user to gain access when needed (usually during an emergency) to a managed system who would ordinarily not have access.

The term “**break glass**” is a reference to someone breaking the glass door or stopper to pull a fire alarm in the event of an emergency.





Although the concept is the same, some people refer to a break glass procedure for a couple of different scenarios.

In this article, we will discuss these scenarios and how PAM provides support in the case of an emergency.

## Scenario #1

User needs immediate access to a Privileged System.

In this scenario, the PAM is online and accessible however there is an emergency with a privileged system that is managed within the PAM.

John, our IT worker, needs immediate access to the Domain Controller because it is offline.

In this example, John would log into the PAM and as usually request access to the Domain Controller.

The Approval Workflow bound to John and this record would be configured with an Emergency approval cycle or be auto-approved.

This type of configuration would allow John to access this privileged system during this specific time frame without having to complete the typical multi-stage approval process.

As a result, John is granted access to perform his emergency task while still maintaining the integrity of the PAM workflow process.

To learn more about Approval Workflows, including Emergency and Auto-approval, please read [System Request and Approval Workflows](#).

## Scenario #2

User needs immediate access to a Privileged System however PAM is inaccessible.

In this scenario, the System is offline and there is **an emergency with a privileged system** that is managed within PAM.

Again, John, our IT worker, needs immediate access to the Domain Controller but the login credentials are stored in the PAM.

In this example, John (assuming he is not a System Administrator) would need to contact a System Administrator in order to extract the credentials from a previously created [the System export](#).

Once the credentials have been extracted, John can use them to access the system using a native client like RDP or PuTTY.

For this Break Glass procedure which involves extracting data, including secrets, from an exported the PAM database, PAM Administrator would perform these steps:

1. Login to the server that is hosting the PAM as an Administrator.
2. Open a command line session.
3. Navigate to \$PAM\_HOME. This is the installation folder for the PAM.
4. Execute the following command to extract secured information from a record. The following variables will need to be replaced as necessary.
  - **{EXPORT}**: The full path to the exported database .ZIP file or the beginning of the .ZIP file for multi-part exports.
  - **{RECORD\_NAME}**: The full record name.
  - **{RECORD\_ID}**: The record ID.
  - **{QUERY}**: The query search for records. This query will return a list of all records (record name, ID, host and description only).
  - **{MASTER\_PASSWORD}**: The PAM Master Password. If a – (dash) is used instead of the master password, then the command will prompt the user for the master password during execution.
    - a. For Windows, substitute your {EXPORT}, {RECORD\_NAME} or {RECORD\_ID} and {MASTER\_PASSWORD} values and issue this command.

```
1 | bin\PamDirectory.cmd Extract {EXPORT} {RECORD_NAME} {MASTER_PASSWORD}
```

```
1 | bin\PamDirectory.cmd Extract {EXPORT} {RECORD_ID} {MASTER_PASSWORD}
```

```
1 | bin\PamDirectory.cmd Extract {EXPORT} {QUERY} {MASTER_PASSWORD}
```

Examples:

```
1 | bin\PamDirectory.cmd Extract c:\xtam\export\xtamexp-20180103113616-119836-0001.zip "Domain Controller" 48BRU7ikr9oIt2YKwzOYBQSoqwI22wAy
```

```
1 | bin\PamDirectory.cmd Extract c:\xtam\export\xtamexp-20180103113616-119836-0001.zip 168473 48BRU7ikr9oIt2YKwzOYBQSoqwI22wAy
```

```
1 | bin\PamDirectory.cmd Extract c:\xtam\export\xtamexp-20180103113616 168473 -
```

```
1 | bin\PamDirectory.cmd Extract c:\xtam\export\xtamexp-20180103113616-119836 "Domain" -
```

- b. For Unix, substitute your {EXPORT}, {RECORD\_NAME} or {RECORD\_ID} and {MASTER\_PASSWORD} values and issue:

```
1 | bin/PamDirectory.sh Extract {EXPORT} {RECORD_NAME} {MASTER_PASSWORD}
```

```
1 | bin/PamDirectory.sh Extract {EXPORT} {RECORD_ID} {MASTER_PASSWORD}
```

```
1 | bin/PamDirectory.sh Extract {EXPORT} {QUERY} {MASTER_PASSWORD}
```

Examples:

```
1 | bin/PamDirectory.sh Extract ~/Documents/xtan/apps/export/xtamexp-20180103113616-119836-0001.zip "Domain Controller" 48BRU7ikr9oIt2YKwzOYBQSoqwI22wAy
```

```
1 | bin/PamDirectory.sh Extract ~/Documents/xtan/apps/export/xtamexp-20180103113616-119836-0001.zip 168473 48BRU7ikr9oIt2YKwzOYBQSoqwI22wAy
```

```
1 | bin/PamDirectory.sh Extract ~/Documents/xtan/apps/export/xtamexp-20180103113616 168473 -
```

```
1 | bin/PamDirectory.sh Extract ~/Documents/xtan/apps/export/xtamexp-20180103113616 "Domain" -
```

5. The command output will display this record's information including the secret parameters. An **Ok** will be printed at the end of the output results.

Output:

```
1 | -----
2 | id=168473
3 | name=Domain Controller
4 | host=10.0.0.2
5 | description=Primary Domain Controller
6 | type=Windows Host
7 | Host=10.0.0.2
8 | Port=3389
```

```
9 | User=domain\\administrator
10 | Password=ZH3zFVzJ8KcZPTTE
11 | Ok
```

## Extract a list of records

If you are unsure of the Record Name or ID or would simply like to extract a list of records from the Exported Database, the PAM Administrator would perform these steps:

1. Login to the server that is hosting the PAM as an Administrator.
2. Open a command line session.
3. Navigate to \$PAM\_HOME. This is the installation folder for the PAM.
4. Execute the following command to extract a list of records. The following variables will need to be replaced as necessary.
  - {EXPORT}: The full path to the exported database .ZIP file or the beginning of the .ZIP file for multi-part exports.
  - {QUERY}: The query search for records. This query will return a list of all records (record name, ID, host and description only):
    - a. For Windows, substitute your {EXPORT} and {QUERY} values and issue this command.

```
1 | bin\PamDirectory.cmd ListExport {EXPORT} {QUERY}
```

Examples:

```
1 | bin\PamDirectory.cmd ListExport c:\xtam\export\xtamexp-20180103113616-119836-0001.zip "Domain Controller"
```

```
1 | bin\PamDirectory.cmd ListExport c:\xtam\export\xtamexp-20180103113616 "Domain"
```

- b. For Unix, substitute your {EXPORT} and {QUERY} values and issue this command.

```
1 | bin/PamDirectory.sh ListExport {EXPORT} {QUERY}
```

Examples:

```
1 | bin/PamDirectory.sh ListExport ~/Documents/xtan/apps/export/xtamexp-20180103113616-119836-0001.zip "Domain Controller"
```

```
1 | bin/PamDirectory.sh ListExport ~/Documents/xtan/apps/export/xtamexp-20180103113616 "Domain"
```

5. The command output will display the record(s) returned by the query search but will only include the record's name, ID, host, description and type. An **Ok** will be printed at the end of the output results.

### Single Result Output:

```
1 | -----
2 | id=168473
3 | name=Domain Controller
4 | description=Primary Domain Controller
5 | host=10.0.0.2
6 | type=Windows Host
7 | Ok
```

### Multiple Result Output:

```
1 | -----
2 | id=168473
3 | name=Domain Controller
4 | description=Primary Domain Controller
5 | host=10.0.0.2
6 | type=Windows Host
7 | -----
8 | id=178125
9 | name=Domain Controller Backup
10 | description=Backup Domain Controller
11 | host=10.0.0.3
12 | type=Windows Host
13 | -----
14 | id=274586
15 | name=Domain Administrator
16 | description=Shared domain Admin account
17 | type=Active Directory
18 | Ok
```

## Best Practices

### Planning your Build Out

The key to a successful deployment and ultimately user adoption is proper planning.

Before you begin your build out process, please consider the following questions and scenarios.

- What are you trying to accomplish with PAM? Do you plan on using your records for secure vaulting and sharing, session management, task automation or all the above?
- Which (and how many) assets, accounts and secrets do you plan on securing within PAM?
- Will PAM be used by a select group of power users like your IT Department or will it be rolled out across your entire organization?
- How do you plan on categorizing your records in PAM so they can be easily found and managed? Organized by department, relationship, or geographies?
- Are approval workflows (Dual Control, Four-eyes) required on any of your records?
- Should users' login with PAM local accounts or reuse their AD or LDAP accounts? Do you want to implement another layer of security by integrating with multi-factor or two-factor authentication?
- Do you understand your "[break glass](#)" scenario?

Answering these questions and understanding your true objective prior to deploying PAM is crucial to starting out on the right foot.

This may require spending time interviewing your various stakeholders and colleagues, gathering requirements and of course collaborating with your team during this process.

While it is possible to change course after the product has been rolled out into production use, it is easier on everyone to start from a solid foundation and build upon it.

Let's get started on building that solid foundation.

## Using Folders for Organization and Inheritance

When most computer users think of electronic organization they tend to think about a Windows file system.

While you certainly could keep all your documents in the root of your **My Documents** folder or your *Desktop*, that makes it quite cumbersome and difficult to find, use and share documents when needed.

Instead, users quite rightly create folder hierarchies to organize these files into some logical structure.

Much like these modern file systems, PAM operates with the same underlying structure of folder organization.

PAM folders contain records or folders and provide the *following benefits*:

- Can be used to easily categorize records based on similarities like department, asset, geographies, office locations and the like.
- Can be used to simplify sharing by establishing a permission inheritance model on a parent folder.
- Can be used to simplify workflow bindings by establishing a workflow inheritance model on a parent folder.
- Each folder can be thought of as individual vault with its own permission model.

When planning your folder hierarchy think about these benefits and how they may be applied to your business need. The more you can take advantage of all forms of logical groupings and inheritance, the easier it will be to manage, maintain and understand PAM.

## Example of a common IT scenario

You are managing several IT assets in PAM, a domain controller, a development web server and a production web server.

Your IT Manager will need access to all three, your Web Developer will only ever need access to your web server and your AD Admin will only ever need access to your domain controller.

How would you best create a folder hierarchy that would support this scenario (and be extensible to support future growth) while keeping the earlier benefits in mind?

A recommended approach would be to start with a parent folder like IT Infrastructure and then create sub-folders beneath it to organize assets by usage.

For example, a folder for Web Server assets and another for [Active Directory](#) assets.

When looking at this hierarchy it makes use of PAM folder benefits by:

- Grouping assets by logical similarities so users can easily find what they need.
- Makes use of permission inheritance by allowing IT Manager(s) access to all assets, Web Developer(s) access to only the web servers and AD Admin(s) access to only AD controllers.
- In a comparable manner to [permissions](#), approval [workflows](#) can be applied (as needed) to these same folders so extra safeguards are placed on the child records.
- Allows for future growth with logical extensibility. As you bring your other IT assets into PAM like your PBX servers, [Azure](#), and Amazon Web services accounts, API keys and more you simply create a new folder under IT Infrastructure and begin to apply the same methodology.

In summary, think about not only how records should be stored in folders, but also how they will be shared (or not shared) with others, if additional safeguards like approval workflows will be used and finally how this hierarchical structure can be expanded for future asset growth.

Once you have a handle on your [folders](#), it's time to begin thinking about your [records](#). But before you jump into creating records, we need to think about a record's foundation which are [record types](#).

## Understanding Record Types

[Record Types](#) are the foundation of [Records](#) simply because when creating a new record, you need to first select which record type to use.

When considering how to structure your [Record Types](#) in PAM, keep these concepts in mind:

- PAM comes with many out of the box record types built in. We recommend that you do not delete or modify these types.
  - Instead of modifying these types, consider creating a new custom record type using these default types as a *Parent* to extend their need.
  - Instead of deleting these types, consider using the *Hide* option to remove them from the list of record types that users can select. This keeps the PAM user interface clean and organized without invoking such a permanent action like *Delete*.
- If creating new record types, keep the names short and easily recognizable.
- Like folders, record types use inheritance for [Formulas](#), [Tasks](#) and [Command Control](#). Consider how these types will be used for records and if any unique or custom tasks can be applied for use with inheritance. Although an [AD](#) record and a Web Server record may both use a *Windows Host* type, the task(s) associated with each may be different so two record types can help in this situation.
- Custom fields can be added to record types to capture additional parameters to records.

How to effectively utilize record types in your PAM deployments is something that needs to be decided early on. Creating too many [record types](#) will lead to user confusion and management difficulties, while too few can lead to misuse by users and setup a scenario where they are not flexible enough to meet your future growth or demands.

# Managing Assets with PAM Records

You have your folder hierarchy, designed and built your record type hierarchy and now it is time to create records to manage your assets.

When [creating records](#), keep these concepts in mind:

- Can the use of a [reference account](#) be used to minimize [configuration](#) and task execution?
- Can I make use of the [Import](#) function to quickly populate records from `.CSV` files or other connection management and PAM products?
- Which folders should they reside in? Be conscious of inherited folder [permissions](#) or [workflows](#) when choosing this location.
- Which record types should be used? Remember [record types](#) use inheritance for [tasks](#), [formulas](#) and [command controls policies](#), so these objects will automatically be applied and could also be executed automatically.
- Should all users be able to create new records? Only users with Owner [permission](#) to a folder are permitted to [create new records](#) within it.

It is important to remember the principles of [inheritance](#) on both folders and types when [creating new records](#). If forgotten or misunderstood, you could unintentionally share an asset with a user.

## Sharing and Permissions

Sharing folders, records and access to PAM configuration are very important decisions that need to be made initially and need to be continually updated as necessary.

When planning your [PAM security](#) model, please keep these concepts in your design:

- Assign permissions to groups, rather than individual users, whenever possible. Managing group membership is far easier than managing hundreds of individual users.
- PAM Administrator role should only be given to a very select group of users. PAM Administrator has access to the entire PAM system including all records and folders, regardless of inherited permissions.
- When deciding which permission to grant, start at the lowest (Viewer) and then ask yourself, does this user or group need more access and if so, why? Starting with least privileged is best.
- Most users will not need more than Viewer permissions to any record or folder. This grants them the ability to see these objects, but not edit, unlock or compromise them.
- Users with Owner permissions to a record or folder have full control of that object (and inherited objects) including the ability to edit, share with others and delete. Limit the number of users who have this level of permissions to any objects.
- Permissions assigned to the PAM Root Folder are applied to the All Records view. That means if a user is granted Viewer permissions to Root Folder, they will have View permissions to every object (folder and record) in PAM that has the default inheritance configured.
- Make use of the PAM User and Inventory [reports](#) to periodically monitor your security model and ultimately make changes when and where needed.



# Tasks, Policies, Execution and Automation

[PAM Tasks](#) are objects that contain a script that is executed against the record's host or object and a policy that dictates when or how it is executed.

When considering your PAM deployment, you must also decide if you are going to take advantage of the PAM Task Engine, and if so, on what records.

Because tasks can also be deployed via inheritance, consider the following when building out your plan:

- Most default PAM record types come pre-built with tasks, which means the use of these record types will apply the tasks via inheritance (for example, *Windows Host* includes the *Windows Password Reset* task already assigned). Be conscious of this concept because some tasks can be set to automatically execute.
- Use [inheritance](#) whenever possible. Rather than organizing tasks on each individual record, consider applying them to record types for ease of use and management.
- [Formulas](#) (password complexity) can also be applied via inheritance which provides the ability to decide which types have more or less complex formulas.

Ensure you understand which Tasks will be applied to each record type when inheritance is being used.

A task may be applied without you realizing that could then run a script automatically (or scheduled) against your host record.

## Workflows

[PAM Workflows](#) provide an extra level of security to both records and actions that can be assigned to users, groups, folders or records.

If you are planning on including approval workflows (dual control, four-eyes) to your PAM deployment, please use the following as guidelines

- Whenever possible, keep the approval as simple as possible. If you require too complex of an approval process, the likelihood of it never being completed increases.
- Think about the who, what, when and where of workflow objects. Putting a workflow request in front of users who are trying to simply complete their work, could lead to frustration if it causes unnecessary slowdowns and layers upon layers of approval.
- Test your workflows (templates, bindings and notifications) with a small group of users before rolling it out to everyone. This will help find any misconfigurations or hiccups in the system before it is put into production use.

Approval workflows are a powerful, and often required, object in many systems throughout an organization, but it is important that they be efficiently built and deployed only where necessary. If you make them too burdensome and overbearing for users, then they will actively look for alternate methods to work around the system.

## Alerts and Notifications

PAM can be configured to send email notifications and in-app alerts to users who have subscribed to certain events.

If yourself or users are going to configure notifications, understand that:

- Alerts and Notifications are user profile specific. The alerts that you subscribe to are only for your account.
- PAM can be as noisy as you want it to be. When you first start out, think about what events you need to be alerted to. Over time, you can adjust the level of notifications, but like all notifications, the more we receive the less we tend to pay attention. Create alerts for notable events and use PAM reports for review.
- If you already have a Syslog or SIEM product capturing security alerts, consider [outputting PAM events](#) to your Syslog for consolidation, reporting and additional alerting.
- If you are a System Administrator, subscribe to system Error alerts so that you receive notifications in the event of system issues. Also subscribing to system Information or Warning events can quickly fill up your inbox or alert listings which can make PAM overly chatty.
- Email notifications (if configured) are sent to the email address associated to the AD account or the Local User account. Be sure these addresses are correct for all your users.
- Email notification templates can be customized. If you would like to change the wording, add or remove placeholders, feel free to do so. Use the test [email template](#) to try your changes before applying them to the production templates.

Take advantage of alerts and notifications, over alert yourself in the beginning stages and then gradually scale back on the events that are less important.

Finding that happy medium between alerts and noise is key to effectively managing PAM.

## Administrative Responsibilities

Like all solutions that are brought under the IT or Security umbrella, a certain amount of maintenance and monitoring by PAM Administrators is recommended.

The following list provides a look into what these duties may entail:

- Do not lose or misplace the [master password](#) that is generated during installation. PAM is encrypted and it cannot be decrypted without this password.
- Ensure you have an adequate [export plan](#) in place (either manual or periodic). Without exports, there is no way to recover from disasters or data loss.
- Monitor system performance on a regular basis, both on and off-peak times. Ensure session connectivity is not lagging, tasks are executed in an expectable amount of time and the user interface is responsive.
- PAM follows an agile release process with weekly [updates](#). When an update becomes available, read the [release notes](#) and if you choose, deploy the update. Keep in mind, that this update should be done during an off-peak time and you should check for any active sessions or scheduled tasks before you begin, as services will go offline during the update process.
- Test any changes that may affect other users before making them. If you have a UAT environment, test system changes, including record types, workflows, tasks and updates, there first and then make them available in production.

# Conclusion

The purpose of this guide was to introduce certain concepts related to Privileged Access Management solutions, specifically Privileged Access Management and to alert you to specific considerations that should be kept in mind when building out your PAM deployment.

PAM makes broad use of inheritance across many objects so that configuration and management of the system can be simplified, but to achieve this goal you need to plan for it.

It's important to get started in the right direction to minimize the changes that may need to be done later, but it is also important to understand that changes can be made later.

Plan, test and deploy, let users login and start using PAM, then reflect on their behavior and requirements and adopt changes were needed.

For additional guidance, consider reviewing common [standards and regulations](#) mandated in your geography or industry. Regulations like NIST, GDPR, ISO and HITRUST can also be helpful when implementing specific policies in PAM.

In the end, a PAM solution deployed in any configuration (even our default settings) is much better than a PAM solution not deployed.

# Installation

## System Requirements

The following are minimum requirements to use PAM for Single Server and medium use Production farms. If questions about architecture and system recommendations for large scale farm deployments remain or issues arise while using PAM, please contact our Support team:

<https://support.imprivata.com/communitylogin>.

	Single Server, Test or Quick Trial	Medium Use Production Farm
Windows O/S (64-bit only)	Windows Server 2019+ / Windows 10	Windows Server 2019+
Other O/S (64-bit only)	Red Hat, Ubuntu, Debian, CentOS	Red Hat, Ubuntu, Debian, CentOS
Database	Included*	MS SQL, MySQL, Oracle, PostgreSQL
Memory (reserved for PAM use)	4GB+	8GB+
Disk Space (reserved for PAM use)	20GB+	50GB+

\*For Single Server, Test or Quick Trial deployments the recommendation is to use the included, internal database however you can use any of the other supported databases that are available to you.

## Software Requirements

Web Browsers: Windows Edge, Google Chrome, Mozilla Firefox or Apple Safari.

Starting July 17, 2022, the Internet Explorer browser will no longer be supported. We recommend IE users transition to using the latest version of Microsoft Edge, Google Chrome or Mozilla Firefox with Imprivata PAM.

## External Database

The default installation includes an internal database that can be deployed. If you would prefer to use an existing database in your environment, the following are supported with a recommendation of **4GB minimum** for disk usage (considerably more if Session Video recordings are configured for database storage).

Please be prepared to supply a valid connection string to your database as well as an appropriate user and password to successfully establish this connection. *Please contact your Database Administrator if you need assistance.*

- Apache Derby version 10.12.1.1+
- Microsoft SQL version 2016+ (SQL Authentication only)

- MySQL Community or Enterprise Edition version 5.7+
- Oracle version 11.2+
- PostgreSQL version 9.5+

If using MySQL or MariaDB as your external database, please make sure **Pessimistic Locking** is enabled. Optimistic locking, which may be the database's default setting, may cause issues with some PAM functionality and is therefore not a supported setting.

## Trial and POC Prerequisite

### System Requirements

The Minimum Requirements are meant for trial, sandbox, and POC environments, Recommended Requirements are intended for production deployments.

### Minimum requirements for basic deployments and trials

Application Server with PAM Internal Database
4 CPU Cores
8 GB RAM (4GB is serviceable but 8GB is better)
30 GB Disk Space
<b>Base OS:</b> Windows Server 2019 <b>Or</b> Linux Server, Latest LTS version (Centos, RHEL, Amazon Linux, Ubuntu)

### Recommended requirements for Production deployments

PAM Application server	External Database Server
4 CPU Cores	Choose one of the following Databases
16 GB RAM	MySQL, MariaDB, MS SQL, PostgreSQL, Oracle, Azure SQL, AWS Aurora, AWS RDS
100 GB Disk Space	Follow the database vendor's hardware and software requirements
Windows Server 2019 <b>Or</b> Linux Server, latest LTS version (Centos, RHEL, Amazon Linux, Ubuntu)	

### Hardware Requirements

PAM can be installed on a physical server or virtual machine on premise or in the cloud.

If you would like to set up front-end (application) clustering, you will need to have two or more PAM servers (PAM Nodes) available and an external database.

For testing of high availability for the Database Server side, you can use your existing high availability database infrastructure or database mirroring. If you choose to test this, this is something your database team will need to prepare in advance.

## Software Requirements

### *Application Server*

PAM can run on Windows or Linux. We recommend installing PAM on freshly installed and updated Windows Server 2019 or newer or a Linux Server OS such as the latest LTS version of Centos, RHEL, Amazon Linux, or Ubuntu.

### *Database Server*

PAM comes with an internal database (Apache Derby) which is fine for POC, Trials and Small deployments that do not require HA.

For additional scalability an external database can be created in an existing database instance, or a new installation of a database server.

PAM supports several different database types including MySQL, MariaDB, MS SQL, PostgreSQL, Oracle, Apache Derby, Azure SQL, AWS Aurora, and AWS RDS.

If you plan on using an external database please have an account with the appropriate permissions available and the database pre-created as per our installation guide.

If using MySQL or MariaDB as your external database, please make sure **Pessimistic Locking** is enabled. Optimistic locking, which may be the database's default setting, may cause issues with some PAM functionality and is therefore not a supported setting.

## *Installation Guides*

### [PAM Installation and Setup](#)

Checklist:

- Windows or Linux Server (1 server, minimum)
- Application server prerequisites above
- Use internal database or external Database Server (Pre-created database, 1 instance, minimum)
- Trusted Third Party Certificate to replace PAM Self Signed Certificate for HTTPS
- AD or LDAP Credentials if AD/LDAP integration is available or use PAM internal directory services.
- SMTP and/or IMAP Credentials for email integration (notification and approval)
- [Firewall Ports necessary](#)
- Advanced implementations and integrations could include various MFA and SSO providers as well as API integrations. If questions remain or issues arise while using PAM, please contact the Support team: <https://support.imprivata.com/communitylogin>.

# Test Accounts

To test some of the basic features of PAM we recommend you have a few servers and accounts ready.

- Windows Server to Test RDP and password rotation
- Linux Server or Linux based Network Device to test SSH sessions and password rotation
- Native Client Testing using PAM advanced RDP, SSH and Http(s) proxies
- Additional Test Machines and Test accounts can be added as testing progresses

# Ports in Use

Below is a list of TCP (Transmission Control Protocol) ports that are used by PAM (Privileged Access Management).

## Open Ports required

Table 1: Open Ports required to install PAM (default configuration)

Process	Description	Port Number
HTTPS Proxy (inbound)	When the PAM HTTPS Proxy Feature is enabled (configured in Settings)	8081
Internal Database	PAM Internal Database	1527
Internal User Directory	PAM Local Directory Services	10389/10636
Session Manager	PAM Session Manager module	4822
SSH Proxy (inbound)	When the PAM SSH Proxy Feature is enabled (configured in Settings)	2022
RDP Proxy (inbound)	When the PAM RDP Proxy Feature is enabled (configured in Settings)	3388
PAM Web Application	HTTPS	6443
PAM Web Application	HTTP	8005
PAM Web Application	HTTP	8080

# Ports used

Table 2: Ports used by PAM Operations (some are optional and user configurable)

Process	Description	Port Number
Active Directory Integration	LDAP/LDAPS	389/636 or 3268/3269
MS SQL Database	Identity Vault (default, but configurable)	1433
MySQL or MariaDB Database	Identity Vault (default, but configurable)	3306
Oracle Database	Identity Vault (default, but configurable)	1521
PostgreSQL Database	Identity Vault (default, but configurable)	5432
Remote Desktop (Sessions)	Windows Host sessions (default, but configurable)	3389
Remote Job Execution (Windows Tasks)	Executing remote tasks for Windows endpoints	5985/5986
SSH (Sessions and Tasks)	SSH sessions and task execution (default, but configurable)	22
Telnet (Sessions)	Telnet Host sessions (default, but configurable)	23
VNC (Sessions)	VNC Host sessions (default, but configurable)	5900+n

## Saving master password during installation

Why is it so important to save my master password during installation? What would I need this for in the future?

PAM encrypts sensitive data stored in the backend database using an AES-256 algorithm.

This algorithm is based on the master key that PAM uses to lock and unlock encrypted data.

Without the master key nothing can decrypt sensitive data in your PAM database.

```
Administrator Account: pamadmin / leveled-revoke-powders?
Directory Password: R7HmHmyreTdQX8
Master Password: TAIQBo2ZY9eRuvIPcmxOM0uK0DDMfRZJ
Database Password: EAn7HP959Xrrs4
```

```
System Admin: pamadmin/Mq7b16
Master Password: Ok: uicvb6UBAQGa83AYvPHtEBc2YAyMkCau
DB Password: Ok: 0L4yEBTDpIr3Y3
Directory Admin Password: Ok: SU8Qwtpn4qDpKl
```

Master Passwords are generated and displayed during installation.

A Windows installation is demonstrated on the left and a Unix installation is demonstrated on the right.

Continue reading [here](#) for additional information about the master password and its use.

## Certificates

### Generate a Certificate Request for your PAM Server

The following article describes the process of generating a certificate request for your PAM server.

Before proceeding, be sure that you have access to the PAM host server (the server on which PAM was installed) and have enough permissions on this server to execute commands and update files.



1. Login to PAM host server and open a command line. Be sure you have the required permissions to execute commands *and / or* run the prompt as an administrator.
2. In the command prompt, navigate to the directory where PAM is installed. We will reference this as `$PAM_HOME`.
3. Type the below command to generate the server's private key. PAM's private key will be located in a `key-store` and both the keystore and the private key will be generated in this step. Please be sure that both the keystore and the private key password are identical.

- a. For Windows deployments:

```
1 | bin\PamKeytool.cmd -keysize 2048 -genkey -alias tomcat -keyalg RSA -  
   keystore xtamkeystore.jks
```

- b. For Linux deployments:

```
1 | bin/PamKeytool.sh -keysize 2048 -genkey -alias tomcat -keyalg RSA -  
   keystore xtamkeystore.jks
```

- c. When this command runs, first, enter and then re-enter a keystore password.
- d. Next, this command will prompt for the X.509 attributes of the certificate. Populate them based on the rules of the organization and Microsoft CA that will be used to generate a certificate. Make sure that the first attribute **First and last name (Common Name (CN))** will contain the domain of your website that you will access PAM with using HTTPS (i.e. [pam.company.com](https://pam.company.com)).
- e. When prompted for the password for the private key alias, press **Enter**. This will set the private key password to the same password used for the keystore entered in the beginning.

Note that SSL certificates can only be used on Web applications using the Common Name specified during CSR generation (in the **First and last name (Common Name (CN))** attribute).

For example, a certificate for the domain "[domain.com](https://domain.com)" will receive a warning if accessing a site named "[www.domain.com](https://www.domain.com)" or "[secure.domain.com](https://secure.domain.com)", because "[www.domain.com](https://www.domain.com)" and "[secure.domain.com](https://secure.domain.com)" are different from "[domain.com](https://domain.com)".

4. Next we will generate a CSR off the generated private key. Type the following command:

- a. For Windows deployments:

```
1 | bin\PamKeytool.cmd -certreq -keyalg RSA -alias tomcat -file xtam.csr -  
   keystore xtamkeystore.jks
```

- b. For Linux deployments:

```
1 | bin/PamKeytool.sh -certreq -keyalg RSA -alias tomcat -file xtam.csr -  
   | keystore xtamkeystore.jks
```

- c. As a result, you will have the file **xtam.csr** in the `$PAM_HOME` directory. Use this file to generate your SSL certificate in Microsoft CA.
5. PAM expects the resulting certificate to be in the format PFX and be in the file with the extension `.pfx`. When you will generate it, use it as the PAM Server certificate. If, instead of a `.pfx` file the certificate authority will generate root (**root.crt**), intermediate (**bundle.crt**) and certificate (**xtam.crt**) CRT files then copy them to the `$PAM_HOME` directory and finally import them into the same keystore generated earlier using the following commands from the `$PAM_HOME` directory:

Make sure to replace the below file names **root.crt**, **bundle.crt** and **xtam.crt** with the certificate file names generated by your CA.

- a. For Windows deployments:

```
1 | bin\PamKeytool.cmd -import -alias root -keystore xtamkeystore.jks -  
   | trustcacerts -file root.crt
```

```
1 | bin\PamKeytool.cmd -import -alias intermed -keystore xtamkeystore.jks -  
   | trustcacerts -file bundle.crt
```

```
1 | bin\PamKeytool.cmd -import -alias tomcat -keystore xtamkeystore.jks -  
   | trustcacerts -file xtam.crt
```

- b. For Linux deployments:

```
1 | bin/PamKeytool.sh -import -alias root -keystore xtamkeystore.jks -  
   | trustcacerts -file root.crt
```

```
1 | bin/PamKeytool.sh -import -alias intermed -keystore xtamkeystore.jks -  
   | trustcacerts -file bundle.crt
```

```
1 | bin/PamKeytool.sh -import -alias tomcat -keystore xtamkeystore.jks -  
   | trustcacerts -file xtam.crt
```

- c. After that use the file `$PAM_HOME/xtamkeystore.jks` (use the full path) as a certificate with the password you generated in **step #3**.

# Using Self-Signed Certificates

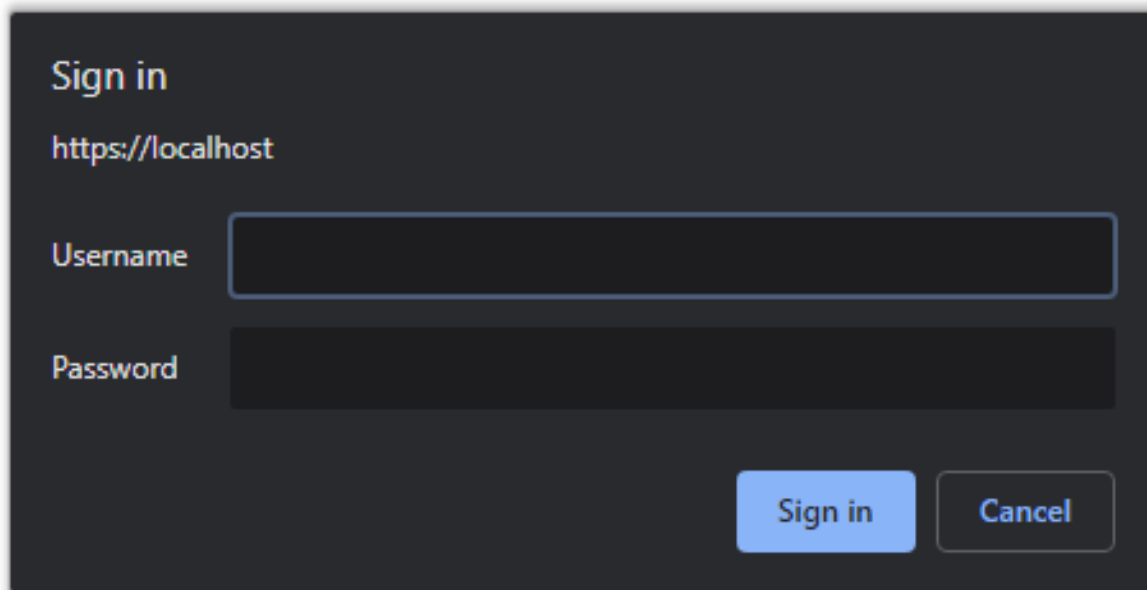
## Changing PAM from a basic login prompt authentication to a login page

If you did not include the [Federated Sign-In](#) Services (CAS) component during the installation, this basic pop-up prompt is the expected login behavior.

This basic pop-up prompt is secure and is designed to handle both local and domain (if configured on the server) user authentication functionality.

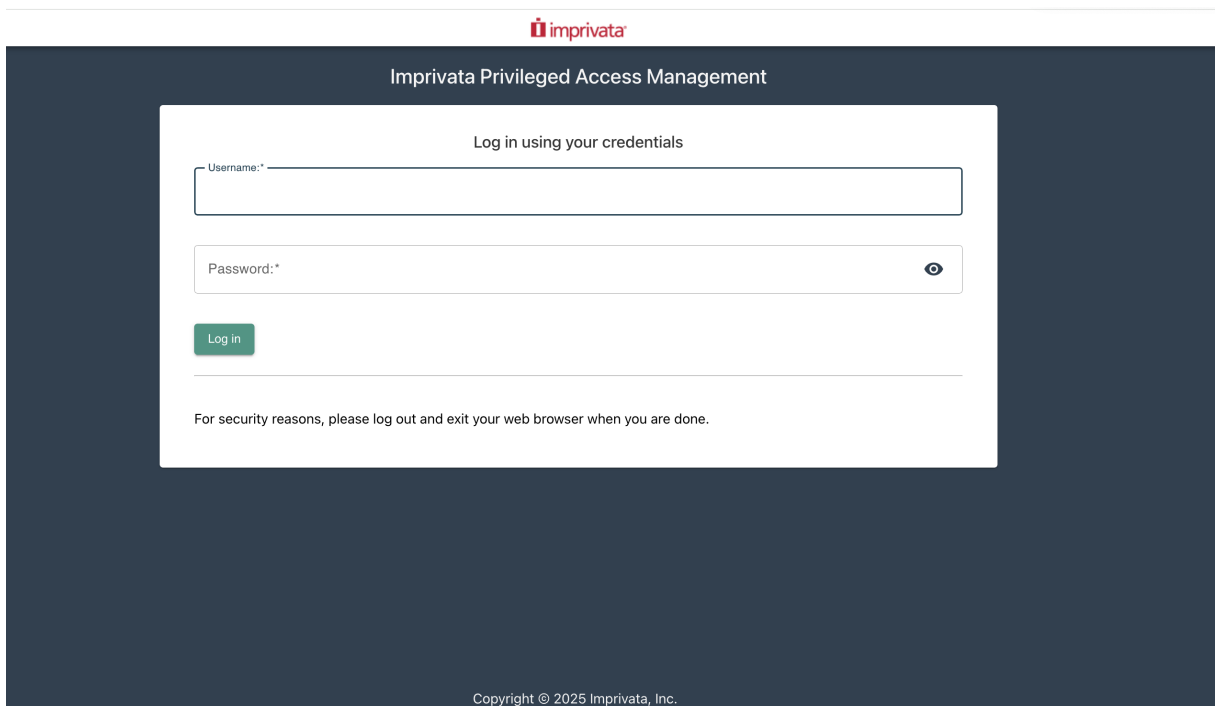
You can login with this pop-up prompt using your pamadmin user and the password you have created during the installation and proceed to use PAM's functionality.

This basic authentication is a valid option for all types of deployments that do not require advanced authentication options like MFA or SSO.



If you would like to switch your PAM deployment to display a more traditional login page instead of the pop-up dialogue to authenticate users (optionally with [MFA](#) or [SSO](#) options), you need to install with its included Federated Sign-In component or [deploy it after the installation](#).

As a PAM Administrator, you can [customize your Federated Sign-In page](#) if needed.



Please note that to support the [Federated Sign-In](#) login page experience, you will need to access PAM using a proper URI (not default localhost or an IP address) with a valid [SSL certificate](#) trusted by browsers, unlike the included self-signed certificate that generates browser warnings.

[Here](#) is the article describing how to replace PAM's default self-signed certificate with the trusted one obtained for the proper URI you assign to PAM (such as [pam.company.com](#)).

## Generating of a Self-signed Certificate

I do not currently have a self-signed certificate, but I would like to generate one.

The following section will describe how to use PAM to create your own self-signed certificate (in JKS format) and then configure PAM to use it.

Please note that this self-signed certificate may not be trusted by all your internet browser, so you may still receive a [browser security warning](#).

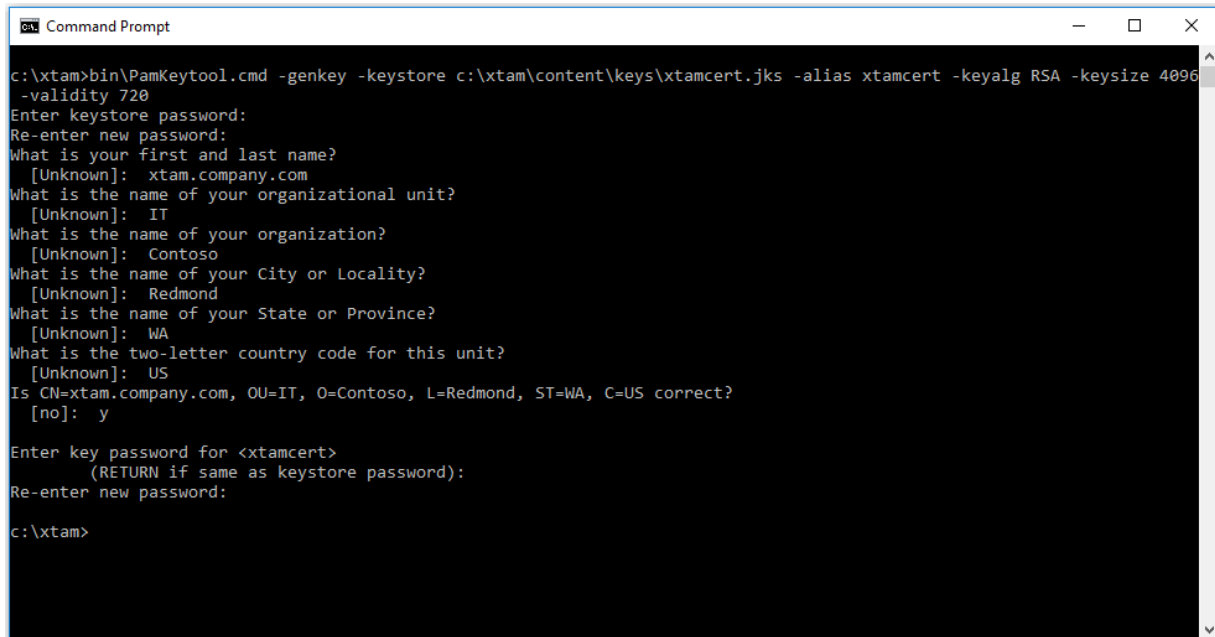
1. Login to the server where PAM is installed.
2. Open a command line and navigate to the folder where PAM is installed `$PAM_HOME` and issue the following command:
  - a. For Windows, substitute your `PATH_TO_KEY_STORE.jks` with a location where the certificate file will be created and its name (for example, `c:\pam\content\keys\xtamcert.jks`). `ALIAS_NAME` is a unique identifying string for the key and can be any value, avoiding spaces and special characters (for example, `xtamcert`)

```
1 | bin\PamKeytool.cmd -genkey -keystore PATH_TO_KEY_STORE.jks -alias ALIAS_
   | NAME -keyalg RSA -keysize 4096 -validity 720
```

- b. For Unix or Linux, substitute your `PATH_TO_KEY_STORE.jks` with a location where the certificate file will be created and its name. **ALIAS\_NAME** is a unique identifying string for the key and can be any value, avoiding spaces and special characters:

```
1 | bin/PamKeytool.sh -genkey -keystore PATH_TO_KEY_STORE.jks -alias ALIAS_
   | NAME -keyalg RSA -keysize 4096 -validity 720
```

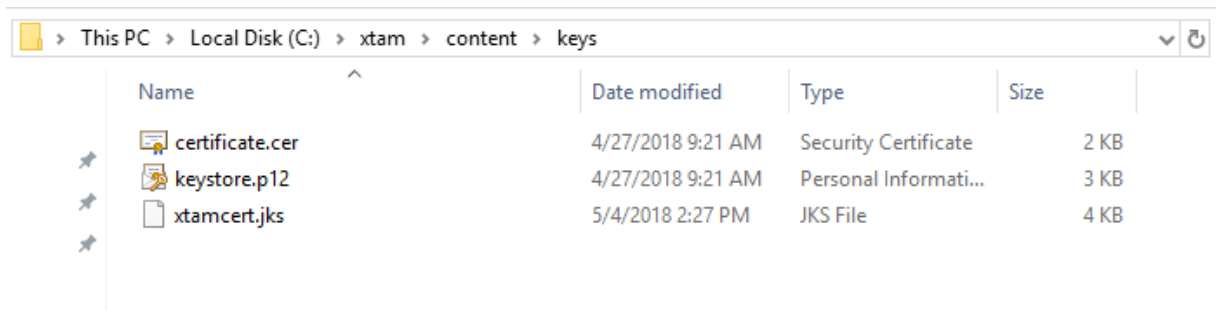
3. After the command is issued, you will be prompted for a number of values. Enter values as described below:
- Keystore Password:** Create a password for the keystore directory defined in the **PATH\_TO\_KEY\_STORE** location.
  - First and Last Name:** The domain name of the server. It looks wrong, but you need to enter the domain name for the certificate here. For example, *xtam.company.com*.
  - Organizational Unit:** Your department name.
  - Organization:** Your company name.
  - City or Locality:** Your city or locality name.
  - State or Province:** Your state or province name.
  - Country Code:** Your two letter country code.
4. Confirm you information by entering **y** for Yes.
5. Create a new password for the key (as defined by its alias name) or reuse the keystore password by pressing the **Enter** key.



```
Command Prompt
c:\xtam>bin\PamKeytool.cmd -genkey -keystore c:\xtam\content\keys\xtamcert.jks -alias xtamcert -keyalg RSA -keysize 4096
-validity 720
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: xtam.company.com
What is the name of your organizational unit?
[Unknown]: IT
What is the name of your organization?
[Unknown]: Contoso
What is the name of your City or Locality?
[Unknown]: Redmond
What is the name of your State or Province?
[Unknown]: WA
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=xtam.company.com, OU=IT, O=Contoso, L=Redmond, ST=WA, C=US correct?
[no]: y

Enter key password for <xtamcert>
(RETURN if same as keystore password):
Re-enter new password:
c:\xtam>
```

6. The certificate will now be generated in the location defined in `PATH_TO_KEY_STORE.jks`



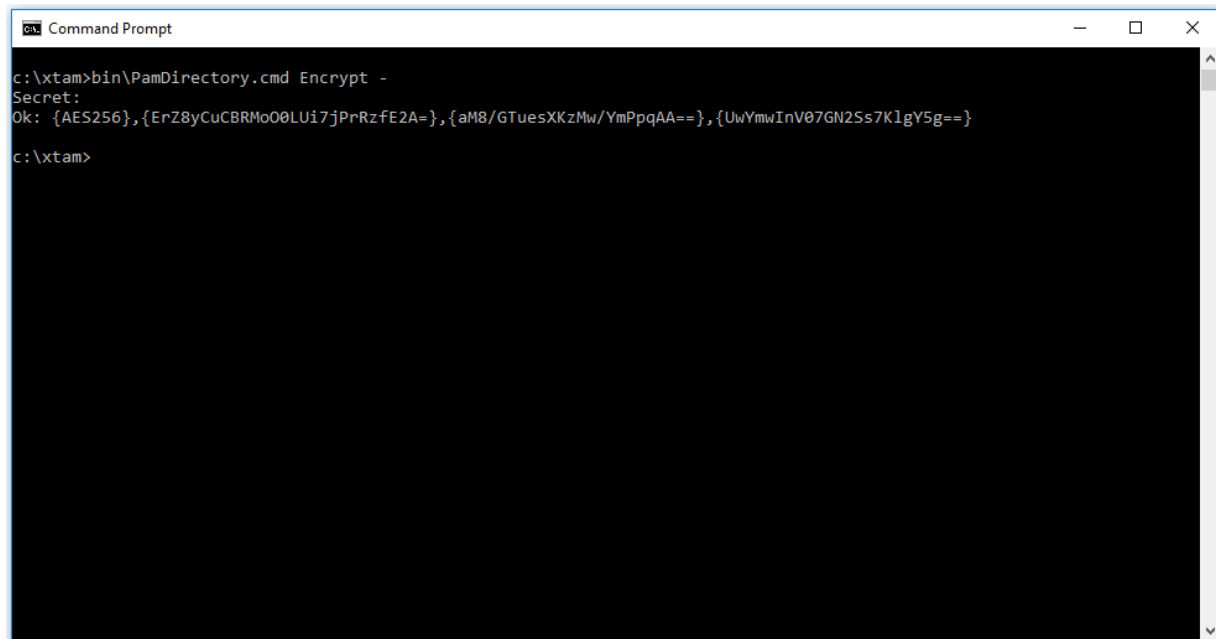
7. Now we want to encrypt your key password. In the same command line, issue the following command:
  - a. For Windows:

```
1 | bin\PamDirectory.cmd Encrypt -
```

- b. For Unix or Linux:

```
1 | bin/PamDirectory.sh Encrypt -
```

8. When prompted, enter your key password (the password from step 5) and press **Enter** to continue. The command output will display the full encrypted password string after the **Ok:** prefix.



9. Now that we have your new certificate (PATH\_TO\_KEY\_STORE.jks) and its encrypted password its time to configure it for use by PAM. Open the file: `$PAM_HOME/web/conf/catalina.properties`
10. Scroll down or search for the section labeled **# SSL Certificate**
11. In this section, replace the existing path and password with your new certificate and its password.
  - a. `xtam.cert.path={PATH_TO_KEY_STORE.jks}`
  - b. `xtam.cert.password={yourEncryptedPasswordString}`

```

# SSL Certificate
xtam.cert.path=C:/xtam/content/keys/xtamcert.jks
xtam.cert.password={AES256},{ErZ8yCuCBRM00LUi7jPrRzfE2A=},{aM8/GTuesXKzMw/YmPpqAA==},{UwYmwInV07GN2Ss7K1gY5g==}

```

12. **Save and close** this file.

13. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service.
14. Open your browser and navigate to the new login page. Remember, the PAM login will now be located at the domain defined in the certificate. For example, <https://xtam.company.com:6443/xtam>.

To summarize, you now have generated your own certificate, an encrypted password for it and have configured PAM to recognize and use this certificate.

This configuration will allow the use of PAM without the [Federated Sign-In](#) module.

## Troubleshooting: Key Store Password Incorrect

The same encryption password used in the `xtam.cert.password` in `catalina.properties` needs to be the same as the password used in the certificate that has the private key.

To fix the problem:

1. Delete the `.pfx` file and repackage this again, and then encrypt the password using the command:

```
1 | PamDirectory.sh Encrypt
```

2. Instead of using **-to prompt** for the secret, just Enter the Password directly to ensure that this is the same as was used in the keystore.
3. Copy out the encrypted password text and put this into the `catalina.properties` file.

In order to also use the [Federated Sign-In](#) module, then please continue to the next section.

## Checking of my Self-signed Certificate

If I imported my self-signed certificate already and want to check that it is in the PAM store.

1. Open a command line and navigate to the folder where PAM is installed `$PAM_HOME` and issue the following command:
  - a. For Windows, substitute `ALIAS_NAME` with the unique identifying string for the key, and `PATH_TO_CERT.der` with the location and name of the `.der` certificate file to be imported and used by the [Federated Sign-In](#) module.

```
1 | bin\PamKeytool.cmd -v -list -keystore jre\lib\security\cacerts
```

- b. For Unix or Linux, substitute `ALIAS_NAME` with the unique identifying string for the key, and `PATH_TO_CERT.der` with the location and name of the `.der` certificate file to be imported and used by the [Federated Sign-In](#) module.

```
1 | bin/PamKeytool.sh -v -list -keystore jre/lib/security/cacerts
```

2. After the command is issued, you will be prompted for the keystore password. Enter the value **changeit** and press the **Enter** key to continue.

The output will list all certificates currently found in the PAM store.

Please note that many well known trusted internet Certificate Authority certificates come with PAM out of the box, so you will need to search through all to locate your self-signed certificate.

## Importing a self-signed certificate for Federated Sign-In

While we continue to recommend the use of a [SSL certificate](#) from a well known internet Certificate Authority, we do understand that not everyone has nor wants to invest in such certificates.

If you have a self-signed certificate that you wish to use in order to use the [Federated Sign-In module](#), then please review the following article which outlines several scenarios and choose the one that fits your needs best.

## Replacing Self-signed Certificate with Trusted Certificate

Replacing the PAM Self-signed SSL certificate with your own Trusted SSL Certificate.

The default installation of PAM includes a self-signed certificate that is deployed in order to provide web traffic encryption.

Because this is a self-signed, non-trusted certificate you will receive a security warning message in your browser.

Although you could choose to accept the warning and safely proceed to the secured localhost connection or deploy the self-signed certificate to your Trusted Root Certificate Authorities store, some may wish to simply replace it all together with their own, trusted certificate.



### This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

✓ [Close this tab](#)

🔍 [More information](#)

**Your PC doesn't trust this website's security certificate.**  
**The hostname in the website's security certificate differs from the website you are trying to visit.**

Error Code: DLG\_FLAGS\_INVALID\_CA  
DLG\_FLAGS\_SEC\_CERT\_CN\_INVALID

⚠️ [Go on to the webpage \(not recommended\)](#)



To replace our self-signed certificate with your trusted certificate, please perform the following steps.

PAM expects the certificate to be in either `.jks` or `.pfx` format. If you have the certificate (`.crt`), the private key (`.key`) and bundle (`.crt`) as individual files, you can combine them into a single, PKCS12 encrypted compatible `pfx` file using an [OpenSSL](#) command like the example shown below (input your actual file names): **openssl pkcs12 -export -out "certificate.pfx" -inkey "private.key" -in "certificate.crt" -certfile "ca\_bundle.crt"**

1. On the PAM installation host server open the file `$PAM_HOME/web/conf/catalina.properties`. Consider making a copy of the file before making any modifications.
2. Scroll down to the section labeled **# SSL Certificate**
3. Enter the `$PAM_HOME` path to your certificate for the parameter **xtam.cert.path=**
4. Enter the password for your certificate in the parameter **xtam.cert.password=**

To encrypt your password, open a command prompt, navigate to the `$PAM_HOME` directory and issue this command: **bin\PamDirectory Encrypt -**. During command execution, you will be prompted to enter the password. Copy the entire encrypted password string output and paste it to the **xtam.cert.password=** parameter.

5. **Save and close** this file.
6. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service.
7. When the service restarts (takes ~1 minute to complete), your login page will now be located at the path defined in your certificate file rather than the default `localhost`. For example, `https://yourDomain.company.com:6443/xtam`.

## Error 500 Troubleshooting

You need to add the certificate to your local machine.

Follow these instructions to import all certificates one by one present in the certificate chain.

1. Import new Wildcard certificate into the PAM Server keystore.
2. Login to the PAM host server using Admin account or elevated privileges.
3. Open the command prompt or shell and navigate to the `$PAM_HOME` directory (where the PAM System is installed).
4. From `$PAM_HOME`, enter the following command:

For Linux:

```
bin/PamDirectory.sh SSLImport {Hostname} {Port}
```

Example of Linux command would be:

**bin/PamDirectory.sh SSLImport xtan.imprivata.com 6443**

For Windows:

```
bin\PamDirectory.cmd SSLImport {Hostname} {Port}
```

Example of Windows command would be:

**bin/PamDirectory.cmd SSLImport xton.imprivata.com 6443**

Follow these instructions to import all certificates one by one present in the certificate chain. After completed, restart the **PamManagement** (Windows) or **pammanager** (Linux) service. The website should be available after ~ 5 minutes.

## Self-signed certificate in DER format

I already have a self-signed certificate encoded in DER format that I would like to use.

The following section will describe how to import your certificate in `.der` format into PAM so that the [Federated Sign-In](#) module can be utilized.

If you do not have a certificate or if it is not in the `.der` format, please review the previous section of this article.

1. Open a command line and navigate to the folder where PAM is installed `{PAM_HOME}` and issue the following command:

- a. For Windows, substitute `ALIAS_NAME` with the unique identifying string for the key, and `PATH_TO_CERT.der` with the location and name of the `.der` certificate file to be imported and used by the Federated Sign-In module.

```
1 | bin\PamKeytool.cmd -import -alias ALIAS_NAME -file PATH_TO_CERT.der -  
keystore jre\lib\security\cacerts
```

- b. For Unix or Linux, substitute `ALIAS_NAME` with the unique identifying string for the key, and `PATH_TO_CERT.der` with the location and name of the `.der` certificate file to be imported and used by the [Federated Sign-In](#) module.

```
1 | bin/PamKeytool.sh -import -alias ALIAS_NAME -file PATH_TO_CERT.der -  
keystore jre/lib/security/cacerts
```

2. After the command is issued, you will be prompted for the keystore password. Enter the value **changeit** and press the **Enter** key to continue.
3. *When asked Trust this certificate [n]:* enter **y** for yes and press the **Enter** key to continue.
4. The confirmation message *Certificate was added to keystore* will appear when the import process has completed successfully.
5. Now that the certificate has been added, you can return to the [Federated Sign-In](#) article to complete the setup using this self-signed certificate.

The import is complete and now the PAM [Federated Sign-In](#) module is now setup to be secured with your own internal or self-signed certificate.

If you have done this previously, are unsure if the import was successfully or you simply want to double check, please [continue to the next section](#) to check which certificate are in the store.

## Self-signed certificate in JKS format

I already have a self-signed certificate encoded in JKS format that I would like to use.

The following section will describe how to convert your existing `.jks` certificate (like the one created in the previous section) into the `.der` format so that the PAM [Federated Sign-In](#) module can be used.

1. Open a command line and navigate to the folder where PAM is installed `{PAM_HOME}` and issue the following command:

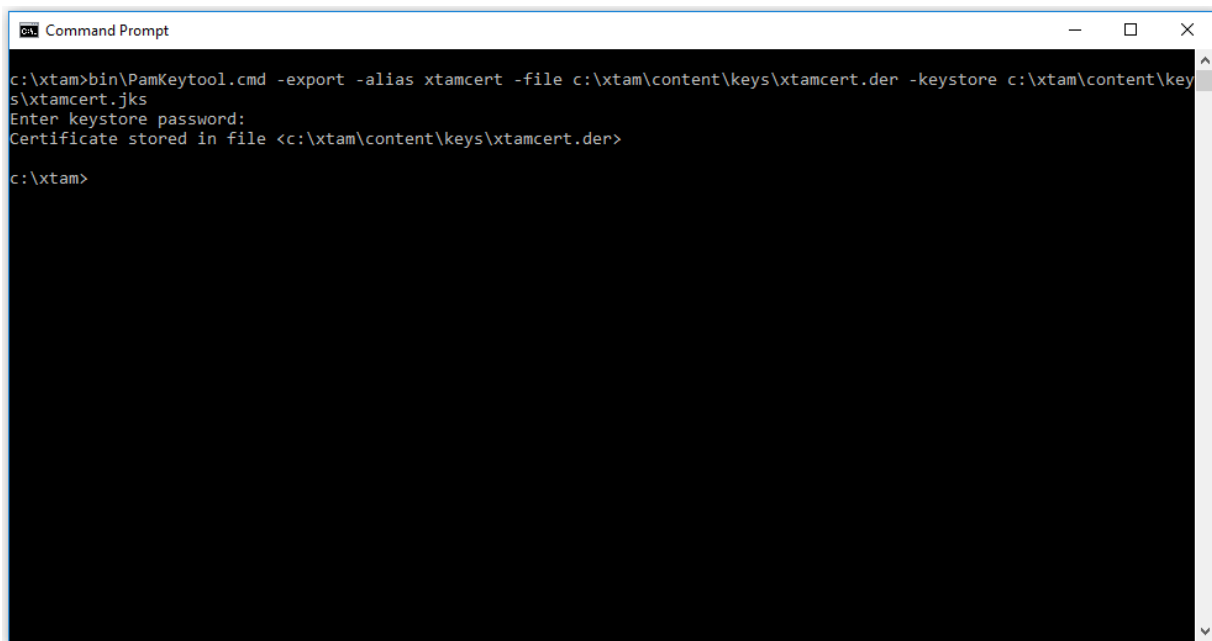
- a. For Windows, substitute `ALIAS_NAME` with the unique identifying string for the key, `CERTIFICATE.der` with the location and name of the converted certificate file in `.der` format and `PATH_TO_KEYSTORE.jks` with the location and name of the `.jks` certificate file to be converted.

```
1 | bin\PamKeytool.cmd -export -alias ALIAS_NAME -file CERTIFICATE.der -  
   | keystore PATH_TO_KEYSTORE.jks
```

- b. For Unix or Linux, substitute `ALIAS_NAME` with the unique identifying string for the key, `CERTIFICATE.der` with the location and name of the converted certificate file in `.der` format and `PATH_TO_KEYSTORE.jks` with the location and name of the `.jks` certificate file to be converted.

```
1 | bin/PamKeytool.sh -export -alias ALIAS_NAME -file CERTIFICATE.der -  
   | keystore PATH_TO_KEYSTORE.jks
```

2. After the command is issued, you will be prompted to enter the keystore password. Enter this password and press **Enter** to continue.



```
Command Prompt  
c:\xtam>bin\PamKeytool.cmd -export -alias xtamcert -file c:\xtam\content\keys\xtamcert.der -keystore c:\xtam\content\keys\xtamcert.jks  
Enter keystore password:  
Certificate stored in file <c:\xtam\content\keys\xtamcert.der>  
c:\xtam>
```

3. The certificate will now be converted and the message Certificate stored in file will be displayed.

Name	Date modified	Type	Size
certificate.cer	4/27/2018 9:21 AM	Security Certificate	2 KB
keystore.p12	4/27/2018 9:21 AM	Personal Informati...	3 KB
xtamcert.der	5/4/2018 2:41 PM	Security Certificate	2 KB
xtamcert.jks	5/4/2018 2:27 PM	JKS File	4 KB

Now we have converted your existing `.jks` certificate into a `.der` certificate so that the PAM [Federated Sign-In](#) module can be secured.

[Continue to the DER certificate section](#) to configure this certificate in the [Federated Sign-In](#) module.

## Self-signed certificate in something other than DER or JKS

I already have a self-signed certificate encoded in something other than DER or JKS that I would like to use.

The following section will describe how to convert your existing non-`.jks` or `.der` certificate into the `.der` format so that the [Federated Sign-In module](#) can be used.

For this we will download and use an external application called [OpenSSL](#) (external link) and provide a few common conversion examples.

Please review [OpenSSL documentation](#) for additional guidance.

There are several utilities available for certificate conversion, so if you would like to use something else ensure it can convert your current certificate format into `.der` format.

1. [Download](#) and install OpenSSL.
2. Open a command line, navigate to OpenSSL and issue the command specific to your conversion needs.
  - a. For example, to convert `.pem` format to `.der`:

```
1 | openssl x509 -in CERT.pem -out CERT.der -outform DER
```

- b. For example, to convert `.pfx` format to `.pem`:

```
1 | openssl pkcs12 -in certificatename.pfx -out certificatename.pem
```

When the conversion is complete (which may require more than one operation), your certificate is now in the required `.der` format.

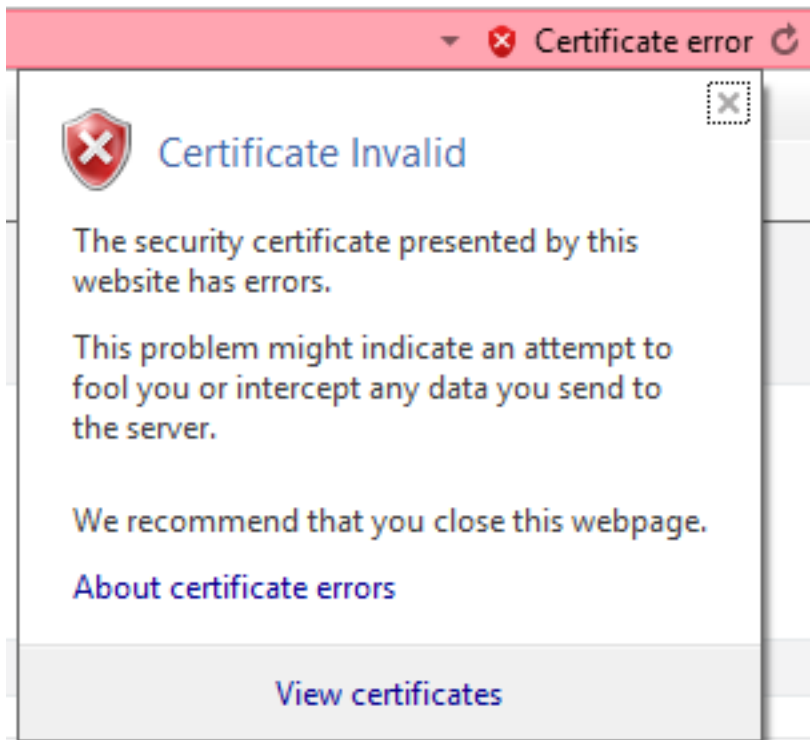
You can continue to the [next section](#) to configure the [Federated Sign-In](#) module with this certificate.

## SSL Certificate Web Browser Security Warning

I installed PAM and my web browser is telling me the connection is not secure. What does this mean?

PAM generates and deploys its own self-signed SSL Certificate during installation so that the secured **port 6443** can be used to encrypt the PAM web traffic.

Because this certificate is self-signed it is not recognized by your browser and certificate authority as trusted and therefore your web browser is rightfully reporting on this by displaying that security warning message.



To continue using the PAM installation, you may consider the following options with regards to the browser warning:

1. If you would rather avoid the use of the secured port all together, and therefore avoid the browser's security warning, you may consider logging in to PAM using the non-secured page at <http://localhost:8080/xtam>.
2. If you wish to continue using the secured port with our self-signed certificate, you should deploy this certificate to your Trusted Certificate Authority using the *Install Certificate* option.
3. If you already have your own trusted SSL certificate and wish to use it instead of ours, then please follow the procedure outlined here: [Replacing the SSL Certificate with a Trusted SSL Certificate](#).

While any of these options can be considered acceptable for Trial or Test deployments of PAM, we would recommend *replacing our certificate with your own trusted certificate* for all Production deployments.

## Sync Session Manager Certificates

Synchronizing session manager certificates between two nodes.

The concept for this article is that each node (A and B) has the PAM WEB GUI (**pammanager**) and the PAM Session Manager (**pamsession**).

On Node A, *pammanager* communicates with *pamsession* using the certificate pair from itself, node A.

On node B, these components use a different cert pair from itself, node B.

So the plan outlined in this article is to bring the certificate bundle from Node A to Node B and then import it to *pammanager* and *pamsession* on Node B.

Node A will remain the same.

- [Procedure for Windows deployment](#)
- [Procedure for Linux deployment](#)

## Windows Deployment

1. Login to both the Node A and Node B host computers. You may need Administrator permissions to perform this procedure.
2. On Node A, copy the `certbundle.zip` file located in `$PAM_HOME`. Paste this file to Node B.
3. On Node B, extract this copied `certbundle.zip` file to a location within `$PAM_HOME`. We will use `$PAM_HOME\ssl\` as an example to illustrate the procedure in this article.
4. On Node B, from a command prompt, navigate to `$PAM_HOME` and execute the following command. This command will remove the current certificate from the *PamManagement* service.

```
1 | bin\PamKeytool.cmd -delete -keystore jre\lib\security\cacerts -alias pam-session.cert
```

5. From the same Node B command prompt, we will now add the certificate copied from Node A to the Node B *PamManagement* service. Adjust the path accordingly to your specific file location.

```
1 | bin\PamKeytool.cmd -import -keystore jre\lib\security\cacerts -alias pam-session.cert -file ssl\pam-session.cert
```

6. On Node B, restart the **PamManagement** service.
7. On Node B, edit the file `$PAM_HOME\guacd\etc\guacamole\guacd.conf` in a text editor. Locate the line in this file that looks like the below. In this case, the key and cert files are located in the folder: `$PAM_HOME\guac\etc\ssl`.

```
1 | server_certificate = C:\xtam\guacd\etc\ssl\session.crt
2 | server_key = C:\xtam\guacd\etc\ssl\session.key
```

8. Replace that line with the one that contains the full path to the `session.crt` and `session.key` you copied from the Node A. In our example for the path we used in step 2 it will look like this:

```
1 | server_certificate = C:\xtam\ssl\session.crt
2 | server_key = C:\xtam\ssl\session.key
```

9. On Node B, after you update the `.conf` script, restart the **PamSession** service.

This completes the required host server configuration. You should now log out of both the Node A and Node B host servers.

Returning back to the PAM web, now you can have two named (not localhost) Session Manager nodes in the Administration > Proximity Groups for the default group and they both should be green (SSL connected). PAM will balance the traffic based on the number of sessions per node.

## Linux Deployment

1. Login to both the Node A and Node B host computers. You may need sudo or root permissions to perform this procedure.
2. On Node A, copy the `certbundle.zip` file located in `$PAM_HOME`. Paste this file to Node B.
3. On Node B, extract this copied `certbundle.zip` file to a location within `$PAM_HOME`. We will use `/opt/pam/ssl/` as an example to illustrate the procedure in this article.
4. On Node B, from your prompt, navigate to `$PAM_HOME` and execute the following command. This command will remove the current certificate from the **pammanager** service.

```
1 | bin/PamKeytool.sh -delete -keystore jre/lib/security/cacerts -alias pam-session.cert
```

5. From the same Node B prompt, we will now add the certificate copied from Node A to the Node B **pammanager** service. Adjust the path accordingly to your specific file location.

```
1 | bin/PamKeytool.sh -import -keystore jre/lib/security/cacerts -alias pam-session.cert -file ssl/pam-session.crt
```

6. On Node B, restart the **pammanager** service.
7. On Node B, edit the file `$PAM_HOME/bin/pamsession` in a text editor. Locate the line in this file that looks like the below. In this case, the key and cert files are located in the folder: `$PAM_HOME/guac/etc/ssl`.

```
1 | guac_ssl_opts="-C $home/guac/etc/ssl/session.crt -K $home/guac/etc/ssl/session.key"
```

8. Replace that line with the one that contains the full path to the session.crt and session.key you copied from the Node A. In our example for the path we used in step 2 it will look like this:

```
1 | guac_ssl_opts="-C $home/ssl/session.crt -K $home/ssl/session.key"
```

9. On Node B, after you update the **pamsession** script as noted in the previous step, you will need to reload the service. How to reload services depends on the specific Linux distribution you are using so please review your O/S guidelines for the specific function. It may be a command like this:

```
1 | systemctl daemon-reload
```

10. On Node B, restart the **pamsession** service.

This completes the required host server configuration. You should now log out of both the Node A and Node B host servers.

Returning back to the PAM web, now you can have two named (not localhost) Session Manager nodes in the Administration > Proximity Groups for the default group and they both should be green (SSL connected). PAM will balance the traffic based on the number of sessions per node.

## Create or renew the PAM Web server certificate

If the PAM Web server certificate has expired, what are the steps needed to renew this certificate? Follow instructions below.

1. Open a Command Prompt and cd to the `$PAM_HOME/PAM` folder.
2. Create the keystore:

```
1 | bin\PamKeytool.cmd -keysize 2048 -genkey -alias tomcat -keyalg RSA -keystore IPAMkeystore.jks
```

- Enter the keystore password (and record this password).
  - Verify the keystore password.
3. Complete the certificate details:
    - What is your first and last name?
      - This is the cert CN. Use the server FQDN
    - What is the name of your organizational unit?
      - This is the cert OU
    - What is the name of your organization?
      - This is the cert O
    - What is the name of your City or Locality?
      - This is the cert L
    - What is the name of your State or Province?
      - This is the cert ST
    - What is the two-letter country code for this unit?
      - This is the cert C
  4. Verify the certificate details are correct.
  5. Create the certificate request with the SAN.

```
1 | bin\PamKeytool.cmd -certreq -keyalg RSA -alias tomcat -keystore IPAMkeystore.jks -file ipam.csr -ext "SAN=dns:pam01.adroit.local,dns:pam01,ip:172.21.28.104"
```



- Enter the keystore password.

```
C:\XTAM>bin\PamKeytool.cmd -keysize 2048 -genkey -alias tomcat -keyalg RSA -keystore IPAMkeystore.jks
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]: pam01.adroit.local
What is the name of your organizational unit?
  [Unknown]: Adroit-Lab
What is the name of your organization?
  [Unknown]: Imprivata
What is the name of your City or Locality?
  [Unknown]: Melbourne
What is the name of your State or Province?
  [Unknown]: Victoria
What is the two-letter country code for this unit?
  [Unknown]: AU
Is CN=pam01.adroit.local, OU=Adroit-Lab, O=Imprivata, L=Melbourne, ST=Victoria, C=AU correct?
  [no]: y

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 90 days
        for: CN=pam01.adroit.local, OU=Adroit-Lab, O=Imprivata, L=Melbourne, ST=Victoria, C=AU

C:\XTAM>bin\PamKeytool.cmd -certreq -keyalg RSA -alias tomcat -keystore IPAMkeystore.jks -file ipam.csr
-ext "SAN=dns:pam01.adroit.local,dns:pam01,ip:172.21.28.104"
Enter keystore password:
```

- The `ipam.csr` file will be generated in the `$PAM_HOME` directory
6. Use the Base64 csr file to create a Web Server certificate in the Domain PKI (via the CA Website), or an external 3rd party PKI.

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded C (Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

-----BEGIN NEW CERTIFICATE REQUEST-----
0w8745yvntd078q34yrt9as3746rtwevb034n587:
67w34t5vh08327456t0w38746tn0w34587t6bv0w:
vw34876ytpbs9345n67p28vyn5bn6249pn24a6vf:
YUI087erg7ynaPOIUYTBN0876B0nOIUYTB0876B9:
tgbIOB876bgTYbiuytb9Bouuygb08V875bog0TBo:

```

**Certificate Template:**

Web Server 1yr ▼

7. Save the created certificate as a Base 64 encoded certificate chain (`ipam.p7b`):

## Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)



8. Import the certificate bundle:

```
1 | bin\PamKeytool.cmd -import -alias tomcat -keystore IPAMkeystore.jks -  
  trustcacerts -file ipam.p7b
```

- Enter the keystore password.

```
C:\XTAM>bin\PamKeytool.cmd -import -alias tomcat -keystore IPAMkeystore.jks -trustcacerts -file ipam.p7b  
Enter keystore password:  
Certificate reply was installed in keystore
```

9. Copy the `IPAMkeystore.jks` file to the `$PAM_HOME/web/conf` folder.
10. Update the `xtam.cert.path=` to reference the new `IPAMkeystore.jks` keystore file.
11. Update the `xtam.cert.password=` with the new password (if needed).
12. Restart the *PamManagement* / *pammanager* service.
13. Once the PAM Web server is running, browse to the webpage and verify that the certificate has been updated.

# Federated Sign-in Module

## Federated Sign-In

Federated Sign-In: benefits and configuration.

PAM provides a federated sign-in experience that can be deployed during or after installation.

The benefits of the PAM Federated Sign-In:

- A more easily recognizable enterprise web login page supporting single sign-on.
- Provides integration opportunities with many commonly used multi-factor authorization (MFA) and two-factor authorization (2FA) providers.
- Allows for the generation and use of Authentication Tokens.
- Allows configuration of session termination due to inactivity timeout while not accessing the application.
- Requires the use of a non-self signed SSL Certificate ensuring web client connectivity is secured.
  1. [Load Balancing for Debian or Ubuntu.](#)
  2. [Load Balancing for Red Hat or CentOS.](#)

Pre-requisite: Make sure a non-self signed, well known and trusted SSL Certificate is deployed and working in your Windows or Unix host. During installation, you will define the URL that PAM will use for web connectivity and this connection needs to be secured with a trusted web certificate. While we recommend using a trusted SSL certificate in all deployments scenarios, if you have a self-signed certificate, please see this [article](#) or configuration options.

[To Deploy PAM Federated Sign-In During Installation](#)

[To Deploy PAM Federated Sign-In Post Installation](#)

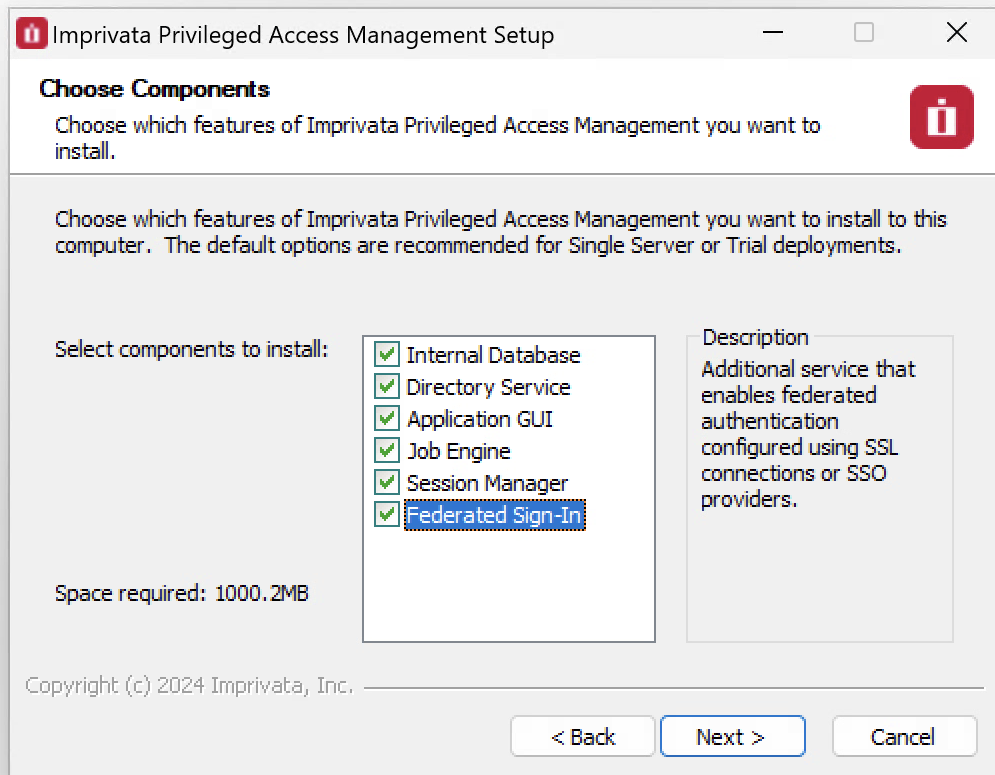
[Federated Sign-In – Certificate Errors](#)

[Federated Sign-In Module – Timeout Error](#)


[To Customize your Federated Sign-in page text](#)

## Deploying Federated Sign-In During Installation

1. During the installation, check the option to include the **Federated Sign-In** component in the wizard.



2. On the Federated Connection page, check the **Enable SSO** option and enter your secured URL into the **Managed Path** field.

 Imprivata Privileged Access Management Setup

**Federated Connection**  
Define your Federated Server Connection.

Enable SSO ☒

Managed Path

Please enter the managed path to your web application that is used for federation (for example, https://host.example.com:6443)

Central Authentication Service version  
☐ 5.2 (Legacy version)  
☒ 6.5 (Latest version)


If new deployment choose latest CAS 6.5, choose 5.2 if extending a pam deployment which is currently using CAS 5.2

Copyright (c) 2024 Imprivata, Inc.

[< Back](#) [Install](#) [Cancel](#)

Please note that if you are using a port other than 443, then please include this value in the Managed Path. For example: `https://xtam.company.com:6443`. In a multi-node setup or an HA environment using CAS v6, a correctly configured load balancer is required and must be setup with sticky sessions. The same managed path across all nodes is required to be set.


3. Complete the PAM installation as required.
4. When the installation is complete, the federated sign-in page will be available at the Managed Path entered in step 2 followed by `/xtam`.

 Imprivata

Imprivata Privileged Access Management

Log in using your credentials

Username:

Password:  

[Log in](#)

For security reasons, please log out and exit your web browser when you are done.

Copyright © 2025 Imprivata, Inc.

[To Customize your Federated Sign-in page text](#)

# Deploying PAM Federated Sign-In Post Installation

## Pre-requisites

- Update the software to its latest version using this guide: [Software Updates](#)
- Update the software's framework using this guide: [Updating the Framework](#)
- Update the software's web container using this guide: [Updating the WEB Container](#)
- Requirements for a multi-node setup or a High Availability (HA) environment using CAS v6:
  - A correctly configured load balancer setup with sticky sessions with the same managed path across all the nodes.
  - Synchronized properties for HA environments. Please follow this article to review and sync the PAM environment <https://help.xtontech.com/content/installation/advanced-deployments/ha-configuration-for-pam-deployments.htm>.
  - AD/LDAP integrations and properties between nodes should be checked and synced properly across the HA environment.
  - PAM certificates and all the certificates you use for your installation should be in a healthy state for all nodes across your HA environment.

Please read the entire procedure outlined in the article before beginning. If you have any questions, please contact the Support team: <https://support.imprivata.com/communitylogin>.

## Deploying PAM Federated Sign-In Post Installation

1. Download the PAM Federated Sign-In component to your PAM host machine (PAM Federated Sign-In download [CAS v5](#) or [CAS v6 \(recommended\)](#)).
2. When the download is complete, unpack the downloaded archive and copy its containing file `cas.war` to `$PAM_HOME/web/webapps`.
3. Edit the file `$PAM_HOME/web/conf/catalina.properties` and make the following modifications (if these any of these lines are not present, please add them):
  - a. Set the property `cas.managed.path` to PAM's managed path (secured URI) so it will look something like this `cas.managed.path=https://pam.company.com:6443`
  - b. Set the property `cas.server.name` to PAM's managed path (secured URI) so it will look something like this `cas.server.name=https://pam.company.com:6443`
  - c. Set the property `cas.server.prefix` to PAM's federated sign-in path (secured URI) so it will look something like this `cas.server.prefix=https://pam.company.com:6443/cas`
  - d. Set the property `cas.view.defaultRedirectUrl` to PAM's GUI URL (secured URI) so it will look something like this `cas.view.defaultRedirectUrl=https://pam.company.com:6443/xtam/`

Please take note of the port (:6443) in the above example. If you are using a port [other than the default 6443](#), update this line to reflect the port number being used. If you are using a reverse proxy which is using port 443 then a possible, working value may be <https://pam.company.com>.

1. Download and then unpack the web archive located [here](#).
2. Consider making a copy of the existing `web.xml` file in `$PAM_HOME/web/webapps/xtam/WEB-INF` in case of issues.
3. Copy the downloaded `web.xml` file to `$PAM_HOME/web/webapps/xtam/WEB-INF` replacing the file with the same name which already exists.
4. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service.
5. When the deployment is complete, the federated sign-in page will be available at the Managed Path entered in step 3a followed by `/xtam`.

Instruction for update [Federated Sign-In](#) component from CAS v5.2 to CAS v6.5 is [here](#).

## Migration to Federated Sign-In Module v6.5

Upgrading to the latest version of PAM provides you with enhanced security, improved performance, and access to all the newest features and enhancements we offer.

To fully benefit from these improvements and ensure optimal compatibility, we encourage you to update your Java environment to at least the minimum supported version.

The third-party vendor we rely on for Federated sign-in, has discontinued support for version 5.2.

As a result, any future enhancements to the PAM authentication module will be compatible only with Federated Sign-in v6.5.

This is a crucial change that needs to be addressed to maintain the security and functionality of your Federated sign-in process.

There are no risks in migrating PAM functionality as all features will be available.

However, while updating, the Federated Sign-in plugin in v6.5 can impact your SAML integration, specifically regarding keystores and metadata files.

Tokens generated with older versions will not work after the migration, so you must generate new ones as instructed in the guide.

## Pre-requisites

Before you begin your migration, be sure you meet the following pre-requisites:

- A working PAM deployment with the [Federated Sign-In](#) experience.
- In order to check the version of [Federated Sign-In](#) module you are on, login to PAM and navigate to Management> *About* and check value under "Authentication". If you are on version 5x, the value will be

version 5.2x.

- An operational PAM deployment with the latest version. Please update to the latest available version before proceeding.
- WEB Container on version 9.0.x.
- An operational PAM deployment with framework version 11, 12,13, 14, 15 or 17. If you are using 1.8\_x, please use [this guide](#) to update.

For PAM deployments integrated with SSO providers, it is necessary to reconnect SSO integration after upgrading from [Federated Sign-In](#) module version 5.2 to version 6.5. This is required because version 6.5 uses different key generation algorithms that are not compatible with the old version. The new keystore `.jks` and `.xml` metadata files should appear in `$PAM_HOME/content/keys` or another location that was defined in your configuration.

Optionally, rather than deleting these files, move the version 5.2 files to a backup location outside of `$PAM_HOME`.

- Requirements for a multi-node setup or a High Availability (HA) environment using CAS v6:
  - A correctly configured load balancer setup with sticky sessions with the same managed path across all the nodes.
  - Synchronized properties for HA environments. Please follow this article to review and sync the PAM environment <https://help.xtontech.com/content/installation/advanced-deployments/ha-configuration-for-pam-deployments.htm>.
  - AD/LDAP integrations and properties between nodes should be checked and synced properly across the HA environment.
  - PAM certificates and all the certificates you use for your installation should be in a healthy state for all nodes across your HA environment.

## Considerations

- The user performing the migration will be required to update files and configurations on the PAM host server. Administrative privileges are required.
- We highly recommend deploying a test instance of PAM that mirrors your production instance as closely as possible to test the migration ([DB type](#), [Federated Sign-In](#), [certificates](#), [MFA/SSO](#), [AD Integration](#), etc).
- Once the migration is successful with the test instance you can reproduce the procedure on your production instance.

The migration steps below need to be done across each node of the multi-node setup across the HA environment using CAS.

Please read the entire procedure outlined in the article before beginning. If you have any questions, please contact our Support team: <https://support.imprivata.com/communitylogin>.

# Migration from version 5.2x to version 6.5

For migration from [Federated Sign-In](#) module version 5.2x to Federated Sign-in module version 6.5 follow the next steps:

1. Configure PAM with the [Federated Sign-In](#) module and ensure that it is working properly.
2. Login to PAM host server.
3. Open a prompt and navigate to the `$PAM_HOME` directory and **delete** the old version of CAS:
  - a. Delete (or move) the file `$PAM_HOME/web/webapps/cas.war` (move this file outside of `$PAM_HOME` folder, please do not rename it in the same folder).
  - b. Delete (or move) the folder `$PAM_HOME/web/webapps/cas` (move this file outside of `$PAM_HOME` folder, please do not rename it in the same folder).
4. **Download** a new CAS version 6.5 file <https://bin.xtontech.com/product/pam-cas.65.zip> and extract the `cas.war` to `$PAM_HOME/web/webapps`.
5. Execute the following command from `$PAM_HOME`:

For Windows deployments:

```
1 | bin\PamDirectory.cmd SwitchCASVersion web 65
```

For Unix or Linux deployments:

```
1 | bin/PamDirectory.sh SwitchCASVersion web 65
```

6. Stop the **PamManagement** (Windows) or the **pammanager** (Linux) service. PAM will be offline until this procedure is completed.
7. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor. In this file, locate the section that begins with `#CAS` add the following new parameters:
  - a. for AzureAD and ADFS integrations add the following line (with the right index):

```
1 | cas.authn.pac4j.saml[0].useNameQualifier=false
```

- b. for ADFS integrations add the following line (with the right index):

```
1 | cas.authn.pac4j.saml[0].sign-service-provider-logout-request=true
```

If you are unsure if you are using an Azure AD or ADFS SAML integration, please review the following:

- If your SSO login redirects to a *microsoftonline* domain, it is likely Azure AD SSO.
  - If your SSO login redirects to *your domain*, it is likely ADFS.
  - You can also review the respective integration guides, [Azure AD SSO](#) and [ADFS](#), to check your current configuration to determine which integration is currently enabled.
8. Save and close the `catalina.properties` file when you are finished.
  9. for ADFS Relaying party add configuration in *ADFS Relaying Party Trusts* in the tab *Endpoints* add **SAML**:



```
1 | Endpoint Type: SAML Logout
2 | Binding: Redirect
3 | Trusted URL: {managed path}/cas/logout
4 | Response URL: {managed path}/cas/logout
```

10. If there are existing [SSO](#) integrations with PAM, you will need to generate new keystore `.jks` and `.xml` metadata files for all [SSO](#) integrations. This is required to the fact that the new CAS version 6.5 uses different key generation algorithms that are not compatible with the old version. To generate these metadata files, navigate to the `$PAM_HOME/content/keys` directory and delete all SSO related keystore `.jks` and `.xml` metadata files.

**We recommended, rather than deleting these files, move them to a backup location outside of \$PAM\_HOME.** These new metadata files will be regenerated during the service *restart* in the next step.

Note that you may need to upload the new `.xml` file to your SSO provider to complete the integration process. Please review the specific integration documentation for your SSO provider to determine if a reupload is required. Here are links to some of our SSO integration articles: [EAM](#), [Azure SSO](#), [Okta SSO](#).

11. In case of multi-node PAM deployments, all nodes should have these properties blocks synced:

```
1 | cas.authn.mfa.gauth.crypto.*
2 | cas.authn.mfa.yubikey.crypto.*
```

For example, these properties can be copied from Node 1 to all other master nodes. The properties would be:

```
1 | cas.authn.mfa.gauth.crypto.signing.key
2 | cas.authn.mfa.gauth.crypto.signing.keySize
3 | cas.authn.mfa.gauth.crypto.encryption.key
4 | cas.authn.mfa.gauth.crypto.encryption.keySize
5 |
6 | cas.authn.mfa.yubikey.crypto.signing.key
7 | cas.authn.mfa.yubikey.crypto.signing.keySize
8 | cas.authn.mfa.yubikey.crypto.encryption.key
9 | cas.authn.mfa.yubikey.crypto.encryption.keySize
```

12. Start the **PamManagement** (Windows) or the **pammanager** (Linux) service and try your updated authentication login.
13. Verify **cas.service-registry.core.init-from-json** in `catalina.properties` file:

- if value set to true, change it to false:

```
1 | cas.service-registry.core.init-from-json=false
```

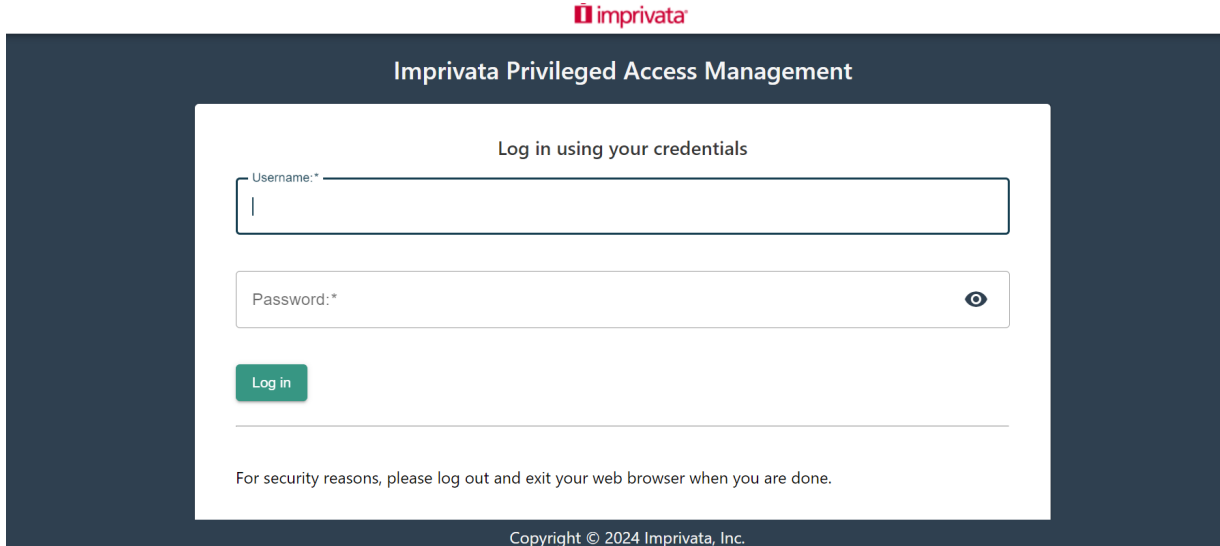
- restart the **PamManagement** (Windows) or the **pammanager** (Linux) service and try your updated authentication login.
14. Clear your browser cache.

15. Tokens generated with older version of [Federated Sign](#) in will not work post migration. New tokens will need to be generated by navigating to Administration > Tokens > **Generate Token**. If MFA is enabled prior to migration, users will be required to re-register their MFA configurations as well.

## Testing

The steps for testing [Federated Sign-in](#) module version 6.5:

1. When the service is fully restarted, open your browser, and navigate to the PAM login page.



imprivata

Imprivata Privileged Access Management

Log in using your credentials

Username:\*

Password:\*

Log in

For security reasons, please log out and exit your web browser when you are done.

Copyright © 2024 Imprivata, Inc.

2. Login to PAM.

## Rollback from version 6.5 to version 5.2

If a setup is deployed with version 6.5 which has never migrated from version 5.x, it will not work to just simply downgrade to version 5.2.

To rollback from Federated Sign-in module version 6.5 to Federated Sign-in module version 5.2:

1. Stop the **PamManagement** (Windows) or the **pammanager** (Linux) service. PAM will be offline until this procedure is completed.
2. Open a prompt and navigate to the `$PAM_HOME` directory and **delete** the old version of CAS.
  - a. Delete (or move) the file `$PAM_HOME/web/webapps/cas.war` (move this file outside of `$PAM_HOME` folder, please do not rename it in the same folder).
  - b. Delete (or move) the folder `$PAM_HOME/web/webapps/cas` (move this file outside of `$PAM_HOME` folder, please do not rename it in the same folder).
3. **Restore** the file `cas.war` for CAS version 5.2 to `$PAM_HOME/web/webapps` from the backup location or download the latest from:  
<https://bin.xtontech.com/product/pam-cas.zip>.
4. (Optionally, for SSO integrations) **restore** the keystore `.jks` and `.xml` metadata files for CAS version 5.2 to `$PAM_HOME/content/keys/` from the backup location or regenerate them.
5. Execute the following command to **switch** PAM configuration to version CAS 5.2:

For Windows deployments:

```
1 | bin\PamDirectory.cmd SwitchCASVersion web 52
```

For Unix or Linux deployments:

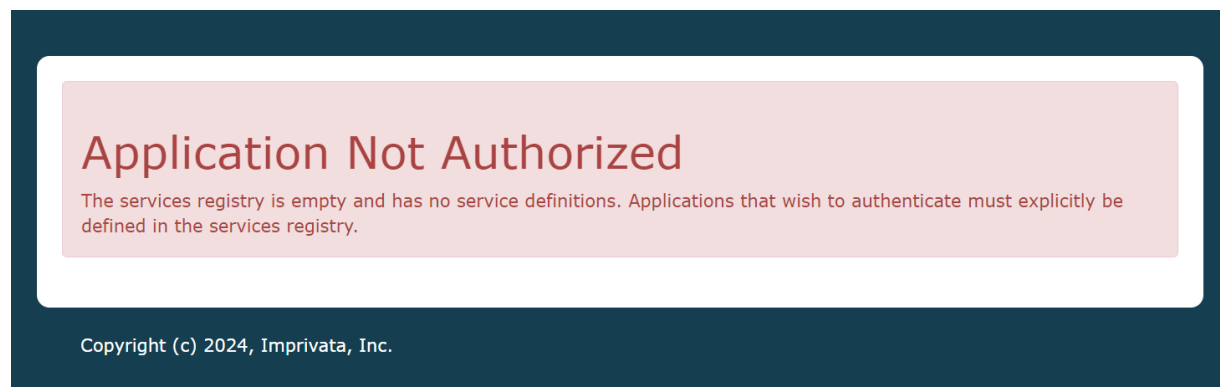
```
1 | bin/PamDirectory.sh SwitchCASVersion web 52
```

6. Start the **PamManagement** (Windows) or the **pammanager** (Linux) service.

## Troubleshooting

Federated Sign-in module version 6.5 Troubleshooting.

### *Application not Authorized* error message



1. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor. In this file, locate the section that begins with `#CAS` and change the following parameter set it to **true**:

```
1 | cas.serviceRegistry.initFromJson=true
```

2. Restart the **PamManagement** (Windows) or the **pammanager** (Linux) service.
3. Once PAM is working and you can see the usual CAS login page, back to the file `$PAM_HOME/web/conf/catalina.properties` in a text editor. Find the section that begins with `#CAS` and change `cas.serviceRegistry.initFromJson` parameter back to **false**:

```
1 | cas.serviceRegistry.initFromJson=false
```

4. Restart the **PamManagement** (Windows) or the **pammanager** (Linux) service.

## FAQs

We understand that upcoming changes to our PAM solution may raise questions, and we want to ensure you have all the information you need. This section is designed to help you better understand the enhancements we're making, how they benefit you, and what steps you might need to take. By providing clear answers to common questions, we aim to make the transition as smooth as possible and have representation about 'Why

*These Changes Are Better for Our Customers’*. We encourage you to read through these FAQs, and as always, feel free to reach out to us if you have any further inquiries. If questions remain or issues arise while using PAM, please contact the Support team: <https://support.imprivata.com/communitylogin>.

**Question:** *What are the high-level benefits we will gain from the upgrade?*

**Answer:** Upgrading to the latest version of PAM provides you with enhanced security, improved performance, and access to all the newest features and enhancements we offer. To fully benefit from these improvements and ensure optimal compatibility, we encourage you to update your Java environment to at least the minimum supported version.

**Question:** *Why is future support for federated sign-in in PAM limited to Federated Sign-in version 6.5?*

**Answer:** The third-party vendor we rely on for federated sign-in, has discontinued support for version 5.2. As a result, any future enhancements to the PAM authentication module will be compatible only with Federated Sign-in v6.5. This is a crucial change that needs to be addressed to maintain the security and functionality of your federated sign-in process.

**Question:** *Are there any risks in migrating to version 6.5 that should be mitigated?*

**Answer:** There are no risks in migrating PAM functionalities as all features will be available. However, while updating, the federated plugin in v6.5 can impact your [SAML integration](#), specifically regarding keystores and metadata files. Tokens generated with older versions will not work after the migration, so you must generate new ones as instructed in the guide.

## Federated Sign-In: Certificate Errors

When configuring the PAM [Federated Sign-In](#) module and using a self-signed SSL certificate, you may receive the below errors.

### **PKIX path building failed ... unable to find valid certification path to requested target**

The reason for this is that the PAM WEB application does not trust the [Federated Sign-In](#) module because the PAM farm is setup to use a self-signed SSL certificate (either individually self-signed or signed by the client’s certificate authority).

The easiest solution for this is to setup PAM with a SSL certificate signed by the well known internet certificate authority known to PAM WEB Container.

Alternatively, a self-signed certificate should be [imported into the PAM key store](#) so that PAM will trust [Federated Sign-In](#) module operating under this certificate.

## Federated Sign-In Module Timeout Errors

PAM Federated Sign-In Module – Timeout, Connection Forbidden or 403 Errors.

After deploying the PAM [Federated Sign-In](#) module (FSM), you may receive generic Timeout or 403 errors in your browser or log files if it was not properly configured.

We assume that after adding the [Federated Sign-In](#) you can login to it successfully but then the PAM page does not appear. Instead, these generic exceptions appear in the log or in your browser.

After authentication by the [Federated Sign-In](#) it generates a ticket and redirects the browser to the PAM WEB Application. The WEB Application then takes this ticket and validates it with the same FSM before generating the page.

To accomplish this the PAM WEB Application, from the computer it is installed, connects to a URL at **https://company.com/cas** (with the ticket to validate and its own URL as parameter).

The error indicates that this call fails. The important event here is that it is not the browser from your workstation that makes this call but PAM WEB app from the computer where PAM is installed.

First, to validate tickets with the FSM, PAM should know it's a load balancer URL.

This value is defined using the following parameters in the `$PAM_HOME/web/conf/catalina.properties` file:

```
1 | cas.managed.path=https://company.com
2 | cas.server.name=https://company.com
3 | cas.server.prefix=https://company.com/cas
```

Check these parameters to ensure they are accurate for your deployment. If they are not, please modify them as required and when finished, save the file then restart the **PamManagement** (Windows) or **pammanager** (Linux/Unix) service to complete the configuration.

Based on our experience with other users, we have found that configurations that may cause this behavior are the following:

- DNS on the PAM computer works differently and does not resolve `cas.managed.path` to the computer where the load balancer resides. For example, there is a host record making it a localhost. We recommend pinging the load balancer to see how it resolves.
- Routing behind the load balancer is configured in such a manner that it does not route traffic from inside the farm to the load balancer front end. For example, it short cuts it back to the localhost again to a non-SSL connection or the traffic from inside the farm comes to the wrong interface of the server with reverse proxy where the load balancer does not listen.
- The load balancer does not process requests that came from inside the farm in the right way like it processes requests from the outside.

## Encrypting Properties of Federated Sign-In Module

In some cases, it is required to encrypt sensitive properties of Federated Sign-In module in `$PAM_HOME/web/conf/catalina.properties` file (properties started with `cas.` prefix).

An example of such properties includes Radius Server Secret or password for SAML IdP integrations.

To do that open the command line prompt on the computer where PAM is installed, change the directory to `$PAM_HOME` folder and execute the following command:

Windows:

```
1 | bin\PamDirectory.cmd GenerateCASCipher web -
```

Unix:

```
1 | bin/PamDirectory.sh GenerateCASCipher web -
```

It is also possible to type the actual password to encrypt instead of the dash at the end (escape special characters in the command line as required) or use dash so this command will prompt for the password to encrypt.

After that, the command will print the encrypted password to the screen.

Use this output for the password parameter *prefixed* with the **{cipher}** like in the example below:

**cas.authn.radius.client.sharedSecret={cipher}ENCRYPTED**

There is one more step to make this all work.

Federated Sign-In Module (CAS) does not decrypt properties defined in the `catalina.properties` file.

All properties that have to be decrypted should be moved out to the external file that CAS will process through its loading mechanism.

To do that, create a file `$PAM_HOME/web/conf/cas.properties` and move there all encrypted properties.

Note that this `cas.properties` file might contain both encrypted and plain text properties.

For the reasons of consistency, the related properties could be grouped together in this file.

Remove or comment on these properties in `catalina.properties` file so that they would not duplicate.

After that, make a reference to this place by adding the following property into `catalina.properties` file:

**cas.standalone.config=\${catalina.base}/conf**

Restart **PamManagement** (Windows) / **pammanager** (Linux/Unix) service for this configuration to reload.

## Integrations

### Active Directory

#### Active Directory Integration

To integrate your Active Directory with PAM, you may configure your settings during or after installation.

PAM does not have any limitation on the version or functional level of Active Directory. It is recommended to use a version that uses TLS 1.2.

If you are looking to integrate with additional AD or LDAP domains, please review our [Multi-domain Configuration](#) article.

If you are looking to integrate with NetIQ eDirectory, please review our [NetIQ eDirectory Integration](#) article.

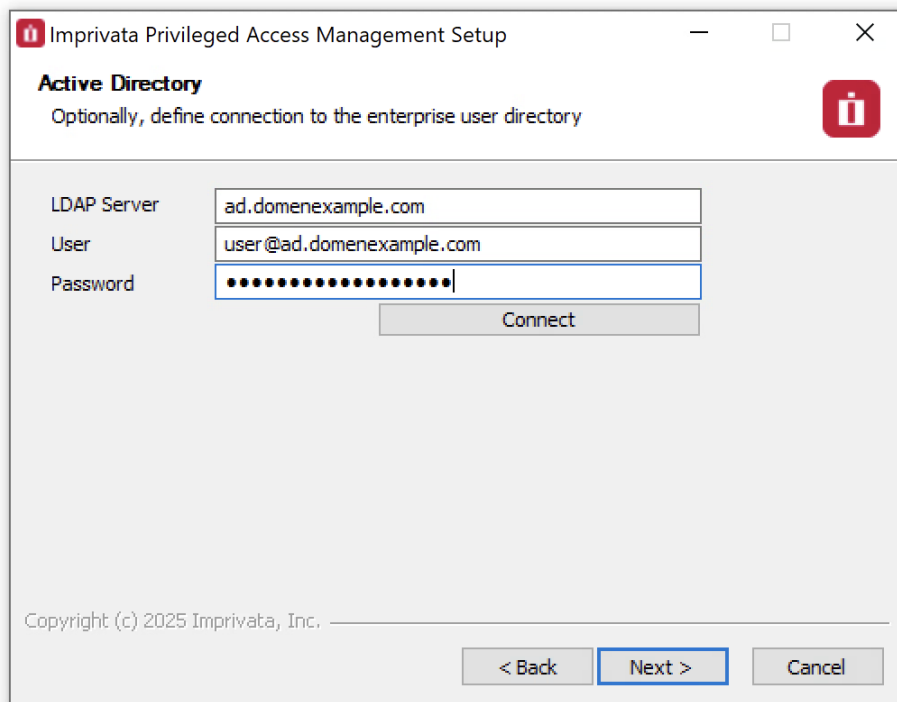
We recommend using an Active Directory account whose password does not change. If the password of this account does change, PAM's integration with your Active Directory will no longer work resulting in AD users being unable to login to PAM. If your AD integration account password does change, then you can follow the procedure outlined in the section *To configure or update an Active Directory binding After Installation* on this page to update PAM with your new password.

## *Active Directory binding During Installation*

To configure an Active Directory binding During Installation:

1. When the installation wizard reaches the section named Active Directory enter the following values:
  - a. **LDAP Server:** Enter the host name or IP address of your Active Directory Domain Controller.
  - b. **User:** Enter the user name of the account that can connect to this server.
  - c. **Password:** Enter the password of this user.
2. Click the **Connect** button to test your connection.
3. If the test connection was successful, click the **Next** button to continue. If the test connection failed,

check your values and try again.



## Active Directory binding After Installation

To configure or update an Active Directory binding **After Installation**:

(June 4, 2018) – If you have updated to PAM version 2.3.201806032154 or later, you can now configure Active Directory integration by simply navigating to Administration > Settings > AD within the PAM interface.

1. **Login** to the server where PAM is deployed as an Administrator.
2. Open a command line and navigate to the folder where PAM is installed (\$PAM\_HOME) and issue the following command:

- for Windows, substitute your **ldap.server**, **ldap.user** and **ldap.password** values and issue:

```
1 | bin\PamDirectory.cmd ADConnect web ldap.server ldap.user ldap.password
```

- for Unix or Linux, substitute your **ldap.server**, **ldap.user** and **ldap.password** values and issue:

```
1 | bin/PamDirectory.sh ADConnect web ldap.server ldap.user ldap.password
```



Please note if your password contains any of the following characters & \ < > ^ | then they must be properly escaped when executing the command by placing a ^ before each like this for ampersand ^&. Alternatively, you can issue the command using a dash – rather than the password in which case you will be prompted to enter the password during execution and in this approach, those special characters do not have to be escaped.

3. If the command returns an *OK* response, then restart the PamManagement (Windows) or pammanager (Linux) service on this computer:

- for Windows:

```
1 | net stop PamManagement
2 | net start PamManagement
```

- for Unix or Linux:

```
1 | service pammanager restart
```

4. If the command returns a *Fail* response, then double check your user and password values. For the {ldap.user} value, be sure to use the **user@domain** format.

5. Active Directory integration is now complete. Objects and permissions may now be shared with AD Users and Groups in PAM.

To support [self-password reset in PAM for your AD users](#), you must configure your AD integration using LDAPS and the defined LDAP binding account must be able to reset the password of other users in this Active Directory

## Multiple Domain Configuration

Configuring PAM to enable Logins from Multiple Domains.

PAM supports the ability to integrate with multiple domains (AD and LDAP) in order to provide login and authentication services for the application.

If you have not integrated with AD yet, please first review our [AD Integration](#) article first.

### *AD or LDAP connections*

To configure additional AD or LDAP connections in PAM:

1. Login to the server where PAM is deployed as an Administrator.
2. Open a command line and navigate to the folder where PAM is installed (`$PAM_HOME`) and issue the following command:
  - i. For Windows, substitute the below placeholders with your connection information and then issue the command:

- {ldap.name} which is used by PAM as an internal reference.
- {ldap.server} which is your server name.
- {ldap.user} which is your ldap user. Use the format **user@domain.com**
- {ldap.password} which is the password for your user.

```
1 | bin\PamDirectory.cmd LdapConnect web {ldap.name} {ldap.server}
  | {ldap.user} {ldap.password}
```

ii. For Unix or Linux, substitute the below placeholders with your connection information and then issue the command:

- **{ldap.name}** which is used by PAM as an internal reference.
- **{ldap.server}** which is your server name.
- **{ldap.user}** which is your ldap user. Use the format **user@domain.com**
- **{ldap.password}** which is the password for your user.

```
1 | bin/PamDirectory.sh LdapConnect web {ldap.name} {ldap.server}
  | {ldap.user} {ldap.password}
```

Please note if your password contains any of the following characters & \ < > ^ | then they must be properly escaped when executing the command by placing a ^ before each like this for ampersand ^&. Alternatively, you can issue the command using a dash – rather than the password in which case you will be prompted to enter the password during execution and in this approach, those special characters do not have to be escaped.

```
1 | bin\PamDirectory.cmd LdapConnect web {ldap.name} {ldap.server} {ldap.user} -
```

```
1 | bin/PamDirectory.sh LdapConnect web {ldap.name} {ldap.server} {ldap.user} -
```

3. If the command returns an OK response, then the connection has been made. You may add another connection following this same procedure. If the command returns a Fail response, then double check your user and password values. For the {ldap.user} value, be sure to use the user@domain format.
4. Once all the connections have been created successfully, please restart the service by issuing the following command:

a. For Windows:

```
1 | net stop PamManagement
2 | net start PamManagement
```

b. For Unix or Linux:

```
1 | service pammanager restart
```

5. Multi-domain AD or LDAP integration is now complete. Objects and permissions may now be shared with these additional AD Users and Groups in PAM.

AD/LDAP user accounts can be added to PAM Local Groups which helps provide a single group that contains membership of multiple domain accounts.

## Disabling

To Disable an Existing Connection:

1. Login to the server where PAM is deployed as an Administrator.
2. Open a command line and navigate to the folder where PAM is installed (`$PAM_HOME`) and issue the following command:
  - a. For Windows, substitute your `{ldap.name}` which was supplied when creating the initial connection and issue:

```
1 | bin\PamDirectory.cmd LdapConnect web {ldap.name} DISABLE
```

- b. For Unix or Linux, substitute your `{ldap.name}` which was supplied when creating the initial connection and issue:

```
1 | bin/PamDirectory.sh LdapConnect web {ldap.name} DISABLE
```

3. When successfully disabled, the command will return an *OK* response.

## Troubleshooting

[Unable to Connect to AD services due to a PKIX Path Building Failure when configuring multiple AD servers behind a Load Balancer](#)

## Multi Domain Forests with AD Trust Configuration

PAM supports the ability to integrate with multiple domains, taking advantage of AD trusts, in order to provide login and authentication services for the application.

This means a single AD integration point will allow multi-domain logins using existing trusts within Active Directory.

Default PAM deployments are configured for both administration and user ease of use.

For this purpose, it starts with using single domain configuration using `sAMAccountName` logins (user).

However, larger or more complex AD structures exist including multi-domain forests with AD trusts. In order to support these configuration, PAM can be configured to support these domains using UserPrincipalNames (user@company.com).

If you have not integrated with AD yet, please first review our [AD Integration article](#) first.

## Integration for UPN Accounts

To configure integration for UPN Accounts:

1. Login to your PAM host server. We will need to modify two files, so make sure you have permissions on this host server to update files.
2. First, open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor.
3. Within the `catalina.properties` file, search for and replace the 2 references and their values to `sAMAccountName` with `UserPrincipalName`

Before:

```
1 | ldap.authn.searchFilter=sAMAccountName={user}
2 | cas.authn.ldap[1].userFilter=(sAMAccountName={user})
```

After:

```
1 | ldap.authn.searchFilter=UserPrincipalName={0}
2 | cas.authn.ldap[1].userFilter=(UserPrincipalName={user})
```

4. Also within this `catalina.properties` file, search for and update this parameter `cas.authn.ldap[1].dnFormat` as illustrated below:

Before:

```
1 | cas.authn.ldap[1].dnFormat=%s@yourDomain.com
```

After:

```
1 | cas.authn.ldap[1].dnFormat=%s
```

5. After both are replaced, save and close the file.
6. Finally, restart the **PamManagement** (Windows) or **pammanger** (Linux) service.

If you have already granted Permissions in PAM using `sAMAccountName`, those logins will no longer work after these changes have been made. Permissions will need to be setup again using the UPN (`user@company.com`) rather than the previously used `sAMAccountName` (user).

In multi-domain cases we recommend to architect PAM deployment to use *UserPrincipalName* (UPN) as a primary user ID. This way, one user can login as *user@domainA.com*, the other user as *user@domainB.com* and local user as *user*. Duo should be configured accordingly keeping in mind that *user@domainA.com*, *user@domainB.com* and / or user from local directory in common case might be three completely different users.

## Secure Connectivity to an Active Directory Domain Controller

PAM use of Secure Connectivity to Active Directory Domain Controller.

Through Microsoft's requirements, password rotation in Active Directory has to be done using the LDAPS protocol, which implies that LDAP Server host is specified in the format **ldaps://dc-host.company.com:port format**.

Furthermore, it implies that the AD domain controller is configured using a trusted certificate to secure the communication link.

This trusted certificate has to be generated for the exact name (*dc-host.company.com*) used in the host property of the LDAP Server describing this AD domain controller; otherwise, the PAM password rotation routine will not trust the certificate and will fail to connect to the domain controller even with your valid Admin credentials.

In the case where your AD domain controller does not support LDAPS connectivity protected by the trusted certificate, PAM cannot rotate passwords for users in this domain controller.

In the case where your AD domain controller supports LDAPS connectivity but the certificate is not signed by trusted internet authorities so that PAM does not trust it out of the box, PAM will attempt to import this certificate automatically into its key store during first connection attempt.

At this time, the first connection attempt might fail while consequent connections might succeed because the certificate will be automatically imported into the PAM key store.

In the case where your domain controller certificate does not include the host name used in the AD host connection string **ldaps://dc-host.company.com:port**, PAM will fail to trust the certificate even it is imported successfully to PAM key store.

In this case, the only resolution to this issue is to align the name on the certificate with the name of the AD domain controller host in the connection string.

One way to do it is to regenerate a certificate for AD and apply it to LDAPS connection in domain controller.

The other way is to create a host record in the OS hosting PAM for the domain controller to address it by the name on the certificate and then use this exact name in the AD connection string in LDAP Server record.

### Troubleshooting

To troubleshoot certificate issues and to force loading AD domain controller certificate into PAM key store in a supervised way, perform the following steps:

1. Login to PAM host as an PAM owner (Linux/Unix) or run command prompt as Administrator (Windows). Navigate to `$PAM_HOME` folder (such as `/opt/pam` or `c:\pam`). Do not navigate to the `bin` subfolder of `$PAM_HOME` folder.

2. Execute the following command where

**dc-host.company.com** is the host name of the Active Directory domain controller

**port** is the LDAPS port of the Active Directory domain controller like **636** or **3269**

For Linux:

```
1 | bin/PamDirectory.sh SSLImport dc-host.company.com port
```

For Windows:

```
1 | bin\PamDirectory.cmd SSLImport dc-host.company.com port
```

The command will either complete with success indicating that PAM trusts the Active Directory domain controller certificate or it will print the certificate on the screen and prompt to import certificate to the PAM key store.

Note that it is possible that the command will print several certificates indicating some intermediate certificates are required to set up trust to the domain controller. Import all certificates into the PAM key store as prompted and repeat the procedure to confirm successful connection.

This command may also generate an error in case of name mismatch of the host in the parameter with the name on the certificate that break the trust.

This issue has to be resolved by using the name on the certificate to connect.

3. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service.

If the problem still persists, reboot PAM.

## AD Authentication is Slow

Active Directory User Authentication to the PAM is slow. What causes this and how can it be improved?

System caches AD group membership by user after their initial login for a period of one day because this is usually the slowest operation for validating permissions (the one that contributes to the slow initial load).

System cleans its cache after the user logouts or when an PAM System Administration presses **Reset Cache** button on the Administration > Settings > AD page.

There are several ways to optimize this initial query. All methods could be used simultaneously or just some of them depending on your requirements.

### *The first method*

The first method is to limit the user and group locations to some branch of the AD forest.

Often, AD forests include very slow trusts that could be eliminated by restricting queries to certain branches where all System applicable users and groups are located.

In a default installation, PAM attempts to use the whole tree because it does not know where users and groups are coming from; however, it is possible to limit the branch for your production use.

To do this, use the following parameters in `$SPAM_HOME/web/conf/catalina.properties` file to define certain org units or other branches of the forest:

```
ldap.rootDn=  
ldap.baseDn=  
ldap.roleBase=
```

For example, we can restrict queries to the following branch `CN=Users,DC=contoso,DC=com` as compared to the complete tree using only `DC=contoso,DC=com`.

```
# MS AD  
ldap.url=ldap://xton-dc001.xton.imp.eng:389  
ldap.rootDn=DC=xton,DC=imp,DC=eng  
ldap.baseDn=DC=xton,DC=imp,DC=eng  
ldap.managerDn=CN=Chris Kolodziejcki,CN=Users,DC=xton,DC=imp,DC=eng  
ldap.managerPassword={AES256},{CQm/+8lCbKw2d63tlyjjexTAIGg=},{6usyMsi(  
ldap.domain=xton.imp.eng  
#ldap.roleBase=DC=xton,DC=imp,DC=eng  
ldap.roleBase=OU=DemoOU01,DC=xton,DC=imp,DC=eng  
ldap.roleBase.1=OU=DemoOU02,DC=xton,DC=imp,DC=eng  
ldap.roleBase.2=OU=Demo OU 03,DC=xton,DC=imp,DC=eng  
ldap.roleBase.3=OU=DemoOUBase,DC=xton,DC=imp,DC=eng  
ldap.authn.searchFilter=sAMAccountName={0}  
ldap.roleName=cn  
ldap.roleSearch=(member:1.2.840.113556.1.4.1941:={0})  
ldap.groupSearch=(&(objectClass=group)(cn={0}))
```

Note: **ldap.roleBase** must remain as a valid parameter as it does in our default configuration today. Additional **ldap.roleBase** parameters can be added, each with an increasing value beginning with **.1**.

```
ldap.roleBase=  
ldap.roleBase.1=  
ldap.roleBase.2=  
ldap.roleBase.3=  
etc
```

## The second method

The second method is to not integrate directly with AD domain controller but rather with its AD Global Catalog which, when optimized, performs faster with complex queries.

The AD Global Catalog is usually accessible on the same domain controller for the forest over port 3268 or 3269 for LDAPS access.

## The third method

The third method is to change the way PAM queries group membership for any specific user.

By default, it does one recursive query to Active Directory that returns all nested groups a user belongs to. While some Domain Controllers are optimized well to execute queries like these, for some Active Directory servers this is very heavy operation.

In this case, it is more desirable for the AD client (like Privileged Access Management) to query groups one-by-one instead of relying on AD to execute a combined recursive query to return all groups. The switch is controlled by the parameter `ldap.roleSearch` in the `$PAM_HOME/web/conf/catalina.properties` file.

The following is the default value for this parameter (recursive query):

```
1 | ldap.roleSearch=(member:1.2.840.113556.1.4.1941:={0})
```

To further narrow the search to only groups that are mapped to PAM, add the following property to in the `$PAM_HOME/web/conf/catalina.properties` file and specify the group names that are associated in PAM. PAM will then ignore all other groups and should help improve the Login experience.

This is only available in PAM version Release 2.3.202503301554 (March 30, 2025) or later:

```
1 | ldap.pam.userGroupsList=(&(objectClass=group)(|(cn=group-001New)(cn=group-002New))(member:1.2.840.113556.1.4.1941:={0}))
```

To switch PAM to execute multiple queries for nested groups, change the parameter to this:

```
1 | ldap.roleSearch=(member={0})
```

Afterwards, **save and close** the file and finally restart the **PamManagement** (Windows) or **pammanger** (Linux) service.

This parameter will instruct the System to execute a query to get all groups a user belongs to and then to execute the same query for each group returned to cover the case of nested AD groups.

We observed that some domain controllers perform faster using this method. Before doing this, you might want to test against your active directory server to determine which query is faster by using some common AD/LDAP query tool like `ldapsearch`, `Softerra`, `Apache Directory Studio`. Also, it is important to understand if your AD domain controller that can even execute queries like these before you make any changes.

## Integration with Active Directory in HA mode

To implement an alternative URL (Domain Controller) for [Active Directory](#), perform the following:

1. Open for edit `$PAM_HOME/web/conf/server.xml`. Find **PAM AD REALM** section there end add this property to **Realm** configuration: `alternateURL="${ldap.alt}"`

The updated realm specification will look like on the exhibition below:



```

1 <Realm
2     className="com.pam.config.JNDIRealmEncrypted"
3     debug="99"
4     connectionURL="${ldap.url}"
5     alternateURL="${ldap.alt}"
6     authentication="simple"
7     referrals="follow"
8     connectionName="${ldap.managerDn}"
9     connectionPassword="${ldap.managerPassword}"
10    userSearch="${ldap.authn.searchFilter}"
11    userBase="${ldap.baseDn}"
12    userSubtree="true"
13    roleSearch="${ldap.roleSearch}"
14    roleName="${ldap.roleName}"
15    roleSubtree="true"
16    roleBase="${ldap.roleBase}"
17 />

```

Result will be similar to this screenshot:

```

<!-- BEGIN: PAM AD REALM -->
    <Realm
        className="com.pam.config.JNDIRealmEncrypted"
        connectionURL="${ldap.url}"
        alternateURL="${ldap.alt}"
        authentication="simple"
        referrals="follow"
        connectionName="${ldap.managerDn}"
        connectionPassword="${ldap.managerPassword}"
        userSearch="${ldap.authn.searchFilter}"
        userBase="${ldap.baseDn}"
        userSubtree="true"
        roleSearch="${ldap.roleSearch}"
        roleName="${ldap.roleName}"
        roleSubtree="true"
        roleBase="${ldap.roleBase}"
    />
<!-- END: PAM AD REALM -->

```

2. Open `$PAM_HOME/web/conf/catalina.properties`. Search for **MS AD** configuration section and add the following line replacing **ALTERNATE-LDAP-URL** with your alternate AD URL:

ldap.alt=**ALTERNATE-LDAP-URL**

```
1 | ldap.alt=ldaps://dc2.somedomain.local:636
```

```
# MS AD
ldap.url=ldaps://dc1.                :636
ldap.alt=ldaps://dc2.                :636
ldap.rootDn=DC=                      ,DC=
ldap.baseDn=DC=                      ,DC=
ldap.managerDn=CN=svc_xtam_ad,OU=Service accounts,DC=          ,DC=
ldap.managerPassword={AES256},{w+xxjlbIYDwq6a+3BwpMyx+/enQ=},{LHXohnY29X
ldap.domain=
ldap.roleBase=DC=                    ,DC=
ldap.authn.searchFilter=sAMAccountName={0}
ldap.roleName=cn
ldap.roleSearch=(member:1.2.840.113556.1.4.1941:={0})
ldap.groupSearch=((&(objectClass=group)(cn={0}))
```

Search for `cas.authn.ldap[1]` properties group. For deployments using [Federated Sign-In](#) component list alternative [LDAP](#) URLs space separated in `cas.authn.ldap[1].ldapUrl`. This property accepts space separated list of domain controllers add necessary controllers there.

Edit parameter like in the example below:

```
1 | cas.authn.ldap[1].ldapUrl=ldaps://dc1.domain.local:636
2 | ldaps://dc2.domain.local:636
```

```
cas.authn.ldap[1].type=AD
cas.authn.ldap[1].ldapUrl=ldaps://dc1.                :636 ldaps://dc2.                :636
cas.authn.ldap[1].baseDn=DC=                      ,DC=
cas.authn.ldap[1].dnFormat=%s@                    ;
cas.authn.ldap[1].useSsl=false
cas.authn.ldap[1].useStartTls=false
cas.authn.ldap[1].connectTimeout=5000
cas.authn.ldap[1].userFilter=(sAMAccountName={user})
cas.authn.ldap[1].subtreeSearch=true
cas.authn.ldap[1].usePasswordPolicy=false
cas.authn.ldap[1].principalAttributeId=
cas.authn.ldap[1].principalAttributeList=
cas.authn.ldap[1].allowMultiplePrincipalAttributeValues=true
cas.authn.ldap[1].allowMissingPrincipalAttributeValue=true
```

3. Ensure that there are no trailing spaces in properties values. **Save and close** both files.
4. Import certificates from all domain controllers to PAM local java keystore on all PAM nodes using PAM CLI Utility `PamDirectory SSLImport` command. This can be done by issuing followed command from `($PAM_HOME)` location:

```
1 | bin/PamDirectory.sh sslimport dc1.somedomain.local 636
```

5. Restart **PamManagment** (`pammanager` for Linux).

`cas.authn.ldap` is for CAS authentication (forms based auth and sso).

# LDAP

## Configuring JumpCloud LDAP Integration

To integrate Jump Cloud's LDAP-as-a-Service with PAM you will need to perform the following procedure.

### *Pre-requisites*

- A JumpCloud account that this configured as an LDAP Binding User. Please reference this [JumpCloud article](#) for more information.
- A connection and account to login to the PAM host server to run commands, update configuration files and restart services.
- A JumpCloud account to test the integration.

### *JumpCloud LDAP Integration*

1. Login to JumpCloud to retrieve your LDAP Binding User and the required parameters to perform the integration. This includes the LDAP Binding Account (DN), LDAP Binding Account password and your JumpCloud OrgID. For additional information, please review this [JumpCloud article](#).
2. On the PAM host server, open a command prompt and navigate to \$PAM\_HOME
3. From the \$PAM\_HOME directory, execute the following command, replace the placeholders with your actual JumpCloud vaules.

- a. For Windows, substitute your <CONNECTION\_NAME>, <LDAP\_BINDING\_USER>, <YOUR\_ORG\_ID> and <LDAP\_BINDING\_USER\_PASSWORD> values and issue:

```
1 | bin\PamDirectory.cmd LdapConnect web <CONNECTION_NAME>
  | ldaps://ldap.jumpcloud.com:636 "uid=<LDAP_BINDING_USER>,ou=Users,o=<YOUR_ORG_ID>,dc=jumpcloud,dc=com" <LDAP_BINDING_USER_PASSWORD>
```

- b. For Unix or Linux, substitute your <CONNECTION\_NAME>, <LDAP\_BINDING\_USER>, <YOUR\_ORG\_ID> and <LDAP\_BINDING\_USER\_PASSWORD> values and issue:

```
1 | bin/pamdirectory.sh LdapConnect web <CONNECTION_NAME>
  | ldaps://ldap.jumpcloud.com:636 "uid=<LDAP_BINDING_USER>,ou=Users,o=<YOUR_ORG_ID>,dc=jumpcloud,dc=com" <LDAP_BINDING_USER_PASSWORD>
```

4. When the command executes successfully (it will return an **Ok** response), next open the \$PAM\_HOME/web/conf/catalina.properties file in a text editor. You will need to manually update a few parameters to complete the integration.
5. Locate the section of this file that is specific to your JumpCloud (it will probably be at the bottom). Update your parameters to match those from below.

```
1 | ldap.name=CONNECTION_NAME
2 | ldap.url=ldaps://ldap.jumpcloud.com:636
3 | ldap.rootDn=ou=Users,o=YOUR_ORG_ID,dc=jumpcloud,dc=com
4 | ldap.baseDn=ou=Users,o=YOUR_ORG_ID,dc=jumpcloud,dc=com
5 | ldap.managerDn=uid=LDAP_BINDING_USER,ou=Users,o=YOUR_ORG_ID,dc=jumpcloud,dc=com
```

```

6 ldap.managerPassword=LDAP_BINDING_USER_PASSWORD
7 ldap.domain=jumpcloud.com
8 ldap.roleBase=o=YOUR_ORG_ID,dc=jumpcloud,dc=com
9 #ldap.authn.searchFilter=uid={0} (Uncomment this line (remove #) if you want
  to login using UID)
10 #ldap.authn.searchFilter=mail={0} (Uncomment this line (remove #) if you
   want to login using Email Address)
11 ldap.roleName=cn
12 ldap.roleSearch=(member={0})
13 ldap.groupSearch=(&(cn={0})(objectClass=groupOfNames))

```

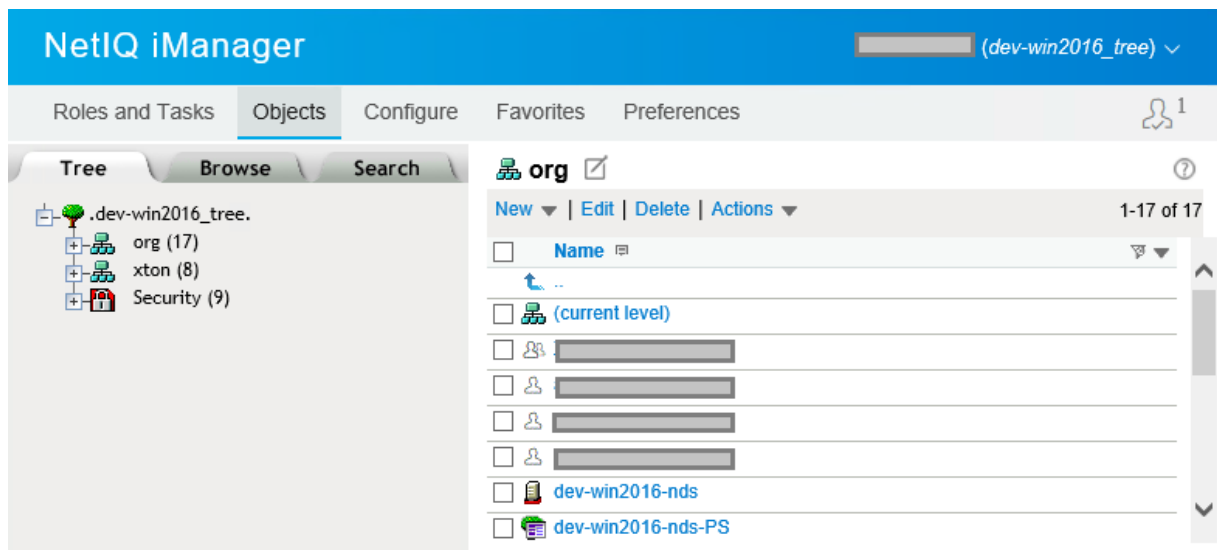
6. After the updates have been made, save and close the file.
7. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service to complete the integration.
8. When the service comes back online (2-5 minutes), test your login using a JumpCloud account.

## Configuring NetIQ eDirectory Integration

Configuring PAM to enable Logins from NetIQ eDirectory.

PAM supports the ability to integrate with NetIQ eDirectory (formerly Novell Directory Services (NDS) or NetWare Directory Services) in order to provide login and authentication services for the application.

If you are looking for Active Directory integration, please see this [Active Directory Integration](#) article.



### Configuring NetIQ eDirectory connections

To configure NetIQ eDirectory connections in PAM:

If you are using eDirectory as your only Directory Service for PAM, skip the AD Integration option during installation.

The following eDirectory integration process is performed post installation only.

1. Login to the server where PAM is deployed as an Administrator.
2. Open a command line and navigate to the folder where PAM is installed (\$PAM\_HOME) and issue the following command:

- a. For Windows, substitute the below placeholders with your connection information and then issue the command:

- **{ldap.name}** which is used by PAM as an internal reference.
- **{ldap.server}** which is your server name. For example, ldaps://host:636
- **{ldap.user}** which is your ldap user. For example, cn=admin,o=org
- **{ldap.password}** which is the password for your user.

```
1 | bin\PamDirectory.cmd LdapConnect web {ldap.name} {ldap.server}
   {ldap.user} {ldap.password}
```

- b. For Unix or Linux, substitute the below placeholders with your connection information and then issue the command:

- **{ldap.name}** which is used by PAM as an internal reference
- **{ldap.server}** which is your server name. For example, ldaps://host:636
- **{ldap.user}** which is your ldap user. For example, cn=admin,o=org
- **{ldap.password}** which is the password for your user.

```
1 | bin/PamDirectory.sh LdapConnect web {ldap.name} {ldap.server}
   {ldap.user} {ldap.password}
```

Please note if your password contains any of the following characters & \ < > ^ | then they must be properly escaped when executing the command by placing a ^ before each like this for ampersand ^&. Alternatively, you can issue the command using a dash – rather than the password in which case you will be prompted to enter the password during execution and in this approach, those special characters do not have to be escaped.

```
1 | bin\PamDirectory.cmd LdapConnect web {ldap.name} {ldap.server} {ldap.user} -
```

```
1 | bin/PamDirectory.sh LdapConnect web {ldap.name} {ldap.server} {ldap.user} -
```

3. If the command returns an *OK* response, then the connection has been made. You may add another connection following this same procedure. If the command returns a *Fail* response, then double check your user and password values.
4. Once all the connections have been created successfully, please restart the service by issuing the following command:

- a. For Windows:

```
1 | net stop PamManagement
2 | net start PamManagement
```

- b. For Unix or Linux:

```
1 | service pammanager restart
```

5. NetIQ eDirectory integration is now complete.

## *Disabling an Existing Connection*

1. Login to the server where PAM is deployed as an Administrator.
2. Open a command line and navigate to the folder where PAM is installed (\$PAM\_HOME) and issue the following command:
  - a. For Windows, substitute your **{ldap.name}** which was supplied when creating the initial connection and issue:

```
1 | bin\PamDirectory.cmd LdapConnect web {ldap.name} DISABLE
```

- b. For Unix or Linux, substitute your {ldap.name} which was supplied when creating the initial connection and issue:

```
1 | bin/PamDirectory.sh LdapConnect web {ldap.name} DISABLE
```

- c. When successfully disabled, the command will return an **OK** response.

## Azure and ADFS

### Azure (Office 365) SSO SAML Integration

A cloud-hosted Azure Active Directory is a service provided by Microsoft that can provide a single sign-on using your Active Directory credentials. PAM supports integration with single sign-on (SSO) logins through a SAML 2.0 identity provider (IDP) like those of Azure AD (AAD) to provide authentication services.

### *Requirements*

Before you begin to integrate PAM with your AAD using SAML, be sure you met the following pre-requisites:

- A working PAM deployment with the [Federated Sign-In](#) experience. The PAM Federated Sign-In module provides the required SAML 2.0 web login functionality.
- A working PAM deployment with [Active Directory integration](#). This Active Directory integration provides the security for users and groups in PAM after they are authenticated via AAD.
- Access to your existing PAM host server. You will need to update a configuration file, certificates and restart services.
- The required Azure subscription plan and an account with access to create and configure *Non-gallery* applications in Azure Active Directory.

### *Step 1: Create and Configure your Azure AD Enterprise Application*

This step describes the process required to create and begin the configuration of your Azure Enterprise Application.

1. Login to your Azure Management Portal and navigate to Azure Active Directory > Enterprise Applications and click on the **Create your own application** button.

2. Enter a new name for your application select *Integrate any other application you don't find in the gallery (Non-gallery)* and click the **Create** button.

Home > XTON Tech > Browse Azure AD Gallery

**Browse Azure AD Gallery** ...

[+ Create your own application](#) [Got feedback?](#)

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Azure AD Gallery, described in [this article](#).

Search application

Single Sign-on : All User Account Management : All Categories : All

**Cloud platforms**

Amazon Web Services (AWS)

Google Cloud Platform

Oracle

**On-premises applications**

**Add an on-premises application**  
Configure Azure AD Application Proxy to enable secure remote access.

**Learn about Application Proxy**  
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

**Create your own application** ✕

[Got feedback?](#)

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

**What's the name of your app?**

ipam-app ✓

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises application

☐ Register an application to integrate with Azure AD (App you're developing)

☒ Integrate any other application you don't find in the gallery (Non-gallery)

**Create**

3. Once your app is created, navigate *Set up single sign-on* menu and click the **SAML** tile.

Home > XTON Tech > Browse Azure AD Gallery >

**ipam-app** | Overview ...

Enterprise Application

Overview

Deployment Plan

**Manage**

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes (preview)

**Security**

Conditional Access

Permissions

Token encryption

**Activity**

View logs

**Properties**

**Name** ⓘ

ipam-app ⓘ

**Application ID** ⓘ

df7e23ec-86d8-4d64-811c-... ⓘ

**Object ID** ⓘ

102f8303-f00d-4809-9e19-... ⓘ

**Getting Started**

**1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)

**2. Set up single sign on**  
Enable users to sign into their application using their Azure AD credentials  
[Get started](#)

**3. Provision User Accounts**  
Automatically create and delete user accounts in the application  
[Get started](#)

**4. Conditional Access**  
Secure access to this application with a customizable access policy.  
[Create a policy](#)

**5. Self service**  
Enable users to request access to the application using their Azure AD credentials  
[Get started](#)

Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more.](#)

Select a single sign-on method [Help me decide](#)



#### Disabled

Single sign-on is not enabled. The user won't be able to launch the app from My Apps.



#### SAML

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.



#### Password-based

Password storage and replay using a web browser extension or mobile app.



#### Linked

Link to an application in My Apps and/or Office 365 application launcher.

4. Now we will begin the first part of this app's **SAML configuration**. In the Basic SAML Configuration section, click the **Edit** button (pencil icon) and populate the following parameters:
- Identifier (Entity ID) (Required)** – Enter your PAM host name like `https://xtam.company.com`
  - Reply URL (Assertion Consumer Service URL) (Required)** – Enter your PAM host name plus `/cas/login?client_name=AzureSSO`. For example, `https://xtam.company.com/cas/login?client_name=AzureSSO`
  - Sign On URL (Optional)** – Enter your PAM login page like `https://xtam.company.com/xtam`
  - Relay State (Optional)** – Enter your PAM login page like `https://xtam.company.com/xtam`
  - Logout URL (Optional)** – leave empty

1

#### Basic SAML Configuration

Identifier (Entity ID)	<code>https://xtam.company.com</code>
Reply URL (Assertion Consumer Service URL)	<code>https://xtam.company.com/cas/login?client_name=AzureADSSO</code>
Sign on URL	<code>https://xtam.company.com/xtam</code>
Relay State	<code>https://xtam.company.com/xtam</code>
Logout Url	<i>Optional</i>

Please do not logout of your Azure Management Portal yet. We will return to this Enterprise Application later to complete the required configuration.

## Step 2: Begin Configuration of PAM

This step describes the process required to modify PAM configuration in order to identify your Azure Enterprise Application.

- Login to the PAM server and open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor.
- Locate the section labeled `# CAS` and add or update the following lines replacing `{cas.managed.path}` with your PAM host server like `https://xtam.company.com`:



```
1 | cas.managed.path={cas.managed.path}
2 | cas.server.name={cas.managed.path}
3 | cas.server.prefix={cas.managed.path}/cas
```

3. Below this # CAS section, create a new section with the following lines:

```
1 | # Azure SSO SAML
2 | cas.authn.pac4j.saml[0].clientName=AzureSSO
3 | cas.authn.pac4j.saml[0].keystorePassword=password
4 | cas.authn.pac4j.saml[0].privateKeyPassword=keystorePassword
5 | cas.authn.pac4j.saml[0].serviceProviderEntityId=https://xtam.company.com/xtam/
6 | cas.authn.pac4j.saml
  | [0].serviceProviderMetadataPath=c:/xtam/content/keys/azuresso.xml
7 | cas.authn.pac4j.saml
  | [0].keystorePath=c:/xtam/content/keys/samlKeystoreAzureSSO.jks
8 | cas.authn.pac4j.saml
  | [0].identityProviderMetadataPath=https://login.microsoftonline.com/yourAzureDi
  | rectoryID/federationmetadata/2007-
  | 06/federationmetadata.xml?appid=yourAzureEnterpriseApplicationID
9 | cas.authn.pac4j.saml[0].maximumAuthenticationLifetime=2073600
```

- a. cas.authn.pac4j.saml[0].clientName: This parameter will define the button name on the PAM login page for this SAML authentication. We recommend not including spaces in this value.
- b. cas.authn.pac4j.saml[0].keystorePassword: Define an alpha-numeric password.
- c. cas.authn.pac4j.saml[0].privateKeyPassword: Define the same alpha-numeric password as the keystorePassword.
- d. cas.authn.pac4j.saml[0].serviceProviderEntityId: Enter the exact value from your Azure Enterprise Application's Identifier (Entity ID) as configured in step 1.
- e. cas.authn.pac4j.saml[0].serviceProviderMetadataPath: Define an PAM path and name that will be used for the Federated Metadata `xml` file. We recommend storing this file in the `$PAM_HOME/content/keys` for example `c:/pam/content/keys/azuresso.xml` (Windows) or `/opt/pam/content/keys/azuresso.xml` (Linux).

For users who installed and use PAM before 2021, the PAM root folder has the name `xtam`, so `$PAM_HOME` path will be for example `c:/xtam/content/keys/azuresso.xml` (Windows) or `/opt/xtam/content/keys/azuresso.xml` (Linux).

- f. cas.authn.pac4j.saml[0].keystorePath Define an PAM path and name for the PAM keystore file (.jks). We recommend storing this file in the `$PAM_HOME/content/keys` for example `c:/pam/content/keys/samlKeystoreAzureSSO.jks` (Windows) or `/opt/pam/content/keys/samlKeystoreAzureSSO.jks` (Linux) \*or `c:/xtam/content/keys/samlKeystoreAzureSSO.jks` (Windows) or `/opt/xtam/content/keys/samlKeystoreAzureSSO.jks` (Linux) for the long time users.
- g. cas.authn.pac4j.saml[0].identityProviderMetadataPath: Enter the entire URL from your Azure Enterprise Application's App Federation Metadata URL. The URL should resemble this format: `https://login.microsoftonline.com/yourAzureDirectoryID/federationmetadata/2007-06/federationmetadata.xml?appid=yourAzureEnterpriseApplicationID`

- h. `cas.authn.pac4j.saml[0].maximumAuthenticationLifetime=2073600`: This value defines a 24 day period (value in seconds) in which a user has generated a last authentication event in Azure Active Directory. This parameter helps if users begin experiencing login issues due to old Azure authentication events.

```
# CAS
cas.managed.path=https://xtam.company.com
cas.server.name=https://xtam.company.com
cas.server.prefix=https://xtam.company.com/cas

# Azure SSO SAML
cas.authn.pac4j.saml[0].clientName=AzureSSO
cas.authn.pac4j.saml[0].keystorePassword=MyPassword1256
cas.authn.pac4j.saml[0].privateKeyPassword=MyPassword1256
cas.authn.pac4j.saml[0].serviceProviderEntityId=https://xtam.company.com
cas.authn.pac4j.saml[0].serviceProviderMetadataPath=C:/xtam/content/keys/azuresso.xml
cas.authn.pac4j.saml[0].keystorePath=C:/xtam/content/keys/samlKeystoreAzureSSO.jks
cas.authn.pac4j.saml[0].identityProviderMetadataPath=https://login.microsoftonline.com/5688bf52-f7dc-48b4-8
cas.authn.pac4j.saml[0].maximumAuthenticationLifetime=2073600

xtam.saml.upn.adjust=true
```

Please note, if PAM is configured to accept *sAMAccountName* logins as opposed to UserPrincipalName (UPN), then you will need to also add this line to this configuration file: **`xtam.saml.upn.adjust=true`**. Otherwise, when PAM is configured for UPN, you do not have to include this line or if you do, set it to false.

If you want to force a login every time for your users, you can add the following line to this configuration file:

```
1 | cas.authn.pac4j.saml[0].forceAuth=true
```

For Federated Sign In using PAM installation with **CAS.V.6.x** version:

open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor, locate parameter to the section labeled `# CAS`, and add or update the following line:

```
1 | cas.authn.pac4j.saml[0].useNameQualifier=false
```

4. Save and close this `catalina.properties` file.
5. Restart the **PamManagement** service (Windows) or **pammanager** service (Linux) and wait 2-5 minutes for the service to come back online.
6. To check your work thus far, open your web browser and navigate to the PAM login page. If you see a red button labelled **AzureSSO** at the bottom right, please proceed to the next step. If you do not, please double check your configuration in the previous steps and restart the PAM service once more.

Log in to Imprivata Privileged Access Management

Username:

Password:

LOGIN

[Forgot your password?](#)

For security reasons, please [log out](#) and exit your web browser when you are done accessing services that require authentication!

Links to Additional Resources

[Documentation](#)

[Contact Imprivata Support](#)

Or login with:

Okta

AzureSSO

Copyright (c) 2021, Imprivata, Inc.

### Step 3: Test the Integration

This final step is used to test the integration between PAM and your Azure Active Directory Enterprise Application.

1. Open a new browser session (private or incognito) and navigate to the Imprivata Privileged Access Management login page.
2. Located on the bottom right of this login page, you should see a new red button labeled **AzureSSO** or whatever value you entered for the client name earlier.

Log in to Imprivata Privileged Access Management

Username:

Password:

LOGIN

[Forgot your password?](#)

For security reasons, please [log out](#) and exit your web browser when you are done accessing services that require authentication!

Links to Additional Resources

[Documentation](#)

[Contact Imprivata Support](#)

Or login with:

Okta

AzureSSO

Copyright (c) 2021, Imprivata, Inc.

3. To test the integration, the following is expected:

- When you click this red **AzureSSO** button, you will be redirected to the Microsoft Login page.
- You will enter your Azure Active Directory username that has been giving access to the Enterprise Application earlier and click **Next**.



## Sign in

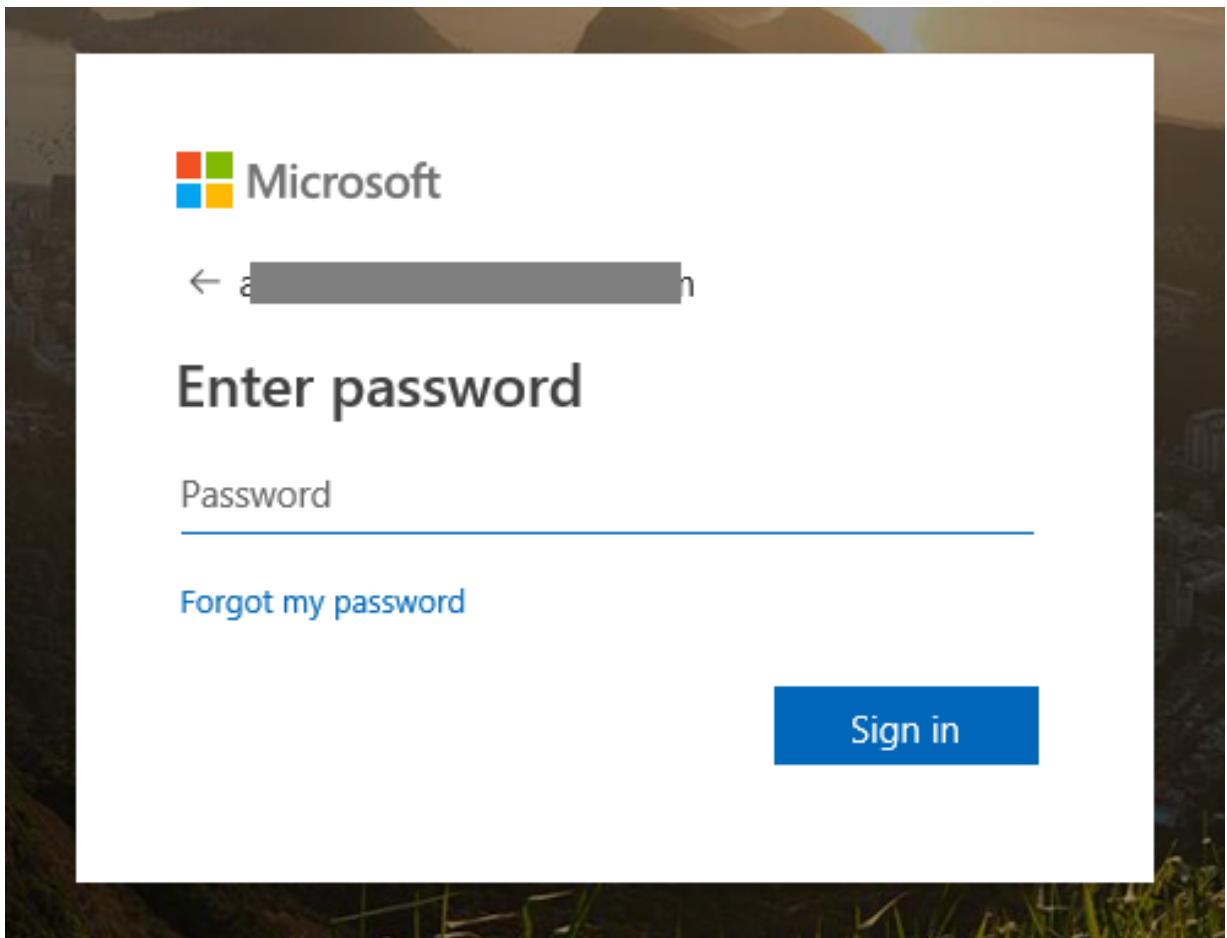
Email, phone, or Skype

---

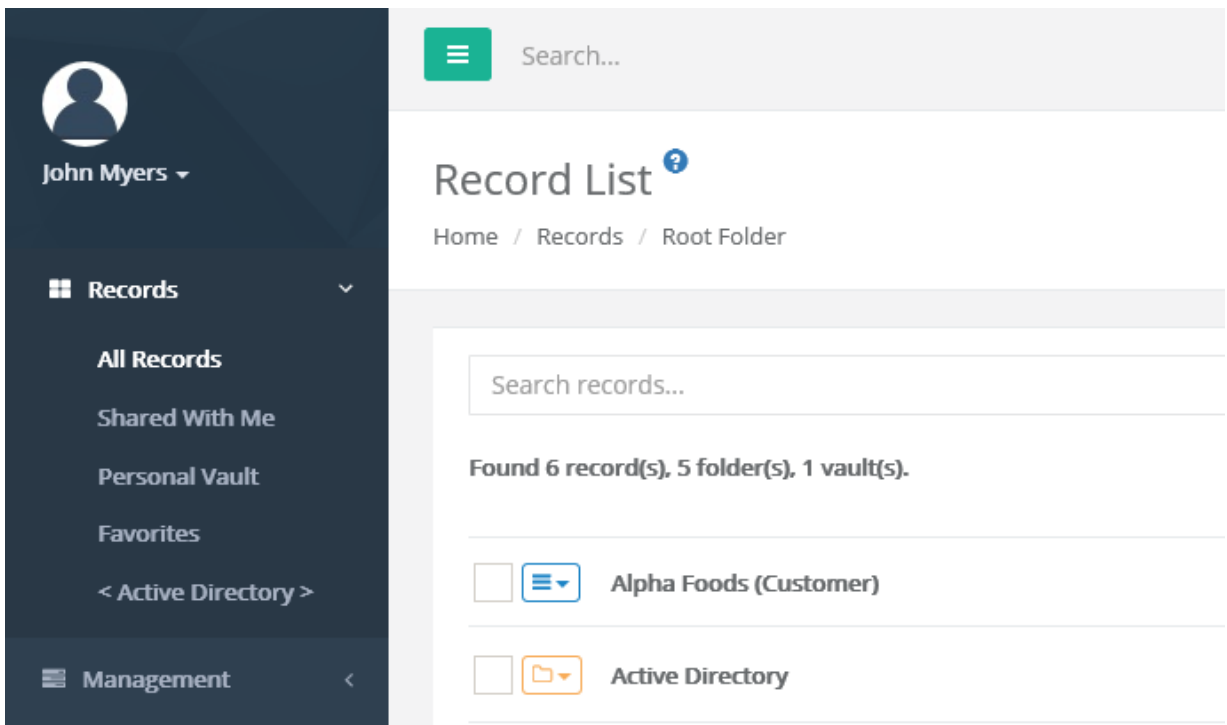
[Can't access your account?](#)

Next

- You will enter the password for this user account and click **Sign in**.



- After the account is authenticated against Azure Active Directory, you will be redirected to the PAM homepage (**All Records** view) and your account should be displayed as logged in.



If you receive any errors during this test procedure, then recheck all configuration that was entered in the previous steps and restart the PAM service again.

## ADFS Integration

A self-hosted Active Directory Federation Services (ADFS) is a service provided by Microsoft that provides a web login using your existing Active Directory credentials.

PAM supports integration with single sign-on (SSO) logins through a SAML 2.0 identity provider (IDP) like those of ADFS to provide authentication services.

### Requirements

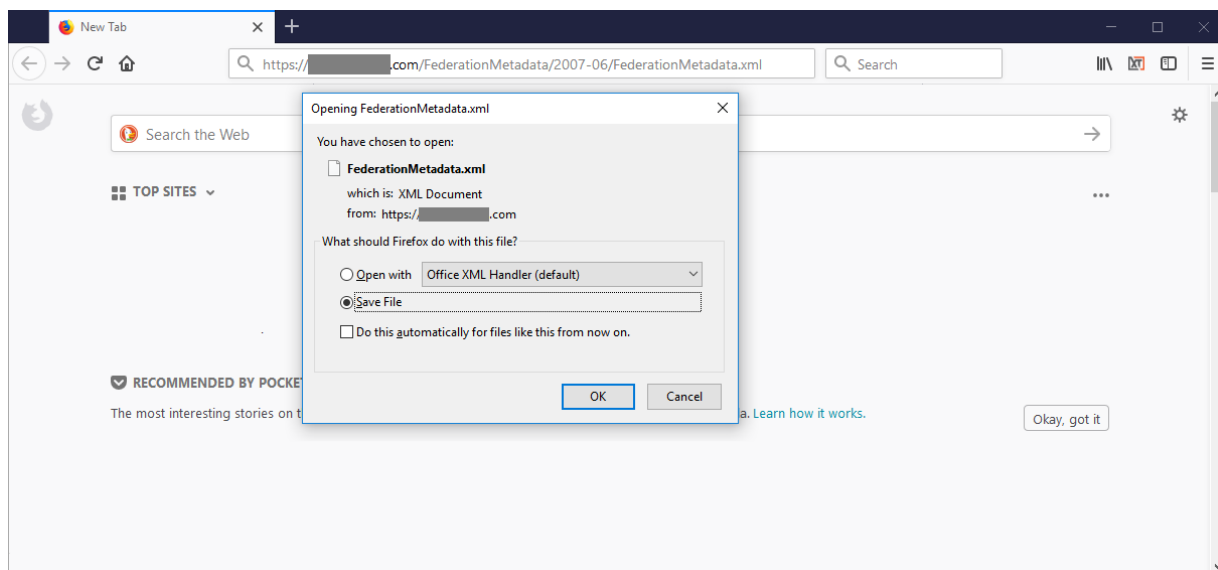
Before you begin to integrate PAM with your ADFS, be sure you met the following pre-requisites:

- A working PAM deployment with the [Federated Sign-In](#) experience. The PAM Federated Sign-In module provides the required SAML 2.0 web login functionality.
- A working PAM deployment with [Active Directory integration](#). The Active Directory integration provides the security for users and groups in PAM after they are authenticated via ADFS.
- Access to your existing PAM host server. You will need to update a configuration file, certificates and restart services.
- Access to your existing ADFS Management module for Active Directory. You will need to create a new Relying Party Trust.
- Your ADFS certificate to sign the login experience.

Configuring and installing ADFS is beyond the scope of this article, so we will provide a link to this [Microsoft KB article](#) for detailed information.

### Step 1: Download your ADFS Federation Metadata File to PAM

1. Login to your PAM host server and open your browser.
2. **Download and Save** your ADFS Metadata `.xml` file to `$PAM_HOME/content/keys`. This file can be found in this example location: `https://<ADFS_hostname>/FederationMetadata/2007-06/FederationMetadata.xml`



## Step 2: Import your ADFS Self-Signed Certificate to PAM

If your ADFS deployment is using a self-signed certificate, then continue with this step. Otherwise, skip step 2 and proceed to step 3.

1. Export your self-signed certificate, copy it to your PAM host server and paste it to `$PAM_HOME/content/keys`.
2. Open a command line and navigate to the folder where PAM is installed `$PAM_HOME` and issue the following command:
  - a. For Windows, substitute `PATH_TO_CERTIFICATE_FILE.cer` with the location and name of the self-signed `.cer` certificate file to be imported and used by PAM.

```
1 | bin\PamKeytool.cmd -import -alias xtadfs -file PATH_TO_CERTIFICATE_
FILE.cer -keystore jre\lib\security\cacerts
```

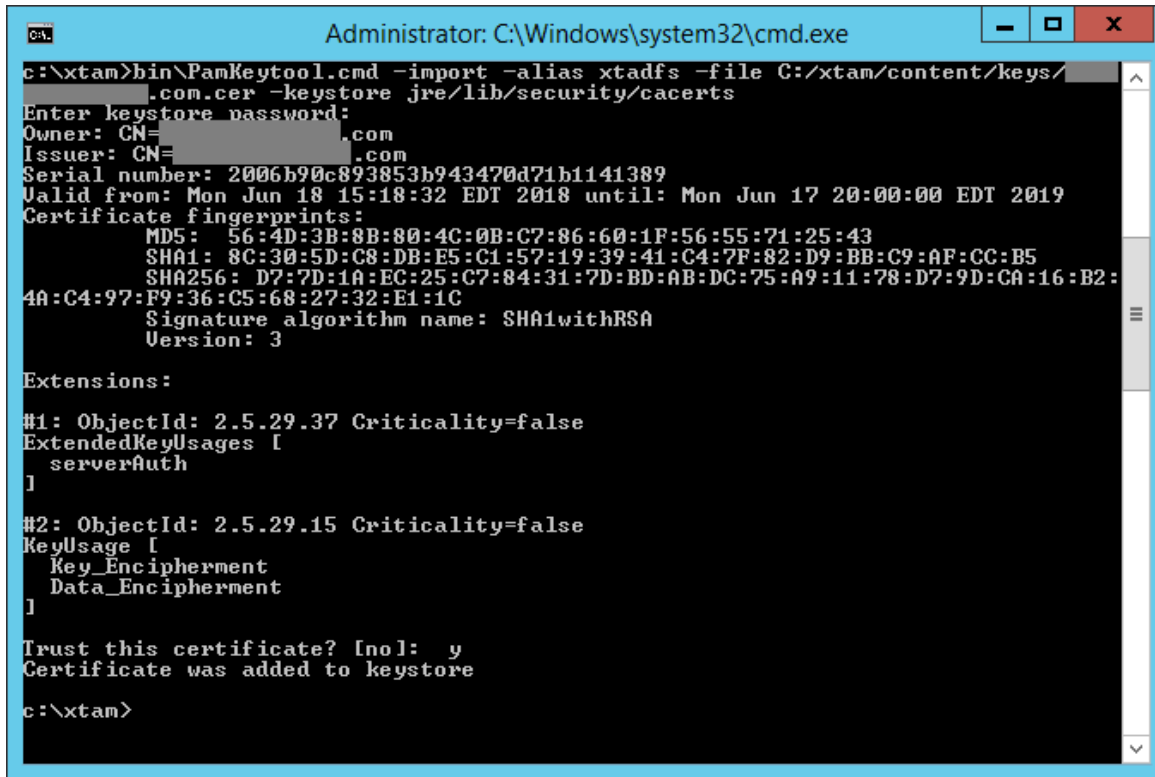
- b. For Unix or Linux, substitute `PATH_TO_CERTIFICATE_FILE.cer` with the location and name of the self-signed `.cer` certificate file to be imported and used by PAM.

```
1 | bin/PamKeytool.sh -import -alias xtadfs -file PATH_TO_CERTIFICATE_FILE.cer
-keystore jre/lib/security/cacerts
```

3. After the command is issued, you will be prompted for the keystore password. Enter the value **changeit** and press the **Enter key** to continue.
4. When prompted *Trust this certificate?* enter **y** and press the Enter key. You will receive the message



Certificate was added to keystore when it has imported successfully.



```
c:\xtam>bin\PamKeytool.cmd -import -alias xtadfs -file C:/xtam/content/keys/...com.cer -keystore jre/lib/security/cacerts
Enter keystore password:
Owner: CN=...com
Issuer: CN=...com
Serial number: 2006b90c893853b943470d71b1141389
Valid from: Mon Jun 18 15:18:32 EDT 2018 until: Mon Jun 17 20:00:00 EDT 2019
Certificate fingerprints:
    MD5: 56:4D:3B:8B:80:4C:0B:C7:86:60:1F:56:55:71:25:43
    SHA1: 8C:30:5D:C8:DB:E5:C1:57:19:39:41:C4:7F:82:D9:BB:C9:AF:CC:B5
    SHA256: D7:7D:1A:EC:25:C7:84:31:7D:BD:AB:DC:75:A9:11:78:D7:9D:CA:16:B2:
4A:C4:97:F9:36:C5:68:27:32:E1:1C
Signature algorithm name: SHA1withRSA
Version: 3

Extensions:
#1: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
    serverAuth
]
#2: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
    Key_Encipherment
    Data_Encipherment
]

Trust this certificate? [no]: y
Certificate was added to keystore
c:\xtam>
```

### Step 3: PAM Configuration

This step describes the process required to modify PAM configuration in order to identify your ADFS provider.

1. Open the following file in a text editor `$PAM_HOME/web/conf/catalina.properties`
2. `cas.authn.pac4j.saml[0].sign-service-provider-logout-request=true`
3. Locate the section labeled **# CAS** and add the following lines:

```
1 cas.server.name={managed_path}
2 cas.server.prefix={managed_path}/cas
3
4 cas.authn.pac4j.saml[0].clientName=ADFS
5 cas.authn.pac4j.saml[0].serviceProviderEntityId={managed_path}
6 cas.authn.pac4j.saml[0].serviceProviderMetadataPath={FederationMetadata.xml}
7 cas.authn.pac4j.saml[0].keystorePath={samlKeystore.jks}
8 cas.authn.pac4j.saml[0].keystorePassword={password}
9 cas.authn.pac4j.saml[0].privateKeyPassword={password}
10 cas.authn.pac4j.saml[0].identityProviderMetadataPath={path}
```

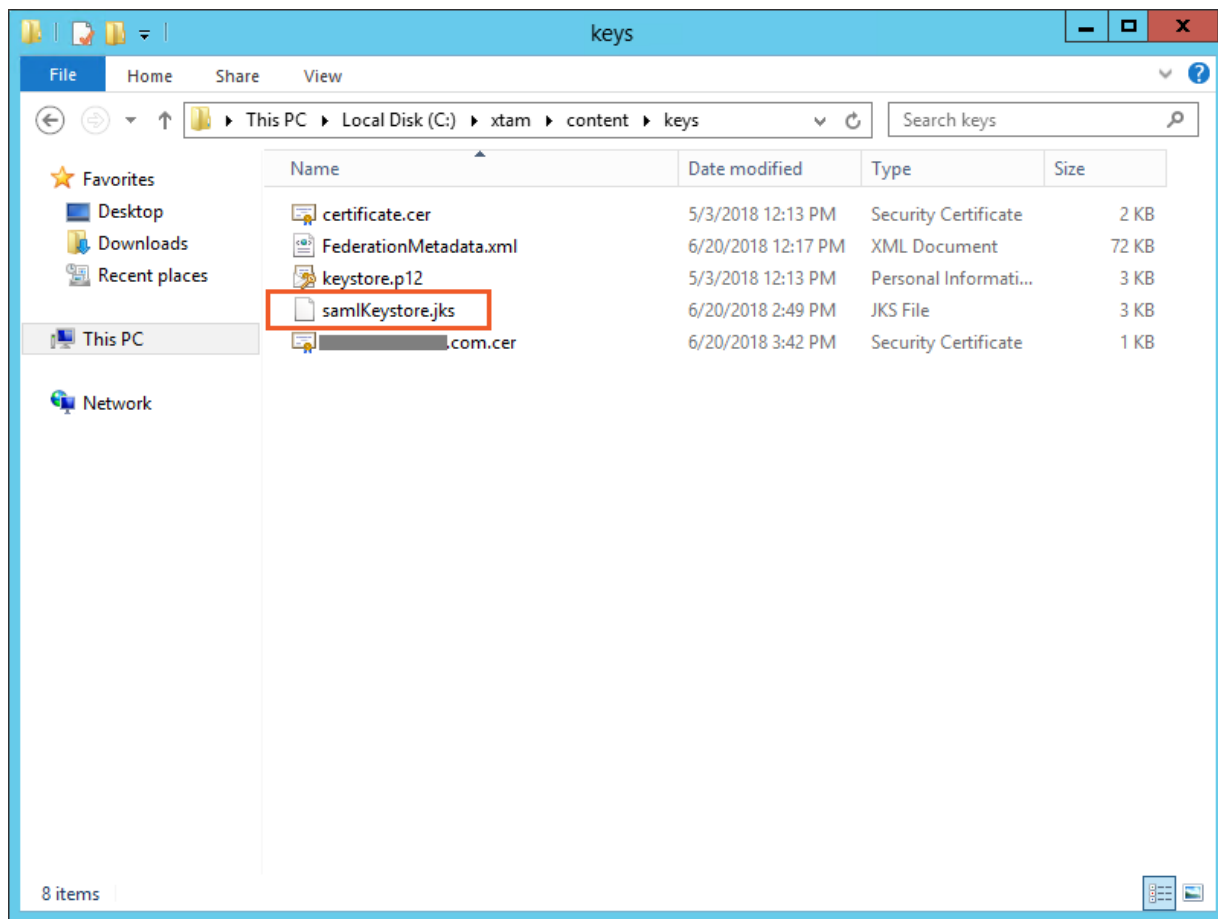
4. In the lines above, the following **{placeholders}** need to be updated using your own values as explained here:
  - a. `cas.server.name={managed_path}` — Your PAM host name. For example, `https://xtam.company.com`
  - b. `cas.server.prefix={managed_path}/cas` — Your PAM host name. For example, `https://xtam.company.com`
  - c. `cas.authn.pac4j.saml[0].serviceProviderEntityId={managed_path}` — Your PAM host name. For example, `https://xam.company.com`

- d. `cas.authn.pac4j.saml[0].serviceProviderMetadataPath={FederationMetadata.xml}` — The full path and file name of the `FederationMetadata.xml` file that was saved in step (1). For example, `C:/xtam/content/keys/FederationMetadata.xml` (use forward slashes not backslashes)
- e. `cas.authn.pac4j.saml[0].keystorePath={samlKeystore.jks}` — Define a path and name for the PAM auto-generated key. For example, `C:/xtam/content/keys/samlKeystore.jks` (use forward slashes not backslashes)
- f. `cas.authn.pac4j.saml[0].keystorePassword={password}` — Create an alphanumeric password. Any value you want to enter.
- g. `cas.authn.pac4j.saml[0].privateKeyPassword={password}` — Create an alphanumeric password. Any value you want to enter.
- h. `cas.authn.pac4j.saml[0].identityProviderMetadataPath={path}` — Copy and paste the full URL from your Identity Provider Metadata used in step (1). For example, `https://<ADFS_host-name>/FederationMetadata/2007-06/FederationMetadata.xml`

To enable the MFA Push/OTP notifications for authentication flow which using the Active Directory Federation Service (ADFS) needs specify Azure SSO SAML follow the steps:

- Setup [Azure SSO App](#) at Azure portal.
- [Add properties](#) for **#Azure SSO SAML** to the following file `$PAM_HOME/web/conf/catalina.properties` in a text editor (be sure the index [0] will be the first in indexes for your `cas.authn.pac4j.saml` settings).
- Re-enable login and password in the workflow using user interface or RDP/SSH.

5. When finished, **save** and **close** this file.
6. Restart the **PamManagement** (Windows) or the **pammanager** (Linux) service.
7. After the service restarts, open a browser and navigate to the PAM login page. If the PAM login page is already open, then simply refresh this page.
8. Open your file explorer, navigate to `$PAM_HOME/content/keys` and ensure that the **samlKeystore.jks** file was created. If the file is not present, then login to PAM using a non-ADFS account and check again.



#### Step 4: Generate an PAM Certificate

This step will generate an PAM certificate to be used later as the Signature in your ADFS Relying Partner Trust.

1. On the PAM host server, open a command line and navigate to the folder where PAM is installed \$PAM\_HOME and issue the following command:

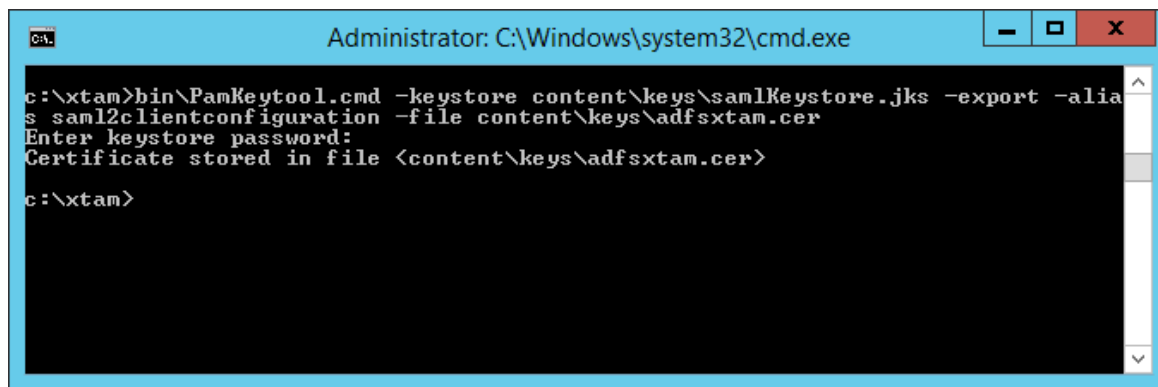
- a. For Windows:

```
1 | bin\PamKeytool.cmd -keystore content\keys\samlKeystore.jks -export -alias  
saml2clientconfiguration -file content\keys\adfsxtam.cer
```

- b. For Unix or Linux:

```
1 | bin\PamKeytool.sh -keystore content/keys/samlKeystore.jks -export -alias  
saml2filesystemkeystoregenerator -file content/keys/adfsxtam.cer
```

2. When prompted for the keystore password, enter the password you supplied in Step 3 Bullet 3f (cas.authn.pac4j.saml[0].keystorePassword={password}).

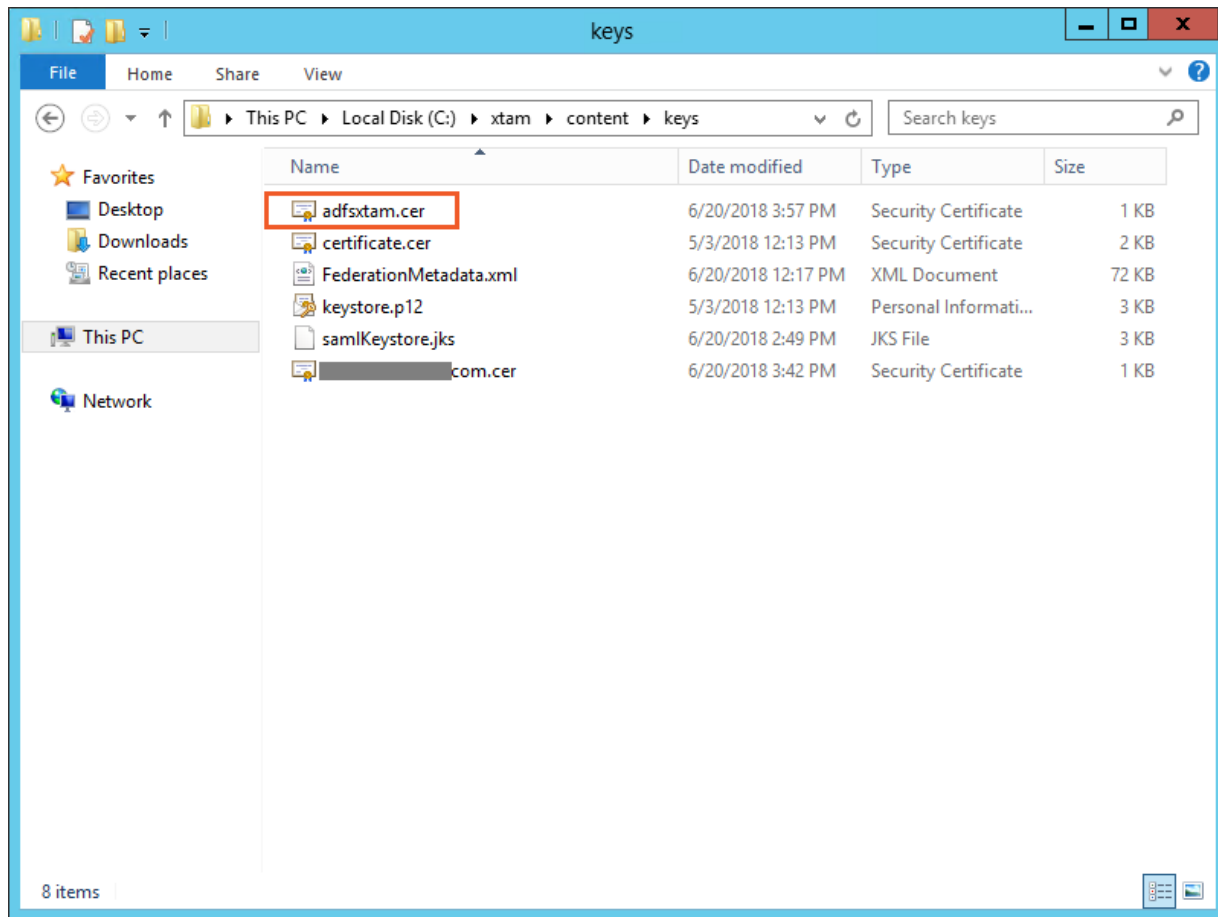


```
Administrator: C:\Windows\system32\cmd.exe

c:\xtam>bin\PamKeytool.cmd -keystore content\keys\samlKeystore.jks -export -alias saml2clientconfiguration -file content\keys\adfsxtam.cer
Enter keystore password:
Certificate stored in file <content\keys\adfsxtam.cer>

c:\xtam>
```

3. The PAM certificate will be generated and saved to `$PAM_HOME\content\keys\adfsxtam.cer`. Locate and then *Copy* this certificate file to your ADFS server.

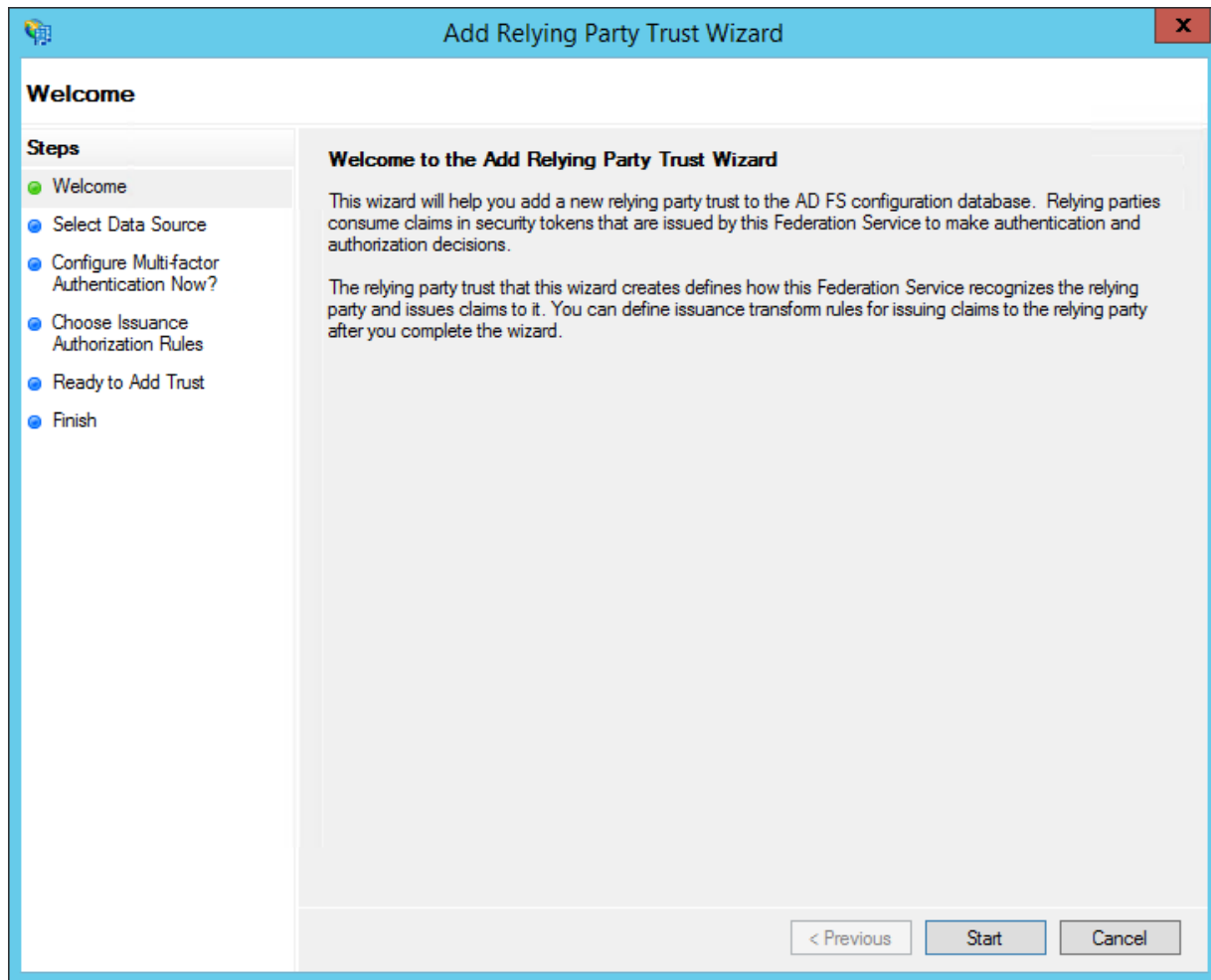


### *Step 5: Create an ADFS Relying Party Trust for PAM*

This section will describe how to create a new Relying Party Trust for PAM to use for the integration. The connection between ADFS and PAM is defined using this Relying Party Trust (RPT).

1. Login to your ADFS server.
2. Open your AD FS Management snap-in and click the **Add Relying Party Trust...** link to open the wizard. On

the wizard's **Welcome** screen, click the **Start** button to begin.



3. On the **Select Data Source** screen, select the last option, **Enter data about the relying party manually** and then click **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar is blue with a close button (X) in the top right corner. The main window has a light gray background. On the left, there is a 'Steps' pane with a list of steps: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled 'Select Data Source' and contains the following text: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network' with a description: 'Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.' It includes a text field for 'Federation metadata address (host name or URL):' with an example: 'fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file' with a description: 'Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.' It includes a text field for 'Federation metadata file location:' and a 'Browse...' button. 3. 'Enter data about the relying party manually' (selected) with a description: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

**Add Relying Party Trust Wizard**

**Select Data Source**

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

Browse...

☒ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous   Next >   Cancel

4. On the **Specify Display Name** screen, enter a **Display name** that you'll recognize and optionally any **Notes** you wish to include and then click **Next**.

**Add Relying Party Trust Wizard**

### Specify Display Name

Enter the display name and any optional notes for this relying party.

**Steps**

- Welcome
- Select Data Source
- Specify Display Name**
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

**Display name:**

XTAM ADFS

**Notes:**

< Previous   Next >   Cancel



5. On the **Choose Profile** screen, select the **AD FS profile** radio button and then click **Next**.

**Add Relying Party Trust Wizard**

### Choose Profile

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile**
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

☒ **AD FS profile**  
This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

☐ **AD FS 1.0 and 1.1 profile**  
This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

< Previous   Next >   Cancel

6. On the **Configure Certificate** screen, leave the certificate settings at their defaults and then click **Next**.

The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard" with a close button (X) in the top right corner. The main area is titled "Configure Certificate". On the left, a "Steps" pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate (which is highlighted with a green dot and a grey background), Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main content area contains the following text: "Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..". Below this text is a form with four labels: "Issuer:", "Subject:", "Effective date:", and "Expiration date:". To the right of these labels is a large rectangular text box. Below the text box are three buttons: "View...", "Browse..." (which is highlighted with a blue border), and "Remove". At the bottom right of the dialog are three buttons: "< Previous", "Next >", and "Cancel".

7. On the **Configure URL** screen, check the box labeled **Enable support for the SAML 2.0 WebSSO protocol**. The relying party service URL will be your {managed path} defined previously plus **/cas/login?client\_name=ADFS**. For example, [https://xtam.company.com/cas/login?client\\_name=ADFS](https://xtam.company.com/cas/login?client_name=ADFS). Click **Next** to continue.

The screenshot shows the 'Add Relying Party Trust Wizard' window with the 'Configure URL' step selected. The left sidebar lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL (selected), Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains instructions and configuration options for ADFS. It includes two checkboxes: 'Enable support for the WS-Federation Passive protocol' (unchecked) and 'Enable support for the SAML 2.0 WebSSO protocol' (checked). The SAML 2.0 WebSSO section includes a text box for the 'Relying party SAML 2.0 SSO service URL' containing the example URL 'https://xtam.company.com/cas/login?client\_name=ADFS'. At the bottom right are buttons for '< Previous', 'Next >', and 'Cancel'.

**Add Relying Party Trust Wizard**

**Configure URL**

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☐ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: <https://fs.contoso.com/adfs/ls/>

☒ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

Example: <https://www.contoso.com/adfs/ls/>

< Previous   Next >   Cancel

8. On the **Configure** Identifiers screen, enter your {managed path} URL and then click the **Add** button. For example, *https://xtam.company.com*

Note that this URL must match exactly to what was used previously. Click **Next** to continue.

**Add Relying Party Trust Wizard**

**Configure Identifiers**

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

9. On the next screen, you may configure multi-factor authentication if desired, but for this article we will enable the **I do not want to configure multi-factor authentication settings for this relying party trust at this time** and then click **Next** to continue.

**Add Relying Party Trust Wizard**

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

☒ I do not want to configure multi-factor authentication settings for this relying party trust at this time.

☐ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

< Previous   Next >   Cancel

10. On the **Choose Issuance Authorization Rules** screen, select the **Permit all users to access this relying party** radio button and then click **Next**.

Add Relying Party Trust Wizard

X

Choose Issuance Authorization Rules

Steps

● Welcome

● Select Data Source

● Specify Display Name

● Choose Profile

● Configure Certificate

● Configure URL

● Configure Identifiers

● Configure Multi-factor Authentication Now?

● Choose Issuance Authorization Rules

● Ready to Add Trust

● Finish

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

☒ Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

☐ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

< Previous

Next >

Cancel

© 2025 Imprivata, Inc. All Rights Reserved.

| 128

11. On the **Ready to Add Trust** screen, review your settings and then click **Next** to continue.

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button (X). The main window has a light blue header with the text 'Ready to Add Trust'. On the left, there is a 'Steps' pane with a list of steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust (highlighted), and Finish. The main area of the wizard has a light gray background. At the top, it says 'The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.' Below this is a tabbed interface with tabs: Monitoring (selected), Identifiers, Encryption, Signature, Accepted Claims, Organization, Endpoints, and Notes. The 'Monitoring' tab is active, showing the text 'Specify the monitoring settings for this relying party trust.' Below this is a text box labeled 'Relying party's federation metadata URL:'. There are two checkboxes: 'Monitor relying party' (unchecked) and 'Automatically update relying party' (unchecked). Below these are two lines of text: 'This relying party's federation metadata data was last checked on: < never >' and 'This relying party was last updated from federation metadata on: < never >'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

**Add Relying Party Trust Wizard**

**Ready to Add Trust**

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust**
- Finish

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring | Identifiers | Encryption | Signature | Accepted Claims | Organization | Endpoints | Notes < >

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

☐ Monitor relying party

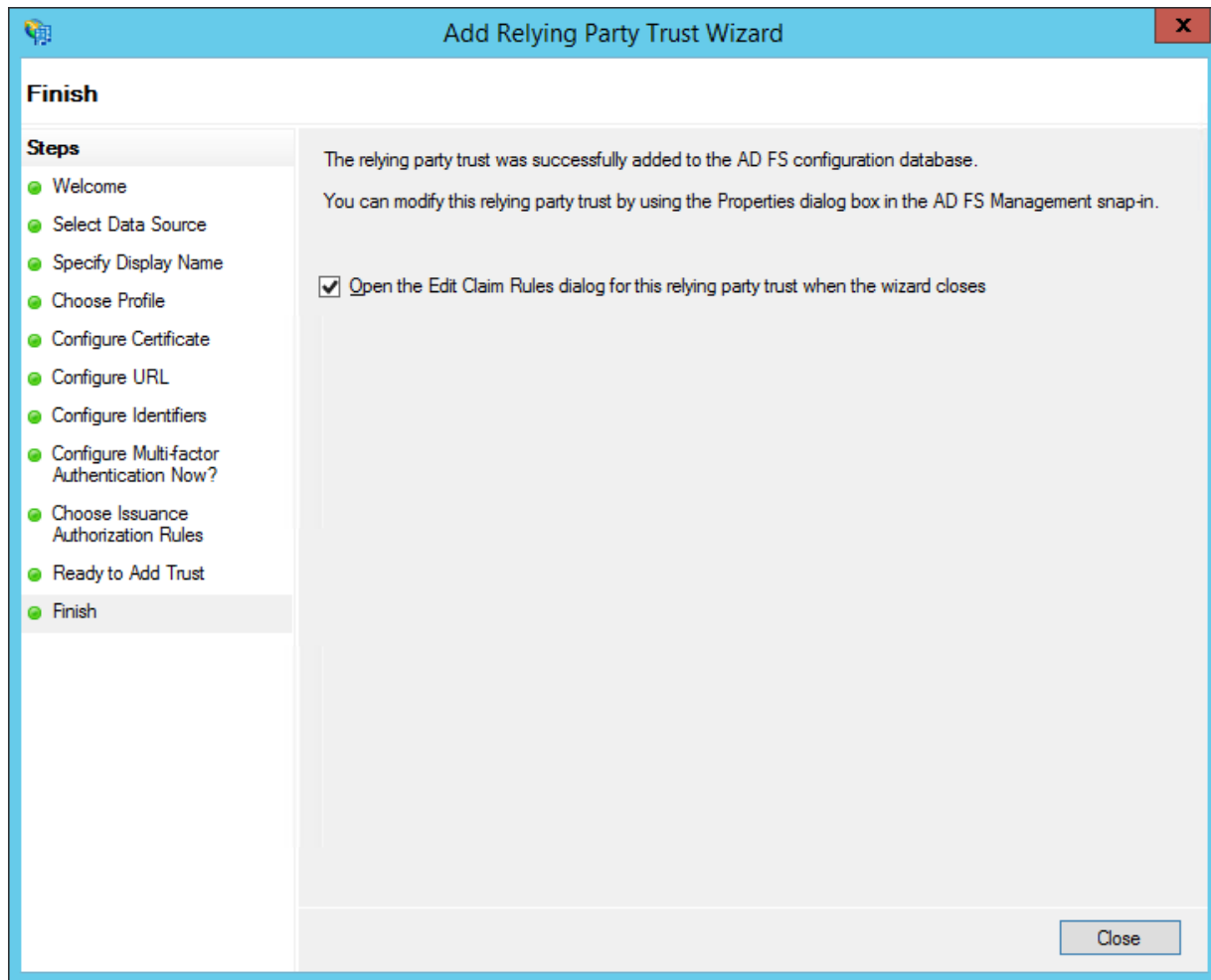
☐ Automatically update relying party

This relying party's federation metadata data was last checked on:  
< never >

This relying party was last updated from federation metadata on:  
< never >

< Previous | Next > | Cancel

- On the **Finish** screen, ensure the **Open the Edit Claims Rules** dialog option is checked and then click the **Close** button to continue.



### *Step 6: Create your ADFS Relying Party Trust Claim Rules*

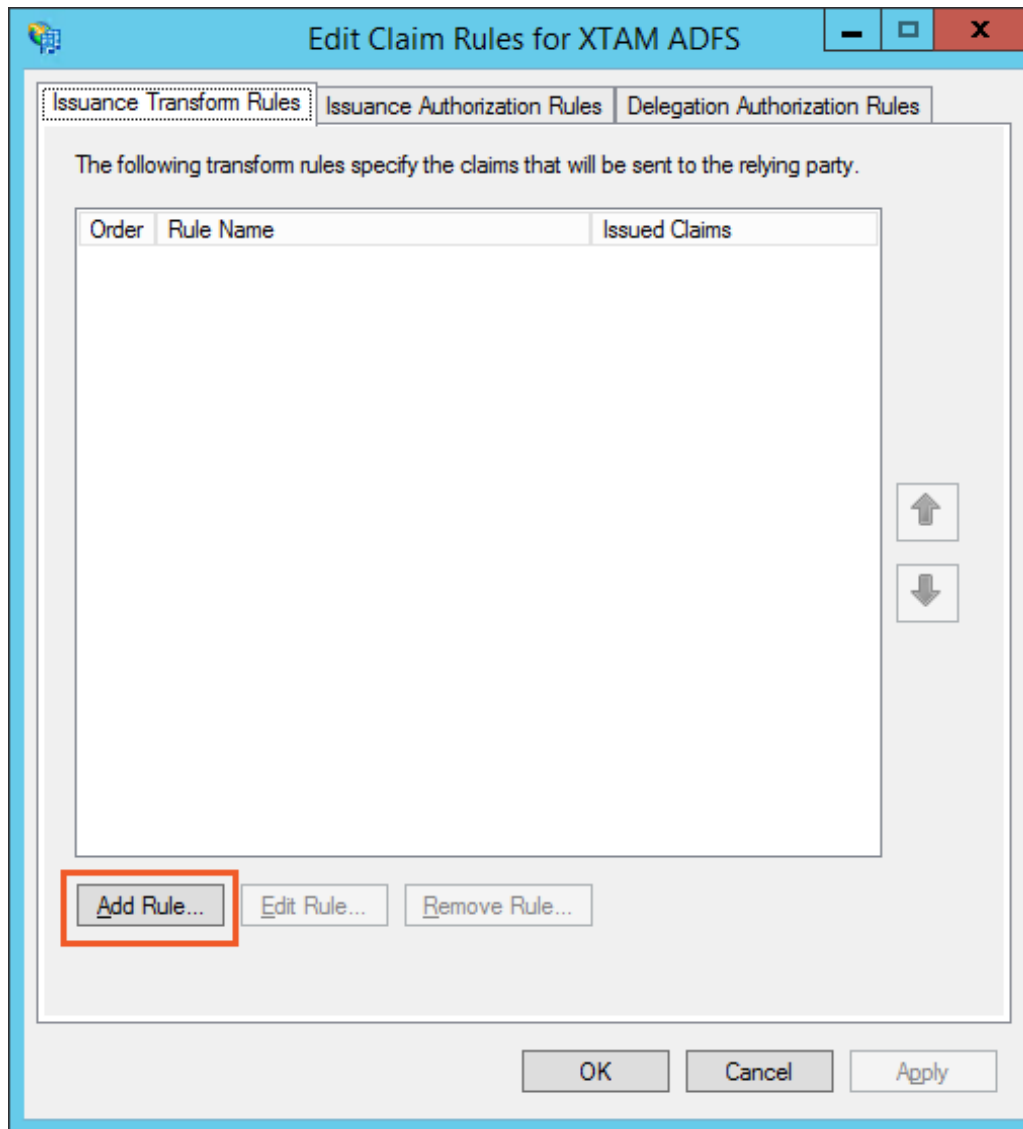
The Edit Claims Rules for your new Relying Trust will open automatically.

If it does not open automatically, select your RPT from the list and then click the Edit Claims Rules options in the Actions menu.

We will now configure a rule to finalize the ADFS integration.



1. On the **Issuance Transform Rules** tab, click on the **Add Rule** button.



2. In the **Add Transform Claim Rule Wizard**, on the **Choose Rule Type** page, select *Send LDAP Attributes as Claims* for the **Claim rule template**. Click **Next** to continue.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box. The title bar is blue with a close button (X) in the top right corner. The main area is white. On the left, there is a 'Steps' sidebar with two items: 'Choose Rule Type' (selected with a green dot) and 'Configure Claim Rule' (unselected with a blue dot). The main content area has a heading 'Select Rule Template'. Below the heading, there is a text block: 'Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.' Below this text is a label 'Claim rule template:' followed by a dropdown menu showing 'Send LDAP Attributes as Claims'. Below the dropdown is a label 'Claim rule template description:' followed by a text box containing the following text: 'Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.' At the bottom right of the dialog, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

3. On the **Configure Rule** screen, enter **Attributes from AD** as the **Claims rule name**.
4. On the **Configure Rule** screen, select **Active Directory** from the **Attribute store** dropdown.
5. On the **Configure Rule** screen, from the **LDAP Attribute** column, select **User-Principal-Name**.

- Configure Rule

Steps

Choose Rule Type

Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Attributes from AD

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	Name ID
*		

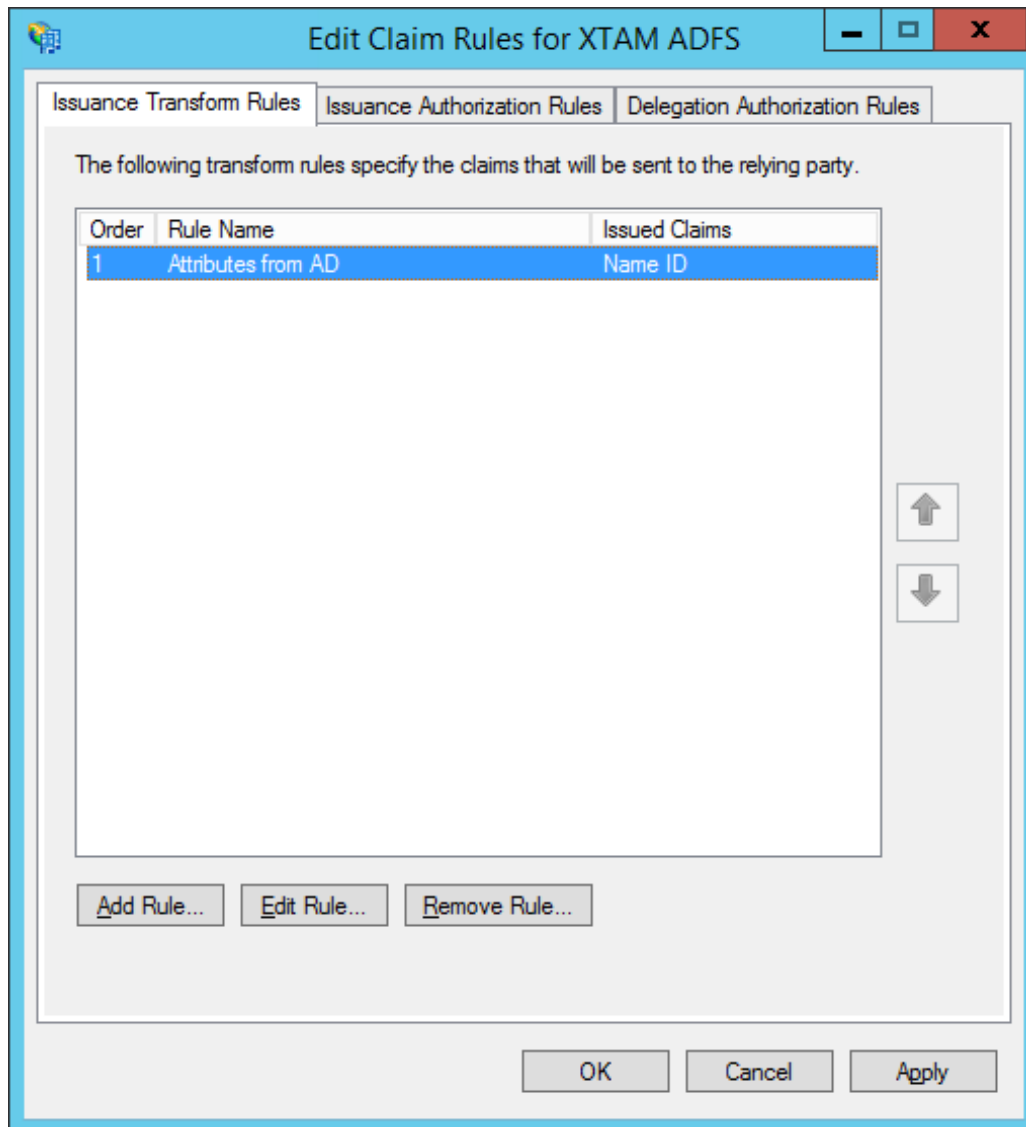
< Previous

Finish

Cancel

- © 2025 Imprivata, Inc. All Rights Reserved.

- When you return to the **Edit Claims Rule** dialog, click its **OK** button to complete the creation of your rules.

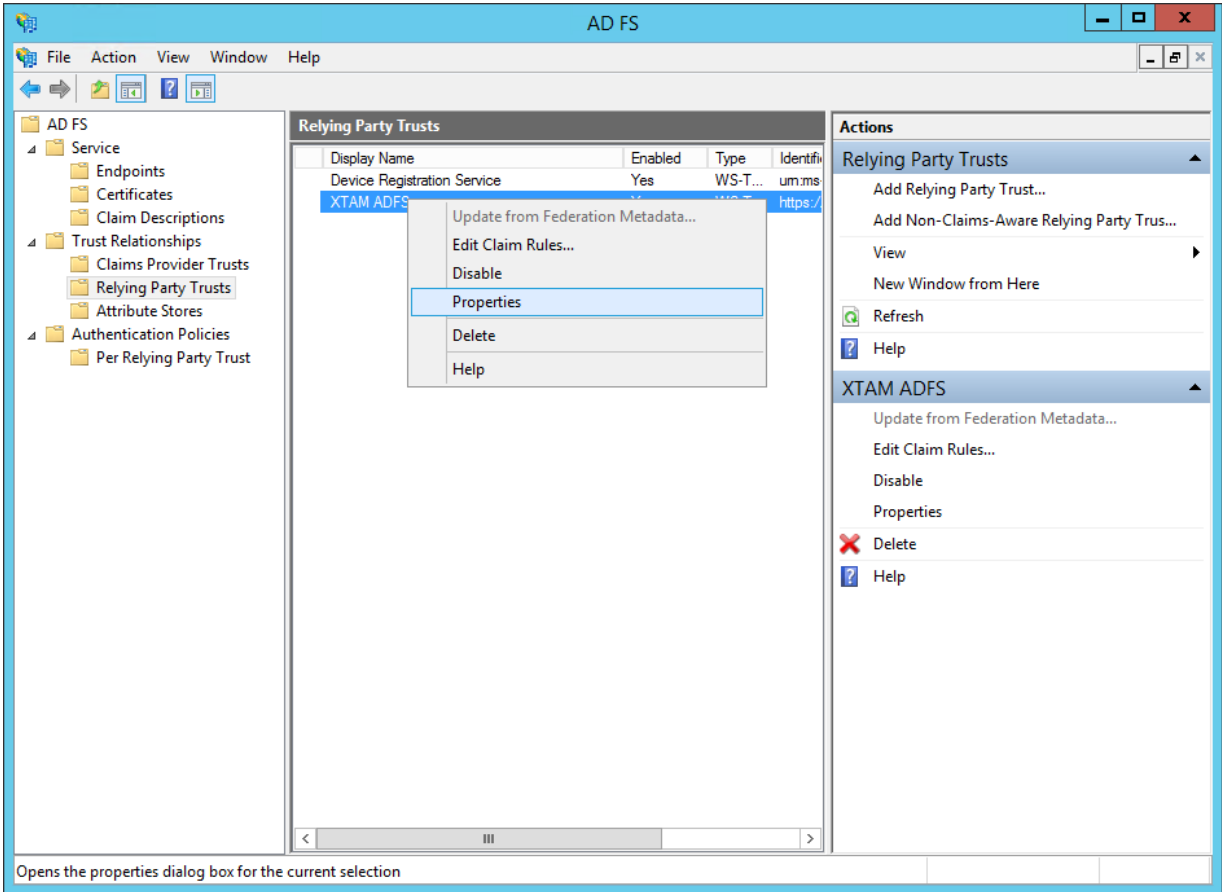


### *Step 7: Add the PAM Certificate to your RPT*

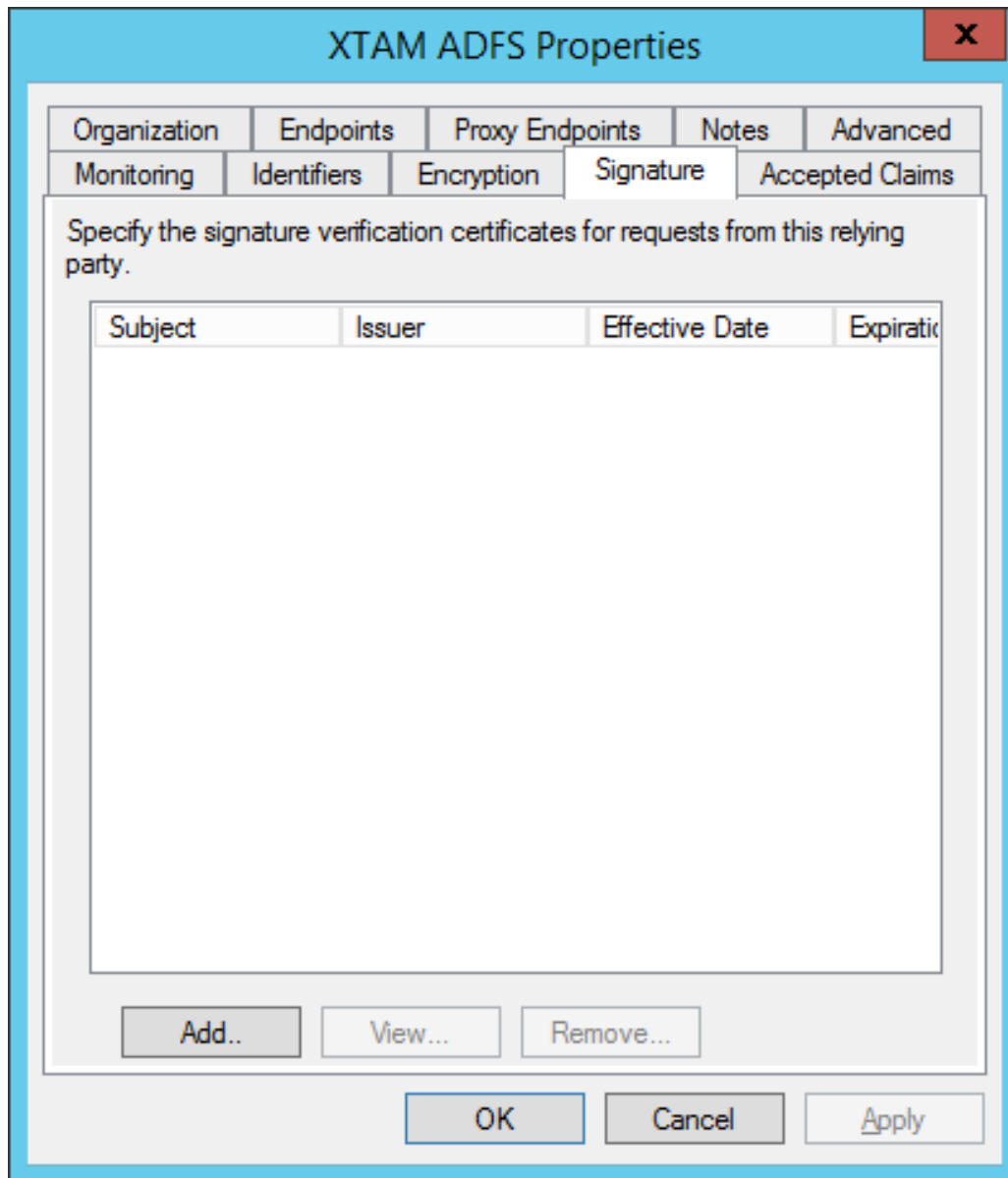
In this step, we will add the PAM certificate that we previously generated to your new RPT.

- In the ADFS Management snap-in, navigate to the ADFS > Trust Relationships > Relying Party Trusts section in the menu.

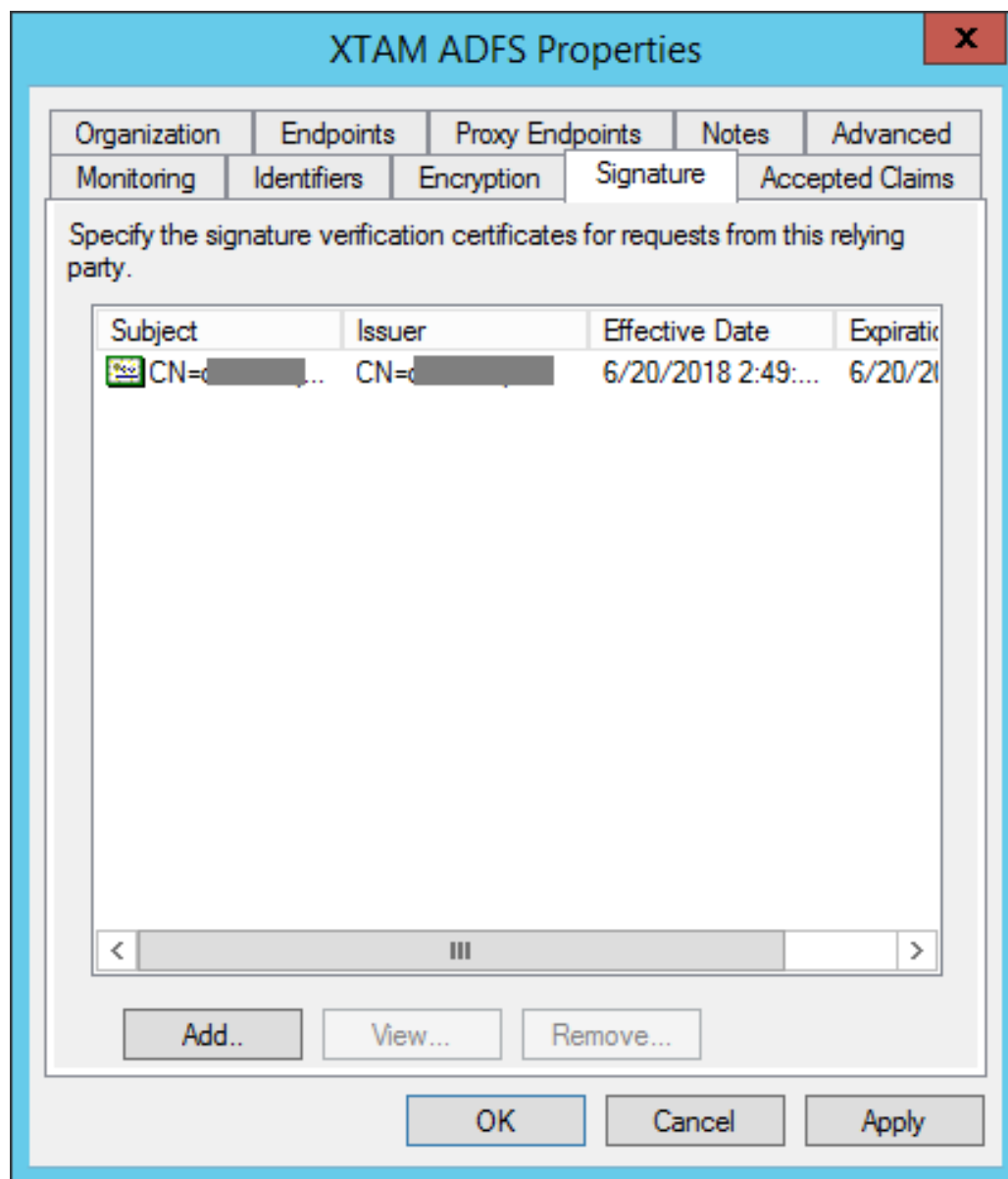
2. Select your newly created RPT from the list, then right click and choose **Properties**.



- When the Properties dialog appears, click on the **Signature** tab.



- Click the **Add** button to add your PAM certificate.
- In the **Select a Request Signature Verification Certificate** dialog, locate and select your `adfsxtam.cer` file (the one we generated in step 4) and then click **Open**.
- Your certificate will now be listed in the Signature table. Click the **OK** button to complete this step.



And that is it. You should now have a working ADFS SSO implementation for your PAM deployment. Return to your PAM login page, refresh and then click on the new Login with **ADFS** option on the bottom right to test your integration.

# Log in to Imprivata Privileged Access Management



Username:

Password:

Log in

[Forgot your password?](#)

For security reasons, please [log out](#) and exit your web browser when you are done accessing services that require authentication!

## Links to Additional Resources

[Documentation](#)

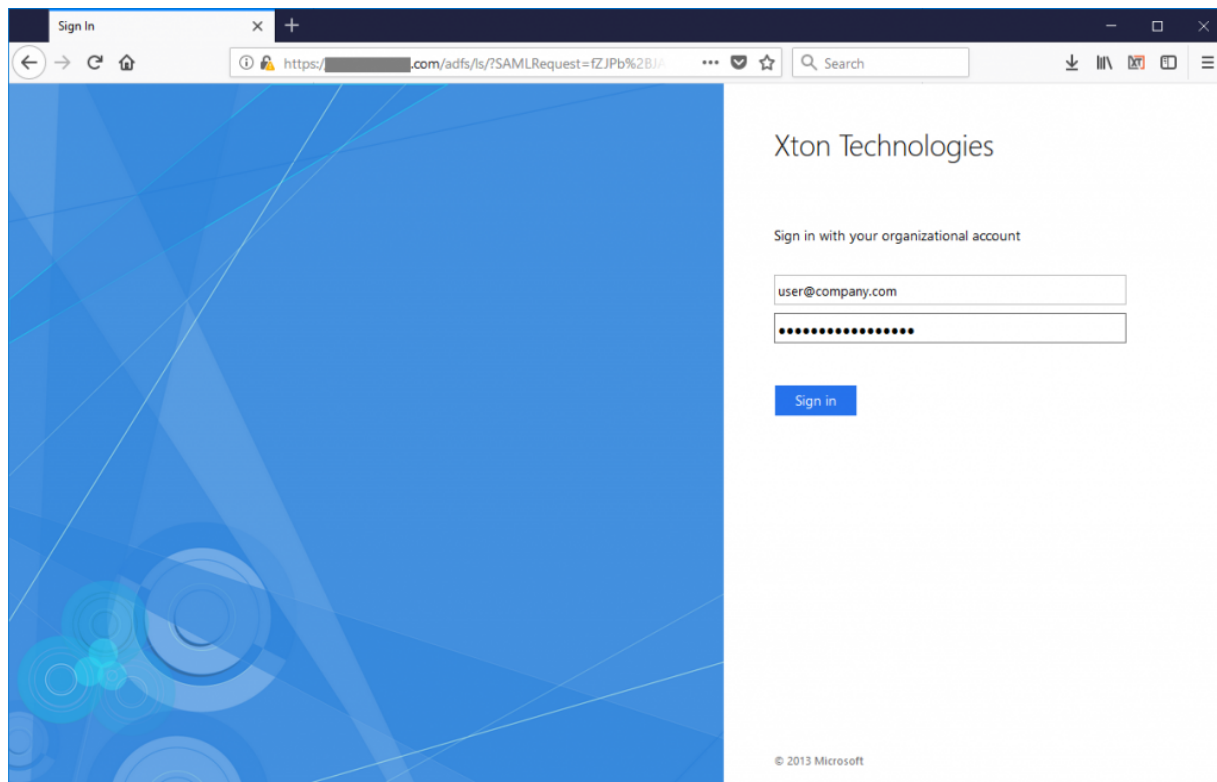
[Contact Imprivata Support](#)

Or log in with:



ADFS

Copyright (c) 2021, Imprivata, Inc.





For security reasons, after you logout of PAM, exit or close your web browser to securely complete the operation.

## Imprivata EAM

### Integration with Imprivata Confirm ID for MFA

#### Configuration for PAM and Imprivata Confirm ID (CIDRA) to provide RADIUS based MFA authentication

PAM supports integration with Imprivata Confirm ID using RADIUS to provide second factor authentication through the use of the Imprivata ID app (token and push).

The following guide describes how to configure your PAM and Confirm ID integration.

#### Requirements

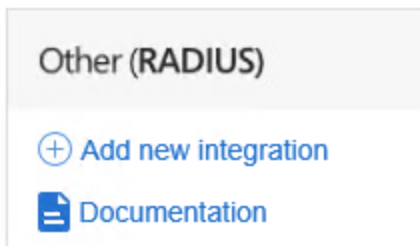
Before you begin your integration, be sure you meet the following pre-requisites:

- A working PAM deployment with the [Federated Sign-In](#) experience.
- Access to your existing PAM host server. You will need to update files and restart services.
- Access to your Imprivata Admin portal to configure your authentication services.
- If Users are created and managed in Imprivata, then a matching user must also be created as an PAM Local User.
- If Users are synced from Active Directory to Imprivata, then you must also integrate PAM with the same [Active Directory](#).
- Users must already enroll their device prior to authenticating with PAM. Device enrollment is not currently supported using PAM.

For customers integrating with Enterprise Access Management (formerly OneSign) v24.1 or higher, for EAM Number Matching feature to retain Push notification support using PAM, customers must update to PAM version 2.3.202410131511 or higher and [federated sign-in version 6.5](#).

#### Step 1: Begin the Imprivata Confirm ID Configuration

1. Login to your Imprivata Admin portal.
2. Navigate to Applications > Remote access integrations.
3. In the *Add new integration* section, locate the **Other (RADIUS)** option and click **Add new integration**.



4. On the *Add new integration* page using the guidance below for the RADIUS client information form:
  - a. **Nickname** – use any relevant value you choose. For example, *PAM*.
  - b. **Host name or IP address** – enter the host name or IP address of the PAM host server.
  - c. **Encryption key** – enter any alphanumeric value in this field which will be used as the shared secret between Confirm ID and PAM.

[Remote access integrations](#) > Add new integration

## Add new integration

### RADIUS client information

Nickname	?
Host name or IP address	
Encryption key	?

5. No other actions are required. Click the **Save** button to complete this configuration.

### Step 2: Configuring PAM for Confirm ID

1. Login to your PAM host server and open the file `$PAM_HOME\web\conf\catalina.properties` in a text editor.
2. Locate the section that begins with **# Radius, RSA Radius, SMSPasscode, etc.** This section will contain the following parameters:

```
#cas.authn.mfa.globalProviderId=mfa-radius
#cas.authn.mfa.radius.client/inetAddress=radius-server-host
#cas.authn.mfa.radius.client.sharedSecret=secret
#cas.authn.mfa.radius.client.authenticationPort=1812
#cas.authn.mfa.radius.client.accountingPort=1813
#cas.authn.mfa.radius.server.protocol=PAP
#cas.authn.mfa.radius.name=name
```

3. In the lines referenced above, make updates using your own values as explained here:
  - a. `cas.authn.mfa.radius.client/inetAddress=radius-server-host` – Enter the host or IP address of your Imprivata Confirm ID appliance. Uncomment this line (remove the # in the beginning).
  - b. `cas.authn.mfa.radius.client.sharedSecret=secret` – Enter the same alphanumeric value that was entered in the Encryption key in your ConfirmID RADIUS configuration during the previous step. Uncomment this line (remove the # in the beginning).
  - c. `cas.authn.mfa.radius.client.authenticationPort=1812` – Uncomment this line (remove the # in the beginning). No other changes are required.

- d. `cas.authn.mfa.radius.client.accountingPort=1813` – Uncomment this line (remove the # in the beginning). No other changes are required.
- e. `cas.authn.mfa.radius.server.protocol=PAP` - Uncomment this line (remove the # in the beginning) and change PAP to CIDRA\_PAP.
- f. `cas.authn.mfa.radius.name=ConfirmID`- Uncomment this line (remove the # in the beginning). For stable work MFA provider CorfirmID this property is required. Enter the CorfirmID name.

`xtam.cidra.auth.method=password+push` - Add this new line if your CIDRA Log in Workflow Policy is configured for only Password + Imprivata ID.

4. After your finish making the changes above, this section will look similar to this example:

```
1 #cas.authn.mfa.globalProviderId=mfa-radius
2 cas.authn.mfa.radius.client.inetAddress=10.157.65.87
3 cas.authn.mfa.radius.client.sharedSecret=yourSharedSecretKeyGoesHere
4 cas.authn.mfa.radius.client.authenticationPort=1812
5 cas.authn.mfa.radius.client.accountingPort=1813
6 cas.authn.mfa.radius.server.protocol=CIDRA_PAP
7 cas.authn.mfa.radius.name=ConfirmID
```

### Step 3: Configure RADIUS MFA Requirements in PAM

PAM can be configured to support two scenarios with [RADIUS MFA](#) enforcement, all user logins will require Imprivata ID or select principals (users or groups) may require Imprivata ID while others may require a different MFA provider like [Duo](#) or [TOTP](#) or perhaps no MFA requirement at all.

**To configure PAM so that all logins require Imprivata ID:**

1. Login to your PAM host server and open the file `PAM\web\conf\catalina.properties` files in a text editor.
2. Search for `xtam-mfa.groovy` to locate this parameter which you will uncomment like shown below (remove the # at the beginning of the line).

Note that the path defined in the parameter may be different depending on your PAM host (Windows or Linux) and its installation directory.

#### Before:

```
1 #cas.authn.mfa.groovyScript=file:///C:/xtam/web/webapps/xtam/WEB-INF/mfa/xtam-mfa.groovy
```

#### After:

```
1 cas.authn.mfa.groovyScript=file:///C:/xtam/web/webapps/xtam/WEB-INF/mfa/xtam-mfa.groovy
```

3. When finished, save and close the file.
4. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service.

- After the service comes back online, login to PAM with a System Administrator account and navigate to the Administration > MFA page.
- On this page we will select ConfirmID as the default MFA provider for user authentication. To use Confirm ID, click the *Add* button, check the **Default box** and in the Provider dropdown select the option *mfa-confirmid*. Click **Save** to complete this configuration. Upon next login, all users not explicitly assigned another mfa provider or none will be required to use ConfirmID as their second factor authentication method.

In the screenshot example configuration below, the **DEFAULT** provider is set to mfa-confirmid so all users will be required to use this provider as their second factor; however, since the user 'xtamadmin' is explicitly set to none as its provider, this account becomes the exception. Upon xtamadmin login, it will not be required to use any (none) second factor for authentication.

Showing 1 to 2 of 2 entries

User	Provider	Enabled	Actions
<input type="checkbox"/> <b>DEFAULT</b>	mfa-confirmid		...
<input type="checkbox"/> Service Administrator (xtamadmin) /Local	none		...

First Previous 1 Next Last

For more information about how to configure MFA on this page, please review our article [Defining MFA per User or Group](#).

#### To configure PAM so that individual logins may use Imprivata ID, TOTP, Duo or No MFA:

- Login to your PAM host server and open the file `$PAM_HOME\web\conf\catalina.properties` files in a text editor.
- Search for **xtam-mfa.groovy** to locate this parameter which you will uncomment like shown below (remove the **#** at the beginning of the line).

Note that the path defined in the parameter may be different depending on your PAM host (Windows or Linux) and its installation directory.

#### Before:

```
1 | #cas.authn.mfa.groovyScript=file:///C:/xtam/web/webapps/xtam/WEB-INF/mfa/xtam-mfa.groovy
```

#### After:

```
1 | cas.authn.mfa.groovyScript=file:///C:/xtam/web/webapps/xtam/WEB-INF/mfa/xtam-mfa.groovy
```

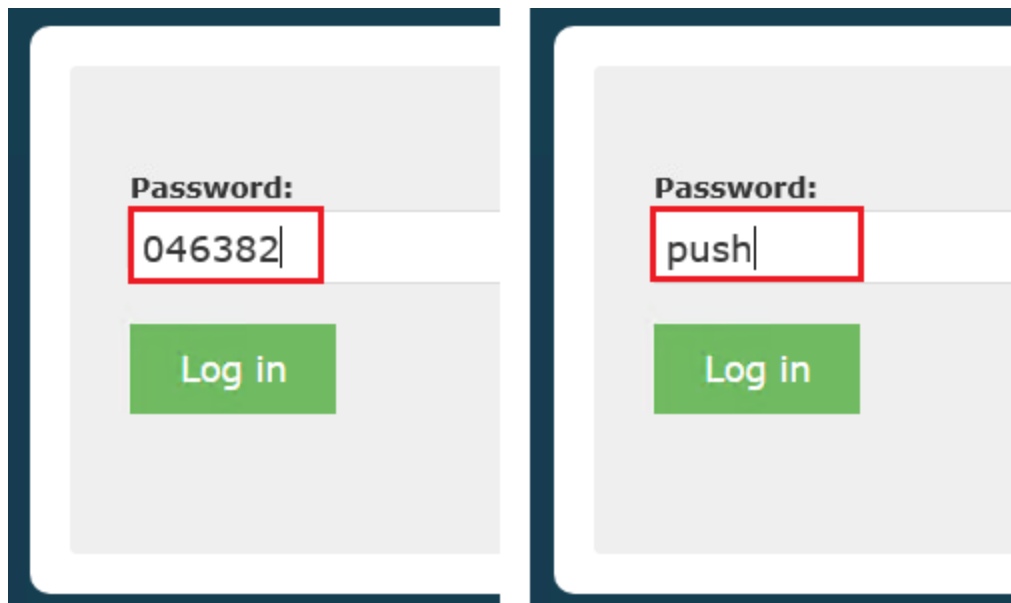
- When finished, save and close the file.

4. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service
5. After the service comes back online, login to PAM with a System Administrator account and navigate to the Administration > MFA page.
6. On this page, configure your users and groups with the provider that should be required for second factor authentication. To use Confirm ID, click the *Add* button, select your principals and in the Provider drop-down select the option *mfa-confirmid*. Click **Save** to complete this configuration and repeat as necessary for other users or groups.

For more information about how to configure MFA on this page, please review our article [Defining MFA per User or Group](#).

### Step 4: Test your Login Integration

1. Navigate to the PAM login page.
2. Enter the login credentials, Username and Password, of an account configured with the Confirm ID provider in the previous step. Click the **Log in** button.
3. After the credentials (first factor) are authenticated, you will be prompted for your second factor on the next page. In the field, you may enter the current Token Code as displayed in the Imprivata ID application on your enrolled device or you may enter the word push to receive a push notification to your enrolled device.



The image displays two side-by-side screenshots of a PAM login interface. Both screenshots show a 'Password:' label above a text input field. In the left screenshot, the input field contains the token code '046382'. In the right screenshot, the input field contains the word 'push'. A red rectangular box highlights the input field in both cases. Below the input field is a green button with the text 'Log in'.

4. When either the token or push is entered into the field, click the **Log in** button to continue. If a valid token was entered, the account will successfully login to PAM. If the push option was used, you will receive a push notification to your enrolled device, click **Approve** and the account will successfully login to PAM.

If you want to be able to send a command "push" in ConfirmID integration,

- open the file `$PAM_HOME/web/conf/catalina.properties` in text editor, locate the section that begins with `#CAS`,
- add the following line to this file:

```
1 | cas.authn.mfa.radius.client.push=true
```

- restart **PamManagement** (Windows) or the **pammanager** (Linux) service.

## Integration with Imprivata Enterprise Access Management (formerly OneSign)

### Configuration for PAM and Imprivata EAM to provide SAML based authentication

PAM supports integration with Imprivata EAM using SAML protocol to defer user authentication to EAM. The following guide describes how to configure your PAM and EAM integration.

### *Requirements*

Before you begin your integration, be sure you meet the following pre-requisites:

- A working PAM deployment with the [Federated Sign-In](#) experience.
- Access to your existing PAM host server. You will need to update files and restart services.
- Access to your EAM portal to configure your authentication services.
- If Users are created and managed in EAM, then a matching user must also be created as an PAM Local User.
- If Users are synced from Active Directory to EAM, then you must also integrate PAM with the same Active Directory.
- EAM must be provisioned with the Imprivata Cloud service before the integration can be performed.

### *Step 1: Begin the Imprivata EAM Configuration*

1. Login to your Imprivata EAM Admin portal.
2. Navigate to Applications > **Single sign-on application profiles**.
3. Click on the *Add App Profile* dropdown and select the **Application using SAML option**.

## OneSign single sign-on application profiles

Search for Applications

Application Profile Name

Add App Profile

Windows application using APG

Application using SAML

Application using OpenID Connect

Import from file...

	Deployment Status
Selected	

If you are presented with a message that this application requires a secure connection to the Imprivata Cloud, then EAM has not yet been provisioned with this service. Please consult your EAM documentation or support engineer for assistance with this required step before continuing.

4. Populate the *Add application using SAML* page using the guidance below:

- Application profile name** and **Application user-friendly name** – use any relevant value you choose. For example, PAM.
- In the *Service provider (SP) metadata* section, assign the following selections:
  - NameID format preference*: **Unspecified**
  - Returned Attribute*:
    - Select **User login name – Pre W2K (sAMAccountName)** if PAM is configured to authenticate using sAMAccountName. This is the default configuration in PAM.
    - Select **User login name (userPrincipalName)** if PAM is configured to authenticate using UPN.

## Service provider (SP) metadata

Imprivata requires SAML metadata configuration information from the application.

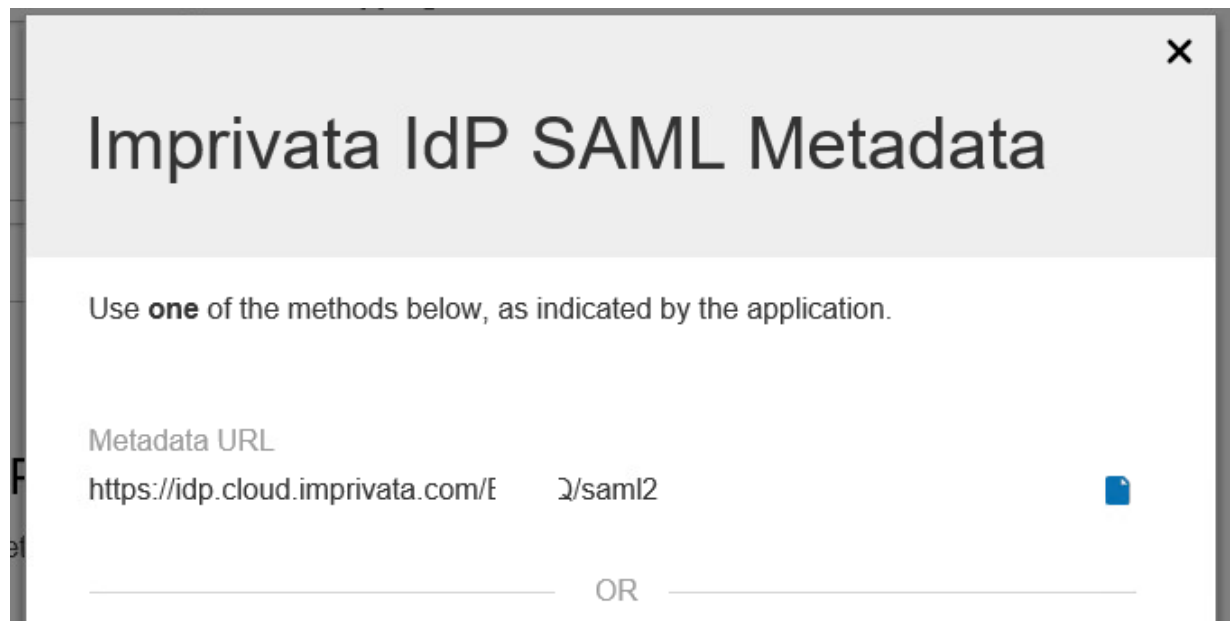
NameID format preference

Unspecified

Returned attribute

User logon name - Pre W2K (sAMAccountName)

3. In the *Identity provider (IdP) metadata* section, click to open the link named **View and copy Imprivata (IdP) SAML metadata**. When the link opens, locate and copy the URL displayed under the *Metadata URL* label. You will use this URL in the PAM configuration described in the next section of this guide.



5. You may close this dialog, but do not logout of the Admin console yet. We will return to complete this configuration later in the guide.

## Step 2: Configuring PAM for EAM

1. Login to your PAM host server and open the file `$PAM_HOME\web\conf\catalina.properties` in a text editor.
2. Locate the section that is labelled # CAS and add the following new lines:  
# Imprivata EAM SSO SAML  
cas.authn.pac4j.saml[0].clientName=EAM Login  
cas.authn.pac4j.saml[0].keystorePassword=password  
cas.authn.pac4j.saml[0].privateKeyPassword=password  
cas.authn.pac4j.saml[0].serviceProviderEntityId=https://xtam.company.com/xtam/  
cas.authn.pac4j.saml[0].serviceProviderMetadataPath=imprivatasso.xml  
cas.authn.pac4j.saml[0].keystorePath=samlKeystoreImprivataSSO.jks  
cas.authn.pac4j.saml[0].identityProviderMetadataPath=path  
cas.authn.pac4j.saml[0].maximumAuthenticationLifetime=2073600
3. In the lines referenced above, the placeholders need to be updated using your own values as explained here:
  - a. cas.authn.pac4j.saml[0].keystorePassword=password - Create an alphanumeric password. Any value you want to enter.



- b. `cas.authn.pac4j.saml[0].privateKeyPassword=password` - Create an alphanumeric password. Any value you want to enter.
  - c. `cas.authn.pac4j.saml[0].serviceProviderEntityId=https://xtam.company.com/xtam/` - Replace this placeholder URL with your full https PAM login page URL ending with /xtam/
  - d. `cas.authn.pac4j.saml[0].serviceProviderMetadataPath=imprivatasso.xml` - The full path and file name of the `imprivatasso.xml` file that will be created after an PAM service restart later in this guide. For example, `C:/pam/content/keys/imprivatasso.xml` (use forward slashes not backslashes). This file will be uploaded to your Imprivata SAML application later in this guide.
  - e. `cas.authn.pac4j.saml[0].keystorePath=samlKeystoreImprivataSSO.jks` - Define a path and name for the PAM auto-generated key. For example, `C:/pam/content/keys/samlKeystoreImprivataSSO.jks` (use forward slashes not backslashes).
  - f. `cas.authn.pac4j.saml[0].identityProviderMetadataPath=path` - Enter the full URL copied from the Metadata URL section of your Imprivata SAML configuration. For example, <https://idp.cloud.imprivata.com/{yourTenantID}/saml2>.
- 4. When finished, **save and close** this file.
  - 5. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service.
  - 6. When the service is fully restarted, open your browser and navigate to the PAM login page. You should see a new red button with the EAM Login label.

### Step 3: Complete the EAM Configuration

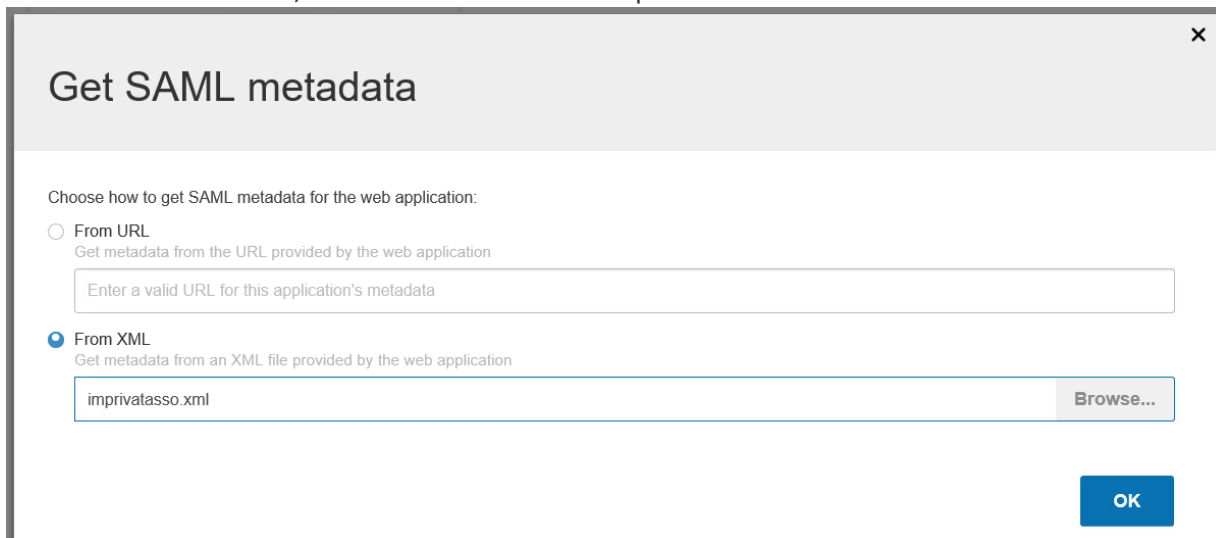
1. Return to the Add application using SAML page in your Imprivata Admin portal.
2. In the section Service provider (SP) metadata click the button labelled **Get SAML metadata**.

## Service provider (SP) metadata

Imprivata requires SAML metadata configuration information from the application.

Get SAML metadata

3. On this Get SAML metadata dialog, select the **From XML** option and click the **Browse...** button.
4. Browse to and select using the **Open** button, the `imprivatasso.xml` file that was created in the location defined in this previous PAM configuration parameter: `cas.authn.pac4j.saml[0].serviceProviderMetadataPath={imprivatasso.xml}`. For example, `C:/pam/content/keys/imprivatasso.xml`
5. After the file is selected, click the **OK** button to complete.



6. Imprivata will process the `.xml` file and display the relevant information in the *Service provider (SP) metadata* section. Please review the metadata and confirm it is accurate.
7. When satisfied, click the **Save** button to complete the creation of this new application profile.
8. Finally, you need to Deploy this application and configure users. Click on the **Not Deployed** link next to your new application. On the *Deploy application: PAM page*:
  - a. Check the **Deploy This Application** checkbox
  - b. Check the **Deploy to All User and Groups** checkbox or use the other options available to deploy to specific domains, OUs, groups or users.

- c. Click **Save** to complete the application deployment

### Deployment

Check the *Deploy This Application?* checkbox to set deployment options and deploy the application profile.

Deploy This Application? ☒

To deploy to selected users and groups, uncheck the *Deploy to All Users and Groups?* checkbox.

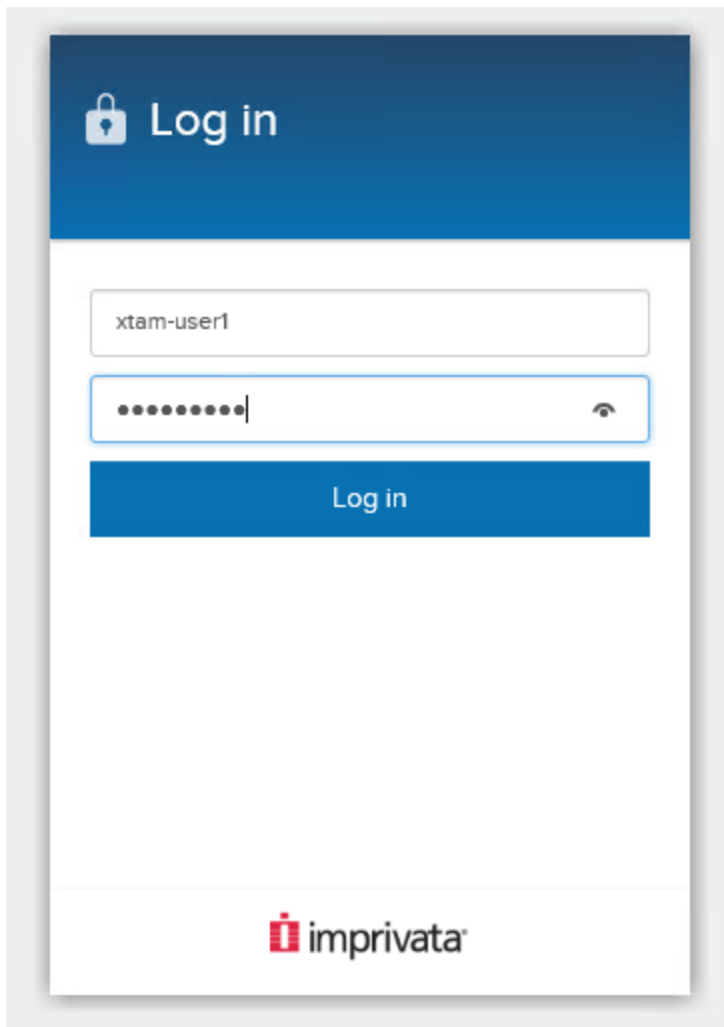
Deploy to All Users and Groups? ☒

9. Your new application will now be listed with the Deployment Status **Deployed**.

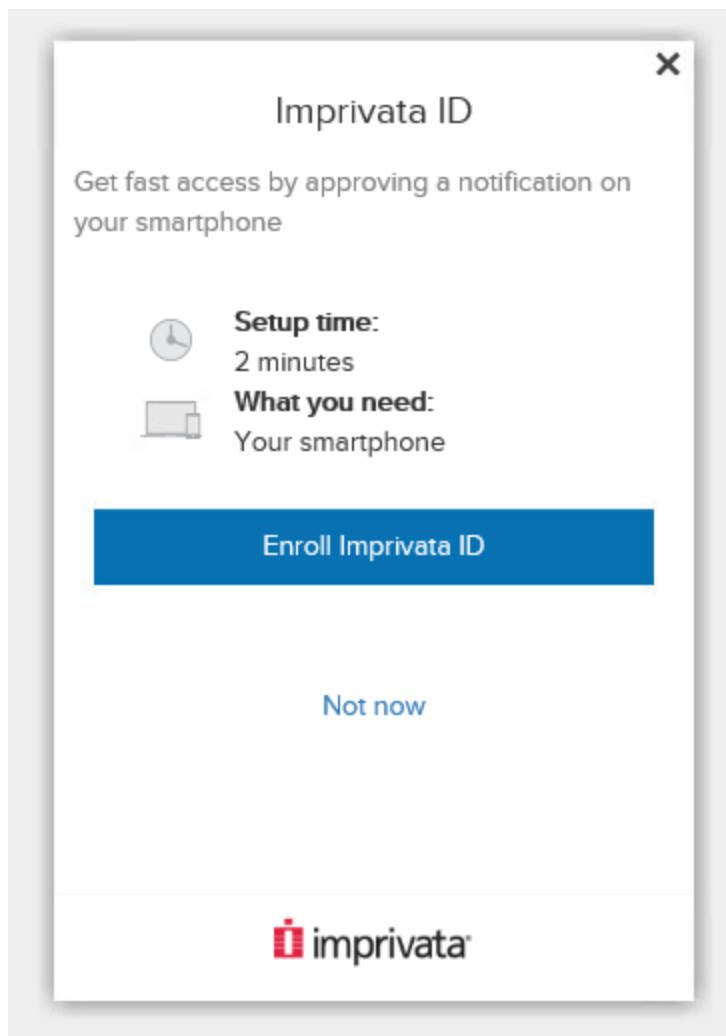
<input type="checkbox"/>	XTAM   SAML	<a href="#">Edit Profile</a>	<a href="#">Deployed</a>
--------------------------	-------------	------------------------------	--------------------------

### Step 4: Test your Login Integration

1. Return back to the PAM login page and click the red **EAM Login** button.
2. You will be directed to the Imprivata login page. Enter credentials that are both valid in Imprivata for the PAM deployed application and valid with PAM. Click the **Log in** button to continue.



3. (Optional) If Imprivata ID is available for your account, it may ask to authenticate with your Imprivata ID or you may be asked to enroll your device if you have not done so previously. Continue with Imprivata ID if required or choose the *Not now* option to do enrollment at a later date.



4. After the SAML authentication is successful, your browser will redirect back into PAM. You have now successfully authenticated into PAM using Imprivata EAM.

## Imprivata Manage EAM Admin AD

PAM supports secure management and rotation of the EAM AD accounts.

The following guide describes how to configure your PAM and EAM integration to rotate the EAM Admin AD account.

### Requirements




Before you begin your integration, be sure you meet the following pre-requisites:

- A working PAM deployment with the [Federated Sign-In](#) experience.
- The version of PAM must be **Release 2.3.202504\*** (April 2025) and beyond.
- Access to your existing *PAM host server*. You will need to update files and restart services.
- Access to your *EAM admin console* to retrieve the *AD account*.
- If Users are synced from *Active Directory* to *EAM*, then you must also integrate PAM with the same Active Directory.
- Ensure that Idaps is configured (otherwise it does not work).

If the AD account used for syncing *AD account* in EAM does not have sufficient rights, you will need to make this account a member of a security group that has sufficient rights (or add a [Shadow Account](#) with sufficient rights to the *EAM AD record Type* you created under **Step 2** point 2) to allow the execution of this task.


## Step 1: Retrieve the AD account from Imprivata EAM

The AD account used to sync AD users in EAM can be retrieved by navigating to User > Directories > Domain on the EAM admin page.

 Users Computers Applications Devices Reports   Log out svc\_onesign\_xena\_ad

**Directories - Edit xton.imp.eng**

Back to [directories](#) Cancel Save

Next >> Find Domain Users 

**xton.imp.eng** (MS Active Directory)

Host name  
xton-dc001.xton.imp.eng

NetBIOS name [Look-up](#)  
XTON

Username  
svc\_onesign\_xena\_ad

Password  
\*\*\*\*\*

☒ Use TLS for secure communication  
Directory server certificate [\(2 certificates\)](#)  
Choose File No file chosen Upload

☐ Validate stored domain credentials before authenticating  
Applies only to non-password authentication methods

**Kerberos authentication**  
Upload the keytab file if using smart cards with Active Directory certificates or authenticating with Kerberos.  

Keytab file [\(No keytab files\)](#)  
Choose File No file chosen Upload


**Password Policy**

You can implement password policy for Imprivata Domains. The domain password will be changed by writing directly to the domain's credential store at the specified interval.

Implement Password Change Policy? ☐

## Step 2: Configuring PAM record to rotate AD account on EAM

1. Add a new record with *Record Type EAM AD Account*. In case this record type is not visible, navigate to Administrator > **Record Types**, edit *EAM AD Account* and uncheck the hidden checkbox.

Record Types List							
Filtered out of 48 record types.				<input type="text" value="EAM"/>	Bulk Actions ▾	New Record Type	PDF 
Other	Record Type / Description	Parent Record Type	Session ...	Enabled	Personal ...	Vaults	Actions
<input type="checkbox"/>	<a href="#">EAM AD Account</a> <i>A record with EAM AD Admin information</i>			✓			<a href="#">Edit</a>

2. The EAM AD record type requires the following input fields:

- a. The script to update the EAM AD account passwords has to run on a windows host. The host information is provided in the following fields:
  - **Host for Remote Execution**
  - **Port**
- b. AD user details to login to the *Windows host*. This is also the AD account configured on EAM should be the same user as the *EAM AD account* used to sync AD as mentioned in **Step 1**:
  - **EAM AD Domain**
  - **User**
  - **Password**
- c. Details for PAM to authenticate to the EAM server:
  - **EAM Host** - EAM appliance FQDN
  - **EAM Authentication Domain**
  - **EAM User** - EAM admin console administrator user

- **EAM Password**

EAM AD Account.1

[Go to Parent](#)
[Execute... ▼](#)

EAM Remote Reset AD Admin

<b>Name</b>	EAM AD Account.1		
<b>Description</b>			
<b>Host for Remote Execution</b>	<input type="text" value="10.153.182.46"/>		
<b>Port</b>	<input type="text" value=""/>		
<b>EAM Host</b>	<input type="text" value="xena241-pam-01.xton.imp.eng"/>		
<b>EAM AD Domain</b>	<input type="text" value="xton.imp.eng"/>		
<b>User</b>	<input type="text" value="XTON\svc_onesign_xena_ad"/>		
<b>Password</b>	<input type="password" value="*****"/>		
<b>EAM Authentication Domain</b>	<input type="text" value="xton.imp.eng"/>		
<b>EAM User</b>	<input type="text" value="irudiuk"/>		
<b>EAM Password</b>	<input type="password" value="*****"/>		

[Record Type:](#) EAM AD Account

[ID:](#) i-LWZVOvcU0

[ID-CAP:](#) L-2V37VOPEYH4

[Reference Record:](#) AD user record.1

[Created By:](#) Service Administrator (pamadmin)

[/Local @ 03/27/2025 10:41](#)

[Last Action:](#) Execute @ 03/27/2025 17:14

[Last Success:](#) Execute @ 03/27/2025 17:14

[Job Queue:](#) (click to refresh)

### 3. Task to execute:

- The EAM AD Account can be reset by running the *EAM Remote Reset AD Admin* task.

## AD Password Reset task

Steps to configure the EAM AD Account task as a dependent task of an AD Password Reset task.

In most cases, Imprivata PAM will have a record to manage the AD account under a *Active Directory User* record. In order to trigger the *EAM AD account* reset on successful rotation of an AD account in PAM, follow the steps below.

1. Configure a record to rotate the *AD account* in PAM, using the same AD account as mentioned in **Step 1** by creating a new *Active Directory User* record.



## Record View

Root Folder / EAM records / AD user record.1


AD user record.1

[Go to Parent](#) [Execute...](#)

**Name** AD user record.1

**Description**




**User** XTON\svc\_onesign\_xena\_ad

**Password** \*\*\*\*\* 

[Record Type:](#) Active Directory User  
[ID:](#) i-IXVW7B6voqE  
[ID-CAP:](#) L-3W2ME2FWG2BFG  
[Created By:](#) Service Administrator (pamadmin)  
/Local @ 03/27/2025 10:42  
[Last Modified By:](#) Service Administrator  
(pamadmin) /Local @ 03/27/2025 17:14  
[JSON](#)

[Last Action:](#) Execute @ 03/27/2025 17:14  
[Last Success:](#) Execute @ 03/27/2025 17:14  
[Job Queue:](#) (click to refresh)

[Audit Log](#) [Change History](#) [Job History](#)

[Manage](#) [Edit](#)   

2. Create a custom *Password Reset LDAP* task and customize the task by updating the script to include a reference of the *EAM AD Account* task. Alternatively, you could also create a custom task and add it to the record.

## Edit Script

Root Folder / Scripts / Password Reset LDAP

Script Password Reset LDAP

Save

Factory Default

Cancel

Script Name

Password Reset LDAP

Description

Use to execute a password reset for a LDAP account.

Job Execution Strategy

LDAP

Custom Code (shell)

1

`\${ResetPassword}

2

#XTAM TRIGGER REF EAM Remote Reset AD Admin

[Script Variables and Placeholders](#)

3. Edit the *EAM AD Account* record by setting the above *Active Directory User* record as a reference record. The *User* and *Password* fields will be set from the referenced record.

When the *Password Reset LDAP* task associated to the *Active Directory User* record runs, PAM reads the script and upon successful completion of this task, will trigger the *EAM Remote Reset AD Admin* task that is referenced in this record to be scheduled and executed. In the Report Center > *Job History* report, the parent task as well as the referenced tasks will be visible.

Job History

The Job History report provides a list of all Jobs that have been scheduled or executed and their details.


Found 2 job records.


Time: Last Day ▾


State: Any ▾

Columns ▾

Bulk Actions ▾







Show 

50 ▾

 entries

Search:

CSV

PDF

TXT

XLSX



CSV Protected

PDF Protected

TXT Protected

XLSX Protected

Showing 1 to 2 of 2 entries

	Time		Type	User	Object	Account Updated	Host	Task	Processed	State	Message	
<input type="checkbox"/>	04/01/2025 09:05:09		On Demand	Service Service (pamservice) /Local	<a href="#">EAM AD Account.1</a>	XTON\svc_onesign_xena_ad	10.153.182.46	EAM Remote Reset AD Admin	04/01/2025 09:05:45	Completed	Script Executed by direct XTON\svc_onesign_xena_ad at 10.153.182.46 AD Admin credentials updated successfully XTAM Success Completed WriteProgress Executed by Node: wh-19-ira1-01:Worker, Version: 2.3.202503311111 Script execution verified by result code	<div>Details</div>
<input type="checkbox"/>	04/01/2025 09:04:49		On Demand	Service Administrator (pamadmin) /Local	<a href="#">AD user record.1</a>	XTON\svc_onesign_xena_ad		Password Reset LDAP	04/01/2025 09:05:09	Completed	Success Password reset AD Executed by Node: wh-19-ira1-01:Worker, Version: 2.3.202503311111 AD Verification Success by the result code	<div>Details</div>

First

Previous

1

Next

Last

## Integration with Microsoft Azure AD

PAM supports integration with [Microsoft's Azure AD cloud directory](#). The capabilities supported are user authorization (web and proxy), queries for search and group membership, and user profile attributes.

### Prerequisites

A working Imprivata PAM deployment with the [Federated Sign-In](#) experience.

The required Azure subscription plan and an account with access to create and configure necessary applications in the [Azure Portal](#).

### Steps to configure Azure

1. In the [Microsoft Azure portal](#), create a new or identify an existing application to be configured from App Registrations:

[Home](#) >

App registrations ✕ ...

[+ New registration](#) [Endpoints](#) [Troubleshooting](#) [Refresh](#) [Download](#) [Preview features](#) | [Got feedback?](#)

2. In the [Microsoft Azure portal](#), navigate to the application you created or wish to reuse and **copy** IDs from *Directory (tenant) ID* and *Application (client) ID* boxes. These will be required to configure `$PAM_HOME/web/conf/catalina.properties` later:

Home > App registrations >

Pam

Search

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Delete Endpoints Preview features

Essentials

Display name : Pam

Application (client) ID : [REDACTED]

Object ID : [REDACTED]

Directory (tenant) ID : [REDACTED]

Supported account types : My organization only

Client credentials : 0 certificate, 1 secret

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in L... : Pam

Get Started Documentation

### Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

3. From the overview page of the registered app, **Select Client credentials** and create a *new client secret*:

Home > App registrations >

Pam

Search

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Delete Endpoints Preview features

Essentials

Display name : Pam

Application (client) ID : [REDACTED]

Object ID : [REDACTED]

Directory (tenant) ID : [REDACTED]

Supported account types : My organization only

Client credentials : 0 certificate, 1 secret

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in L... : Pam

Get Started Documentation

### Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

Home > App registrations > Pam

Pam | Certificates & secrets

Search

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

Home > App registrations > Pam

**Pam | Certificates & secrets**

Search

Overview  
Quickstart  
Integration assistant

**Manage**  
Branding & properties  
Authentication  
**Certificates & secrets**  
Token configuration  
API permissions  
Expose an API  
App roles  
Owners  
Roles and administrators  
Manifest

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value
No client secrets have been created for this application.		

**Add a client secret**

Description: Pam Client Secret

Expires: Recommended: 6 months

**Add** Cancel

4. Once added, **copy** the Value of the secret as this will be used to configure later.

\$PAM\_HOME/web/conf/catalina.properties

**Note:** Client secret values cannot be viewed, except for immediately after creation. Be sure to save/copy the secret when created before leaving this page and progressing further.

Home > App registrations > Pam

**Pam | Certificates & secrets**

Search

Overview  
Quickstart  
Integration assistant

**Manage**  
Branding & properties  
Authentication  
**Certificates & secrets**  
Token configuration  
API permissions  
Expose an API  
App roles  
Owners  
Roles and administrators

Got feedback?

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

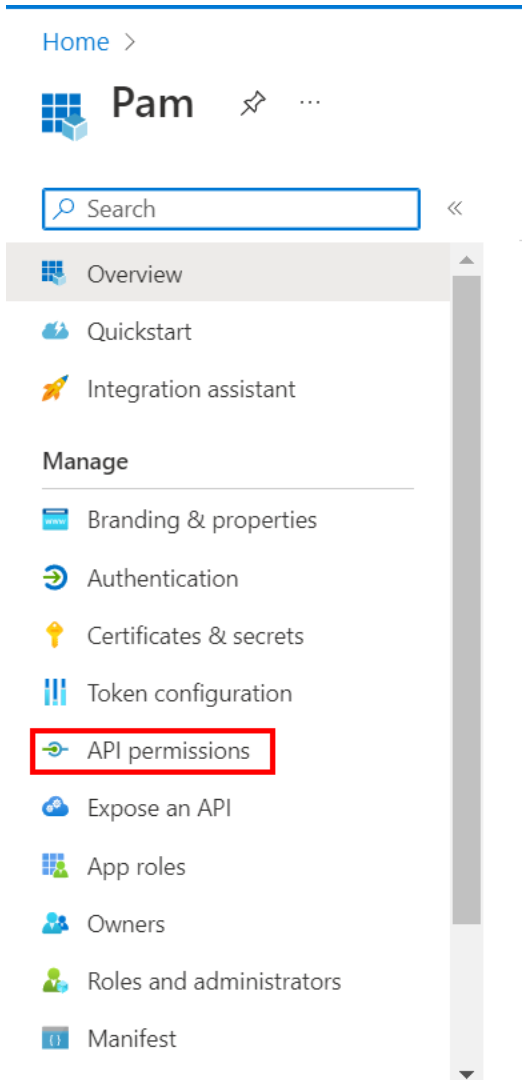
Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

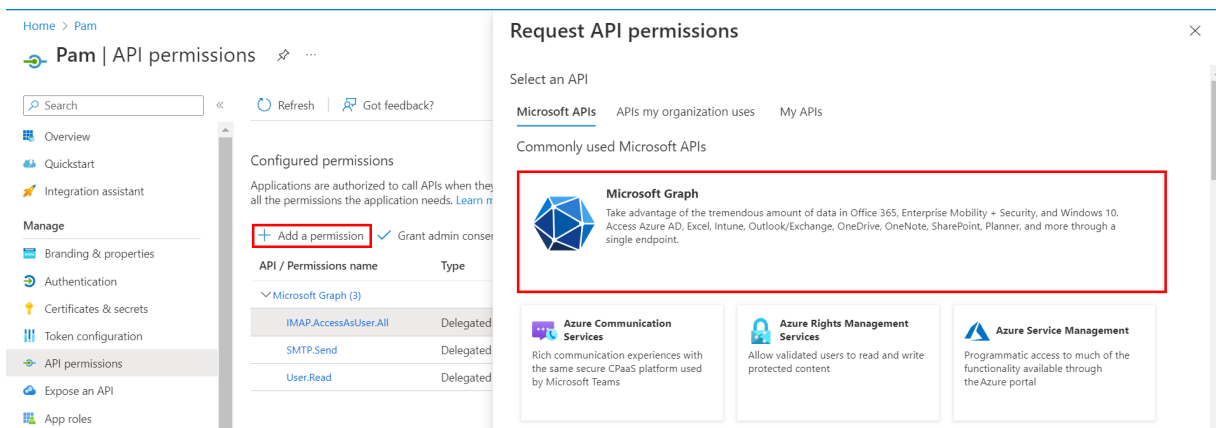
+ New client secret

Description	Expires	Value	Secret ID
Pam Client Secret	4/18/2023	[REDACTED]	[REDACTED]

5. Add permissions to the registered app by navigating to *API Permissions* and selecting **Add a permission**:



From the *Request API permissions* tab select **Microsoft Graph**:



6. Select **Application permissions** and include the following requirements from the list of permissions:


- Application.Read.All
- Directory.Read.All
- Group.Read.All


- GroupMember.Read.All
- User.Read.All

Request API permissions

×

← All APIs

 Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) 

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Request API permissions

×

Delegated permissions


Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

expand all

 application

×

Permission	Admin consent required
Application (1)	
<input checked="" type="checkbox"/> Application.Read.All ⓘ Read all applications	Yes
<input type="checkbox"/> Application.ReadWrite.All ⓘ Read and write all applications	Yes
<input type="checkbox"/> Application.ReadWrite.OwnedBy ⓘ Manage apps that this app creates or owns	Yes

> Policy

Request API permissions


×

your application needs to access the API as the signed-in user.

your application runs as a background service or daemon without a signed-in user.

Select permissions

expand all

 directory

×

Permission	Admin consent required
Directory (1)	
<input checked="" type="checkbox"/> Directory.Read.All ⓘ Read directory data	Yes

## Request API permissions



> Calls

### Group (1)

<input type="checkbox"/>	Group.Create ⓘ Create groups	Yes
<input checked="" type="checkbox"/>	Group.Read.All ⓘ Read all groups	Yes
<input type="checkbox"/>	Group.ReadWrite.All ⓘ Read and write all groups	Yes

### GroupMember (1)

<input checked="" type="checkbox"/>	GroupMember.Read.All ⓘ Read all group memberships	Yes
<input type="checkbox"/>	GroupMember.ReadWrite.All ⓘ Read and write all group memberships	Yes

> PrivilegedAccess

## Request API permissions



> User.Read

> UserShiftPreferences

### User (1)

<input type="checkbox"/>	User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage all users' identities	Yes
<input checked="" type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes
<input type="checkbox"/>	User.ReadBasic.All ⓘ Read all users' basic profiles	Yes
<input type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

7. Now select **Delegated permissions** and include the following requirement from the list of permissions:

- User.Read



## Request API permissions



[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

## Request API permissions



➤ UserNotification

➤ UserTimelineActivity

▼ User (1)

<input type="checkbox"/>	User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage user identities	Yes
<input checked="" type="checkbox"/>	User.Read ⓘ Sign in and read user profile	No
<input type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes

Once all necessary permissions are selected, click on **Add permissions**:

## Request API permissions



[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Start typing a permission to filter these results

Permission	Admin consent required
▼ OpenId permissions	
<input type="checkbox"/> email ⓘ View users' email address	No
<input type="checkbox"/> offline_access ⓘ	No

Add permissions

Discard

8. To enable Password Reset Task with Microsoft Entra ID, add the following permissions:

a. With a Shadow Account:

- i. Add User Administrator role to the user mapped to the Shadow Account record.
- ii. Add the following App permissions:
  - User.ReadWrite.All
  - Directory.AccessAsUser.All

MFA enabled [Shadow Accounts](#) are not supported. MFA must be disabled on Entra ID accounts that are to be used for Shadow Account functionality.

b. Without a Shadow Account:

- i. Add delegated permission:
  - Directory.AccessAsUser.All

To add support for self password reset from Management > My Profile page, include the following delegated permission:

- Directory.AccessAsUser.All

**Note: This step must be done by an admin user.**

9. The client app is now ready to be configured on PAM.

Home > Pam

Pam | API permissions

Search Refresh Got feedback?

+ Add a permission ✓ Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (6)				
Application.Read.All	Application	Read all applications	Yes	✓ Granted for
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for
Group.Read.All	Application	Read all groups	Yes	✓ Granted for
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for

10. Configure PAM: Edit `$PAM_HOME/web/conf/catalina.properties` and add the following properties with the values from Steps 2 & 4:

```
1 #Azure AD
2 azureAD[0].name={unique name}
3 azureAD[0].tenantID=00000000-0000-0000-0000-000000000000
4 azureAD[0].clientID=00000000-0000-0000-0000-000000000000
5 azureAD[0].secretValue={AES256},{73dMf0bkaTVHjM73pR6l4yHRzSU=},
  {vuErr/+HSD/RdKFqmtSi oQ==},
  {AgDH95leDji01KJ2jHnhV8FKU0g8xZW+N+RVbMKmGbLrraqkooqhi0y+nsH//7n0}
```

Note: In order to add multiple domains, copy and add the same properties and increment the index value.

```
1 #Azure AD
2 azureAD[1].name={unique name}
3 azureAD[1].tenantID=00000000-0000-0000-0000-0000000000010
4 azureAD[1].clientID=00000000-0000-0000-0000-000000000001
5 azureAD[1].secretValue={AES256},{73dMf0bkaTVHjM73pR6l4yHRzSU=},
  {vuErr/+HSD/RdKFqmtSi oQ==},
  {AgDH95leDji01KJ2jHnhV8FKU0g8xZW+N+RVbMKm3bLrraqkooqhi0y+nsH//7r0}
```

Note: For best practice it is recommended to encrypt your *Client Secret Value* by using the command below. This will generate your encrypted secret value which will be used in the `catalina.properties`. Using the default Client Secret Value which was copied in step 4, is supported as well in this field.

- a. For Windows, substitute your *Client Secret Value* with {SECRET VALUE} and issue this command from `$PAM_HOME`:

```
1 | bin\PamDirectory Encrypt {SECRET VALUE}
```

- b. For Unix, substitute your *Client Secret Value* with {SECRET VALUE} and issue this command from `$PAM_HOME`:

```
1 | bin/PamDirectory.sh Encrypt {SECRET VALUE}
```

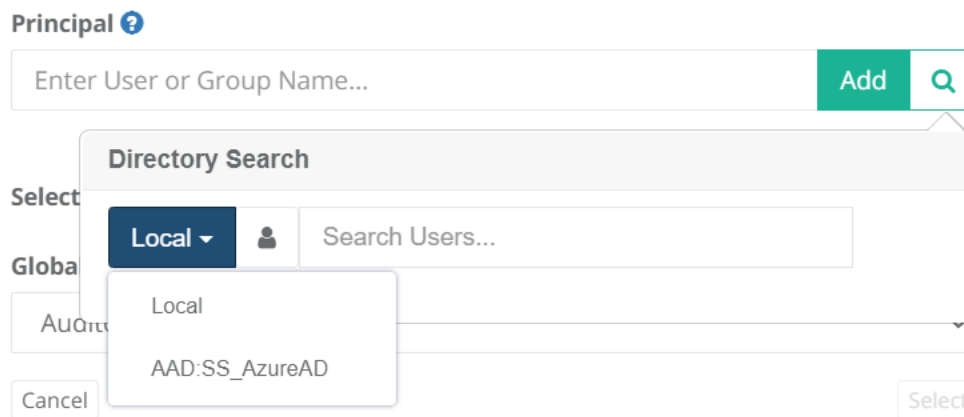
**Copy** the newly generated encrypted value and insert it to the property shown below:

```
1 | azureAD[0].secretValue={ENCRYPTED SECRET}
```

11. Restart **Pammanager** (Linux) or **pammanagement** service on Windows.

Test the integration: You should now see the unique name configured in `catalina.properties` **azureAD** `[1].name={unique name}` in the drop down when searching for AD users from the Global Users, Permissions or Local Groups > **Add member** popup.

## Grant Access



## Azure MSI

Azure Managed Identity, also known as Managed Service Identity (MSI), is a powerful feature that enhances the security of applications hosted on Azure.

System Assigned Managed Identities can now be discoverable within PAM's Directory mapping.

This will allow an Azure resource, with a System Assigned Managed Identity, to be assigned permission to PAM records and use an Azure JWT token for authentication.

## Requirements

- Microsoft Entra ID (Azure AD) integration configured with PAM using the following article, <https://help.xtontech.com/content/installation/integrations/azure-ad.htm>. Copy and save the Client ID of your App Registration which will be used later.

An Azure resource, such as a virtual machine, with a **System assigned** Managed Identity.

vm-pam787 | Identity ☆ ...  
Virtual machine

Search

Availability + scale

- Size
- Availability + scaling

Security

- Identity
- Microsoft Defender for Cloud

Backup + disaster recovery

- Backup
- Disaster recovery
- Restore point

Operations

System assigned User assigned

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID, so you don't have to store any credentials in code.

Save Discard Refresh Got feedback?

Status ⓘ

Off On

Object (principal) ID ⓘ

30eaf5d8-9e98-495a-9fdb-8d4b25335d8f

Permissions ⓘ

Azure role assignments

## PAM Configuration

- Following the linked Azure AD guide in the Requirements section of this article, the `catalina.properties` file will have the Microsoft Entra ID Registered App details to look similar as below.

- Entra ID Registered app details:

```
1 azureAD[0].name={unique name}
2 azureAD[0].tenantID=00000000-0000-0000-0000-000000000000
3 azureAD[0].clientID=00000000-0000-0000-0000-000000000000
4 azureAD[0].secretValue={AES256},{85dMf0bkaTVHjM27pR614yHRzSU=},
  {vuErr/+HSD/RdKFqmtSioQ==},
  {AgDH35leDji01KJ2jHnhV8FKU0g8xZW+N+RVbMKmGbLrraqkooqhi0y+nsH//7n0}
```

- Add the following property to enable searching for Managed Identities in PAM:

```
1 | xtam.landing.azure_auth=true
```

- If [MFA](#) (Multi Factor Authentication) is configured, ensure the MFA for the Managed Identity is set to **None** and individual MFA configuration is enabled. Please review this article for more information about this step: <https://help.xtontech.com/content/administrators-and-power-users/mfa-configuration/defining-mfa-per-user-or-group.htm>.
- Assign the required permission to the System assigned Managed Identity for the PAM records. From the *Permission* assignment module, use the directory search option and select the *Microsoft Entra ID (Azure AD)* choice that begins with 'AAD:'. Use the *Search Users...* option to find and assign the Managed

Identity.

The screenshot shows the 'Grant Access' interface. At the top, there's a 'Principal' section with a search bar labeled 'Enter User or Group Name...'. Below this, a 'Directory Search' dropdown is open, showing a search bar with the text 'AAD:Azure AD xtontech' and a list of results. The results include 'Local', 'AD', and 'AAD:Azure AD xtontech'. The 'AAD:Azure AD xtontech' option is highlighted. To the right of the search bar, there's an 'Add' button and a magnifying glass icon.

## Steps for Implementation

1. Generate a JWT token from the Azure VM directly using your System Assigned Managed Identity:  
`curl 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx' -H Metadata:true -s`

The *resource* is the value of the Client ID from the App Registration.

2. Authenticate with the Azure JWT token and retrieve a session cookie for PAM

```
1 | curl -k -X POST https://<PAM HOST>:6443/xtam/landing\  
2 | -H "Content-Type: application/x-www-form-urlencoded"\  
3 | -c pam.cookies \  
4 | -d "azure=$JWT" $@
```

3. Call the required PAM API. For this example, it is requesting an unlock of a PAM record:

```
1 | curl -k -X GET https://<PAM HOST>:6443/xtam/rest/record/unlock/<RECORD ID> \  
2 | -b pam.cookies $@
```

## Output

Without proper permissions granted to a PAM record you should expect an error response like shown below:

```
{  
  "error": "HTTP 401 Unauthorized"  
}
```

Permissions ?

Root Folder / AzureVM / Permissions

Permissions for AzureVM

Found 1 entries.

Bulk Actions

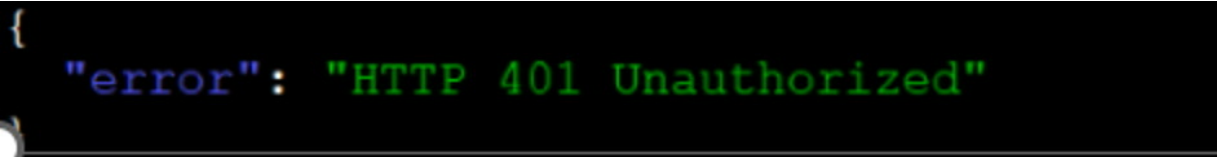
Grant Permission

Revoke Permission

Inherit from Parent

Access Report

Principal	Type	Record Control	Session Control	Task Control	Actions
<input type="checkbox"/> System Administrator (pamadmin) /Local	User	Owner	Connect (Optionally Recording with Session Events)	Manage	<div>Edit</div>



With proper permissions granted to a PAM record you should expect a successful response like shown below:

Permissions

Root Folder / AzureVM / Permissions

Permissions for AzureVM

Found 2 entries.

Bulk Actions

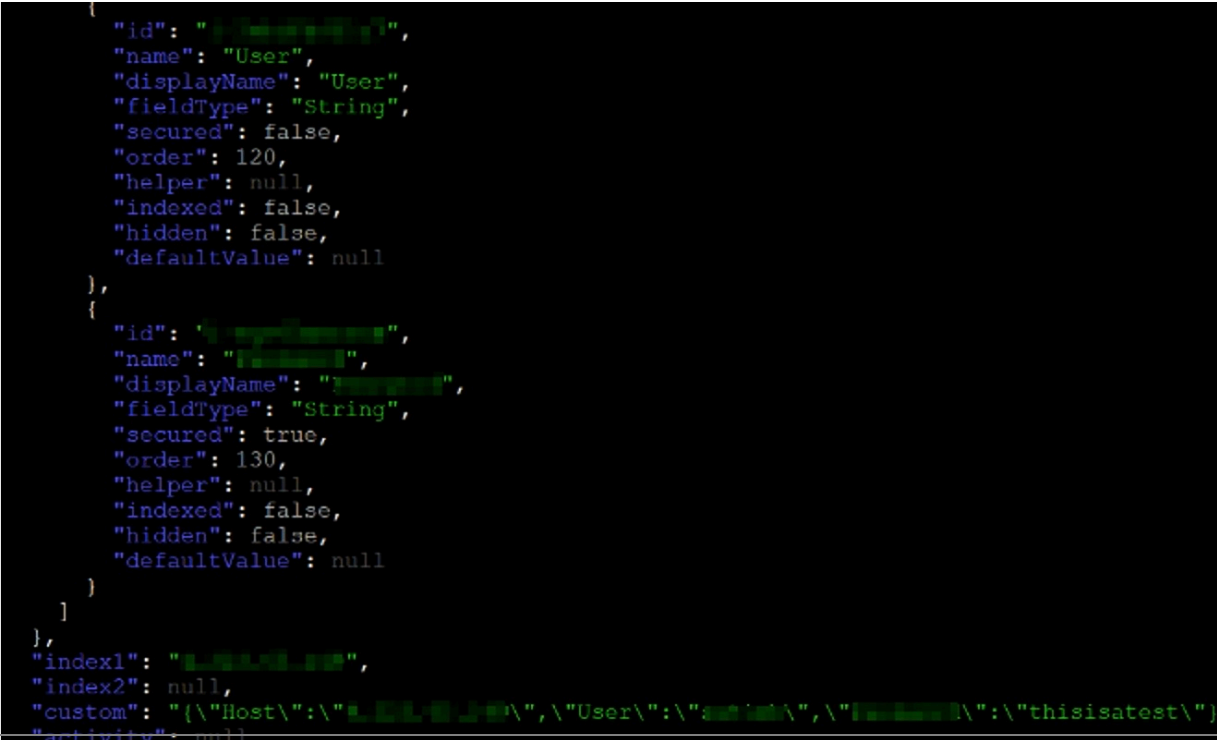
Grant Permission

Revoke Permission

Inherit from Parent

Access Report

Principal	Type	Record Control	Session Control	Task Control	Actions
<input type="checkbox"/> System Administrator (pamadmin) /Local	User	Owner	Connect (Optionally Recording with Session Events)	Manage	<div>Edit</div>
<input type="checkbox"/> alts Microsoft.Compute (vm) /SS_AzureAD	User	Unlock	None	None	<div>Edit</div>



# Integration with Duo Security

If you are already a user of Duo Security Multi-factor or Two-factor authentication and would like to configure PAM to use Duo, then please perform the following steps.

Please note that you will need to be able to access and modify files on the PAM host computer. Contact your PAM System Administrator for assistance.

Pre-requisite: PAM must be deployed with and configured to use its [Federated Sign-In](#) component in order to integrate with multi-factor authentication providers.

As of March 30, 2024, Duo Security will no longer support the traditional Duo Prompt and will only support Universal Prompt. This will require updating the [Federated Sign-In](#) component with the following instruction to [Migration to Federated Sign-in v6.5](#).

The PAM integration with Duo does not use the native Duo user directory; Duo Directory Sync is required. User accounts are first authenticated against PAM (using AD or Local users) and then the second authentication is done solely through Duo.

1. Log on to the PAM host computer.
2. Open the file `$PAM_HOME/web/conf/catalina.properties`
3. Uncomment the following line only when a single global MFA for the entire `$PAM_HOME` is desired:

```
1 | #cas.authn.mfa.globalProviderId=mfa-duo
```

If you wish to enable different MFA providers for individual users or group, please read [Configuring Different MFA Providers for Users or Groups](#) article for additional information.

4. Edit the following lines by replacing the values after "=" with your specific Duo configuration parameters:

To generate the required keys in Duo, please refer to this [Duo guide](#) which describes how to create the *Web SDK* application.

```
cas.authn.mfa.duo[0].duoSecretKey=duoSecretKey
cas.authn.mfa.duo[0].duoApplicationKey=duoApplicationKey|duoSecretKey
cas.authn.mfa.duo[0].duoIntegrationKey=duoIntegrationKey
cas.authn.mfa.duo[0].duoApiHost=duoApiHost
```



Use your same Duo Secret Key for both the `cas.authn.mfa.duo[0].duoSecretKey=` and `cas.authn.mfa.duo[0].duoApplicationKey=` parameters in the above configuration.

5. When complete, **save and close** this file.
6. Restart the service **PamManagement**.

## Adding Additional Duo Integrations

In the case where more than one Duo instance is to be used for MFA services, you may configure two or more unique Duo instances for your PAM deployment.

To add additional Duo instances:

1. Log on to PAM host computer.
2. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor.
3. Locate the section where you defined your first Duo integration and add this new section below it.  
**Change the values shown in red** to those specific to your second Duo instance:

```
# Duo Authenticator (Second instance config)
#cas.authn.mfa.globalProviderId=mfa-duo
cas.authn.mfa.duo[1].duoSecretKey=duoSecretKey
cas.authn.mfa.duo[1].rank=0
cas.authn.mfa.duo[1].duoApplicationKey=duoApplicationKey|duoSecretKey
cas.authn.mfa.duo[1].duoIntegrationKey=duoIntegrationKey
cas.authn.mfa.duo[1].duoApiHost=duoApiHost
cas.authn.mfa.duo[1].trustedDeviceEnabled=false
cas.authn.mfa.duo[1].id=mfa-duo-UniqueName
cas.authn.mfa.duo[1].name=PAMDuo
```

Please note that the index for your second configuration is [1] vs [0] for your first. If you have a third, the index for that would be [2], fourth would be [3], etc.

You must identify each Duo configuration with a unique ID defined by `cas.authn.mfa.duo[n].id=` and unique name `cas.authn.mfa.duo[n].name=`, as this is what will be displayed on the PAM's MFA page as the Provider and what you will select to assign users or groups to their Duo instance. The user assignment is created using the ID value of your configuration, so if you change the ID later, you must manually reassign all users and groups from the original provider ID to the new provider ID. Starting on [CAS v6.5](#) if customer has more than one instance of DUO this parameter should be unique.

4. When complete, **save and close** this file.
5. Restart the **PamManagement/pammanager** service.

6. When the service comes back online, login to the System and navigate to Administration > MFA. In the Provider dropdown menu, you will now see your two Duo instances that you can use to assign your users and groups to their respective Duo instance.

To enable the Duo Universal Prompt:

1. Log on to PAM host computer.
2. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor.
3. Locate the section where you defined your first Duo integration and add this new section below it:

```
1 #Duo Universal Prompt
2 cas.authn.mfa.duo[0].duoSecretKey=<Client secret>
3 cas.authn.mfa.duo[0].duoApplicationKey=
4 cas.authn.mfa.duo[0].duoIntegrationKey=<Client ID>
5 cas.authn.mfa.duo[0].duoApiHost=<API Hostname>
```

4. Locate these same named parameters from your original Duo integration section and comment out each of those 4 by placing a # before the start of each line. You will need to have these 4 new parameters enabled (not commented out) to support the Duo Universal Prompt.

Please note that the parameter `cas.authn.mfa.duo[0].duoApplicationKey=` is present and the value provided is blank. This is required to enable the Duo Universal Prompt.

## Integration with Okta SSO

If you are implementing or currently an Okta user, then the following article describes how to integrate the PAM login with Okta SSO.

This SAML integration currently supports the following features:

- SP-initiated SSO
- IdP-initiated SSO

Before you begin, be sure you met the following pre-requisites.

### Pre-requisites

- A working PAM deployment with the [Federated Sign-In](#) experience.
- Access to the PAM host server to make application changes.
- An Okta Administrator account that can add Applications and basic Okta Administrative knowledge.
- PAM does not support the use of native Okta accounts for login. Accounts have to originate in Active Directory and be synced to Okta in order to be used for PAM authentication.

## Add to Okta Application

This section will describe how to add the PAM Application in your company's Okta tenant.

1. Login to Okta with an Administrator account.
2. Navigate to the Applications section and click the **Browse App Catalog**.
3. In the Search for an application box, enter *Imprivata Priveleged Access Managment*. Click the **Add** button next to the application name.



# Imprivata Privileged Access Management

Overview Capabilities

Add

## Categories

[Security](#)

## Capabilities

[SAML](#)

## Support

[support@imprivata.com](mailto:support@imprivata.com)

## Last updated

2021-12-16T09:24:04

## Overview

Imprivata Privileged Access Management, a key component of the Imprivata digital identity framework, is a comprehensive, easy-to-use privileged access management solution that helps customers improve security by protecting privileged accounts from unauthorized access. With single sign-on, Okta allows organizations to have a more consistent user experience when working within Imprivata Privileged Access Management throughout their lifecycle.

4. In "General Settings" click **Done**.


## Configuring PAM for your Okta SSO

This section will describe how to configure PAM to support your Okta SSO login.


We will be taking information from your PAM Okta Application and using them in the PAM configuration, so be sure you have access to both.


1. In tab "Assignments" assign rights to users. Click **Assign** and choice peoples or groups.

[← Back to Applications](#)



Active

 [View Logs](#)

 [Monitor Imports](#)

General

Sign On

Mobile

Import

Assignments

Assign

Convert assignments

Search...

People

Assign to People

Assign to Groups

Groups

Type

01101110

01101111

01101100

01101000


01101001


01101110

01100111

No users found

REPORTS

 [Current Assignments](#)

 [Recent Unassignments](#)

SELF SERVICE

You need to enable self service for org managed apps before you can use self service for this app.

[Go to self service settings](#)

Requests

Disabled

Approval

-

Edit

© 2021 Okta, Inc.

[Privacy](#)

Version 2021.12.0 C

OK12 Cell (US)

[Status site](#)

[Download Okta Plugin](#)

[Feedback](#)


2. In tab "Sign On" press "Edit" in section "Advanced Sign-on Settings" enter your ACS URL and Audience URI values into the corresponding fields.
- a. ACS URL - <URL to your host>/cas/login?client\_name=<SSO provider>,  
ex. [https://pam.company.com:6443/cas/login?client\\_name=Okta](https://pam.company.com:6443/cas/login?client_name=Okta)

b. Audience URI - unique identifier, ex. urn:mace:saml:pac4j.org

Disable Force Authentication ☒

Never prompt user to re-authenticate.

Preview SAML



**SAML 2.0** is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

### Advanced Sign-on Settings

These fields may be required for a Imprivata Privileged Access Management proprietary sign-on option or general setting.

ACS URL


Please enter your ACS URL. Refer to the Setup Instructions to obtain this value.

Audience URI

Please enter your audience URI. Refer to the Setup Instructions to obtain this value.

### Credentials Details

Application username format

Okta username 

3. End pressing **Save**.

4. In point *SAML Signing Certificates* click **Actions**, choose *View IdP metadata* and **copy** the opened URL.

© 2025 Imprivata, Inc. All Rights Reserved.

| 175

## SAML Signing Certificates

Generate new certificate

Type	Created	Expires	Status	Actions
SHA-2	Today	Jul 2032	Active	Actions ▾

Sign On Policy

Add Rule

Priority	Rule Name	Status	Actions
1	Default sign on rule	Active	Not editable
CONDITIONS		ACTIONS	
👤	User assigned this app	🔑	Allow access
📍	Anywhere		
📱	Any client		
🛡️	Any		

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

View SAML setup instructions

Sign On Policy

A sign on policy is a set of rules that determine how users access this application. For example, you can deny access when a specific user or group of users is off network.

Every application starts with a default rule that allows access to anyone assigned the app from anywhere.

Rule Priority

You can determine rule precedence by setting the priority number. For example, a rule with a priority value of 1 has first priority and takes precedence over all other rules.

5. On the PAM host computer, open the following file in a text editor `$PAM_HOME/web/-conf/catalina.properties` locate the section labeled **# CAS** and add the following lines:

```
1 cas.authn.pac4j.saml[0].clientName=Okta
2 cas.authn.pac4j.saml[0].keystorePassword={password}
3 cas.authn.pac4j.saml[0].privateKeyPassword={password}
4 cas.authn.pac4j.saml[0].serviceProviderEntityId=urn:mace:saml:pac4j.org
5 cas.authn.pac4j.saml[0].serviceProviderMetadataPath={okta.xml}
6 cas.authn.pac4j.saml[0].keystorePath={samlKeystore.jks}
7 cas.authn.pac4j.saml[0].identityProviderMetadataPath={path}
```

In the lines above, the following **{placeholders}** need to be updated using your own values explained here:

- `cas.authn.pac4j.saml[0].clientName={Okta}` - name SSO provider, it must match with item 2a.
- `cas.authn.pac4j.saml[0].keystorePassword={testPassword}` - Create an alphanumeric password. Any value you want to enter.
- `cas.authn.pac4j.saml[0].privateKeyPassword={privatePassword}` - Create an alphanumeric password. Any value you want to enter.
- `cas.authn.pac4j.saml[0].serviceProviderEntityId={urn:mace:saml:pac4j.org}` - audience URI, it must match with item 2b.
- `cas.authn.pac4j.saml[0].serviceProviderMetadataPath={okta.xml}` - The full path and file name of the `okta.xml` file. For example, `C:/pam/content/keys/okta.xml` (use forward slashes not backslashes)
- `cas.authn.pac4j.saml[0].keystorePath={samlKeystore.jks}` - Define a path and name for the PAM auto-generated key. For example, `C:/pam/content/keys/samlKeystore.jks` (use forward slashes not backslashes)
- `cas.authn.pac4j.saml[0].identityProviderMetadataPath={path}` - Copy and paste the full URL from your Identity Provider Metadata used in step (4). For example, [https://subDomain.okta.com/app/\[externalKey\]/sso/saml/metadata](https://subDomain.okta.com/app/[externalKey]/sso/saml/metadata).

- When finished, **save and close** this file.
- Restart the **PamManagement** (Windows) or the **pammanager** (Linux) service.
- When the service is fully restarted, open your browser and navigate to the PAM login page. Use the new option **Login** using Okta located on the bottom right side of the page.

## Integration with Shibboleth SSO

This guide describes how to configure integration between Imprivata PAM and Shibboleth Identity Provider to provide SAML authentication.

We currently support integration with V4 of the Shibboleth Identity Provider.

## Requirements

Before you begin your integration, be sure you meet the following pre-requisites:

- A working PAM deployment with the [Federated Sign-In experience](#).
- Access to your existing PAM host server. You will need to update files and restart services.
- Access to your host running Shibboleth in order to configure your authentication services.
- Shibboleth administrator to configure required settings (metadata files, AD integration) on Shibboleth.

## Step 1: Generate Service Provider Metadata file for PAM

1. Login to the PAM host server and open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor.

In this file, locate the section that begins with `#CAS` add the following new parameters:

```
1 #Shibboleth SSO
2 cas.authn.pac4j.saml[0].clientName=ShibbolethSSO
3 cas.authn.pac4j.saml[0].keystorePassword={password}
4 cas.authn.pac4j.saml[0].privateKeyPassword={password}
5 cas.authn.pac4j.saml[0].serviceProviderEntityId={pam_managed_path}
6 cas.authn.pac4j.saml[0].serviceProviderMetadataPath={shibbolethssso.xml}
7 cas.authn.pac4j.saml[0].keystorePath={samlKeystoreshibbolethSSO.jks}
8 cas.authn.pac4j.saml[0].identityProviderMetadataPath={IDP Metadata URL}
9 cas.authn.pac4j.saml[0].maximumAuthenticationLifetime=2073600
```

2. In the lines referenced above, the `{placeholders}` should be updated to reflect your specific values as explained here.

Save and close the file when you are finished.

- `cas.authn.pac4j.saml[0].keystorePassword={password}` - Create an alphanumeric password. Any value you want to enter.
  - `cas.authn.pac4j.saml[0].privateKeyPassword={password}` - Create an alphanumeric password. Any value you want to enter.
  - `cas.authn.pac4j.saml[0].serviceProviderEntityId=https://pam.yourorg.com/xtam/` - Replace this placeholder URL with your full https PAM login page URL ending with `/xtam/`.
  - `cas.authn.pac4j.saml[0].serviceProviderMetadataPath={shibbolethssso.xml}` - The full path and file name of the `shibbolethssso.xml` file that will be created after a PAM service restart later in this guide. For example, `C:/pam/content/keys/shibbolethssso.xml` (use forward slashes not backslashes).
  - `cas.authn.pac4j.saml[0].keystorePath={samlKeystoreshibbolethSSO.jks}` - Define a path and name for the PAM auto-generated key that will be created after a PAM service restart later in this guide. For example, `C:/pam/content/keys/samlKeystoreshibbolethSSO.jks` (use forward slashes not backslashes).
  - `cas.authn.pac4j.saml[0].identityProviderMetadataPath={IDP Metadata URL from step 1}` – This will be the full URL of the IDP Metadata URL from the Shibboleth Application temporarily saved to a file in the previous step.
3. Restart the PAM service **PamManagement** (Windows) or **pammanager** (Linux).
  4. After the restart is complete, navigate to the PAM login page. Confirm that both files, `samlKeystoreshibbolethSSO.jks` and `shibbolethssso.xml`, were created in the location you defined.

## Step 2. Configure your Shibboleth Identity Provider for Integration

Shibboleth supports multiple features which are detailed in

<https://shibboleth.atlassian.net/wiki/spaces/IDP4/pages/1265631633/ConfigurationFileSummary>.

The main configuration is:



1. Configuring the Service Provider metadata (reference `shibbolethssso.xml` from previous step).
2. Setup relaying parties in the `relaying-party.xml`. Reference article <https://shibboleth.atlassian.net/wiki/spaces/IDP4/pages/1265631678/RelyingPartyConfiguration>

A sample entry for static relaying party configuration will look like:

```
1 <bean parent="RelyingPartyByName"
2   c:relyingPartyIds="https://pam.some.org:6443/xtam/">
3   <property name="profileConfigurations">
4     <list>
5       <bean parent="SAML2.SSO"
6         p:encryptAssertions="false"
7         p:nameIDFormatPrecedence="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified" />
8     </list>
9   </property>
10 </bean>
```

Where `c:relyingPartyIds` is the PAM managed path url.

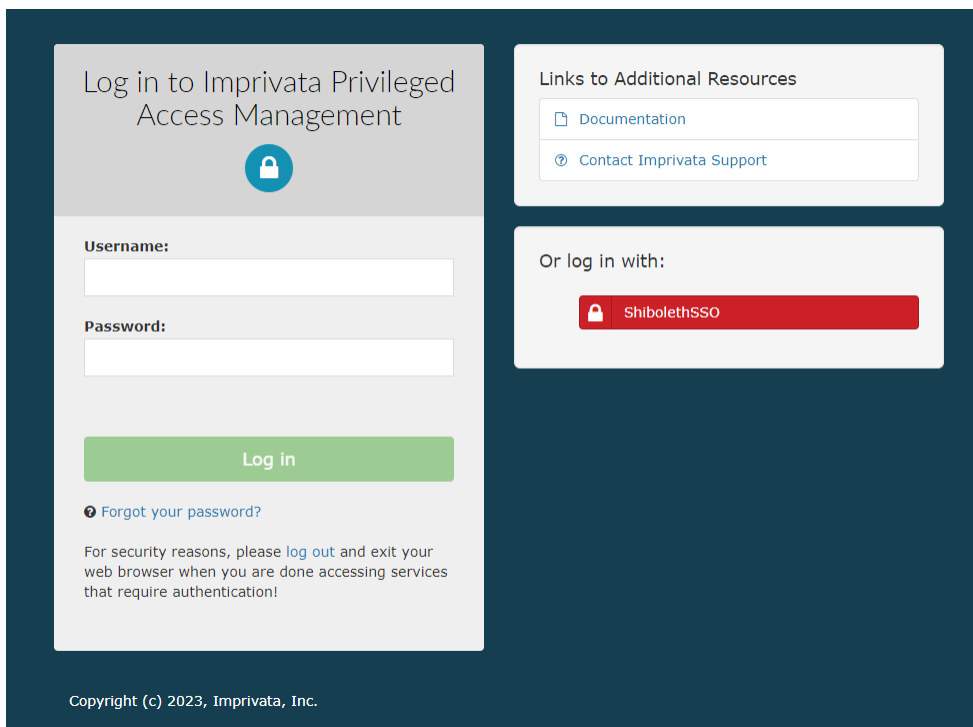
3. Update the `saml-nameid.xml` with the source id's in case of integration with Active Directory. Reference article for *Name id config* <https://shibboleth.atlassian.net/wiki/spaces/IDP4/pages/1265631671/NameIDGenerationConfiguration>
4. A sample entry in case Shibboleth is integrated with Active Directory. The `p:attributeSourceIds` would hold **UserPrincipalName**, **uid** or any property name that identifies a user

```
1 <bean parent="shibboleth.SAML2AttributeSourcedGenerator"
2   p:omitQualifiers="true"
3   p:format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
4   p:attributeSourceIds="#{ {'userPrincipalName'} }" />
```

## Testing the integration

When the service is fully restarted, open your browser, and navigate to the PAM login page.

Use the new Login using Shibboleth button located on the right side of the page.



## Integration with PingIdentity SSO

This guide describes how to configure integration between PAM and PingIdentity to provide SAML authentication.

### Requirements

Before you begin your integration, be sure you meet the following pre-requisites:

- A working PAM deployment with the [Federated Sign-In experience](#).
- Access to your existing PAM host server. You will need to update files and restart services.
- Access to your PingIdentity web portal to configure your authentication services.
- An identical user must be created as a PAM Local User for every account that will login using PingIdentity.

### Step 1: Configure your PingIdentity SAML Application for Integration

1. Login to your PingIdentity Web Console using an Administrator account.
2. Navigate to the **Administrator's** Environment.
3. Click on the Connections > **Applications** menu.
4. On the Applications page, click the + button to add a new application.
  - For this new Application, add a descriptive **Application Name** like *Imprivata PAM*.
  - For the Application Type, select *SAML Application*.

Finally, click the **Configure** button.

Add Application

**Name and Describe Application**

Create a name and description for this application that will make it easy to identify.

Application Name \*


ImprivataPAM

Description


Icon

Max Size 1.0 MB


**Choose Application Type**



SAML Application



OIDC Web App



Native

**SAML Application**

Some additional configuration is required to create a SAML application.

Connection Type

SAML

Configure

Cancel

On the SAML Configuration page, choose the **Manually Enter** option and input your values as described here. Replace <https://pam.yourorg.com> in our examples with your PAM URL and click **Save** when complete.

- ACS URLs: [https://pam.yourorg.com/cas/login?client\\_name=PingIdentitySSO](https://pam.yourorg.com/cas/login?client_name=PingIdentitySSO)
- Entity ID: <https://pam.yourorg.com/xtam/>

© 2025 Imprivata, Inc. All Rights Reserved.

| 181

☐ Add Application

## SAML Configuration

Provide Application Metadata

☐ Import Metadata ☐ Import From URL ☒ Manually Enter

ACS URLs \*

[https://pam.yourorg.com/cas/login?client\\_name=PingIde ...](https://pam.yourorg.com/cas/login?client_name=PingIde...)

[+ Add](#)

Entity ID \*

<https://pam.yourorg.com/xtam/>

5. After it is saved, switch to the *Configuration* tab of this new Application and copy the value from the **IDP Metadata URL** to a temporary file. We will need this value in the next step.

ImprivataPAM

Client ID: a id

Profile

Configuration

Attribute Mappings

Policies

Access

Connection Details

Download Metadata

Download Signing Certificate

Issuer ID

https://auth.pingon

16

Single Logout Service

https://auth.pingon

10

Single Signon Service

https://auth.pingo

0

IDP Metadata URL

https://auth.pingoi

9e-

Initiate Single Sign-On URL

https://auth.pingon

- Switch to the Attribute Mappings tab and click the **Edit** button. On the Edit Attribute Mappings page, for the OUTGOING VALUE select **Username** from the dropdown menu. If PAM is configured for UPN, select the Email Address option instead. Click **Save** when complete.

Please note that each account's Username or Email Address should exist in PAM as a valid user.

ImprivataPAM

Client ID: a d

Profile

Configuration

Attribute Mappings

Policies

Access

!

If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

APPLICATION ATTRIBUTE

OUTGOING VALUE

saml\_subject

←

Username

REQUIRED

Test Output

- Optionally, if MFA is required, switch to the Policies tab and click the **Edit** button. On the *Edit Policies* page, select the MFA policy to apply and click **Save** when complete.
- Finally, use the UI control to **Enable** this application for use.

ImprivataPAM

Client ID: a d

Profile

Configuration

Attribute Mappings

Policies

Access

You don't have any policies added.

## Step 2: Configure PAM for PingIdentity Integration

- Login to the PAM host server and open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor

In this file, locate the section that begins with `# CAS` add the following new parameters:

`# PingIdentity SSO SAML`

`cas.authn.pac4j.saml[0].clientName=PingIdentitySSO`

`cas.authn.pac4j.saml[0].keystorePassword={password}`

`cas.authn.pac4j.saml[0].privateKeyPassword={password}`

`cas.authn.pac4j.saml[0].serviceProviderEntityId={managed_path}`

`cas.authn.pac4j.saml[0].serviceProviderMetadataPath={pingidentitysso.xml}`

`cas.authn.pac4j.saml[0].keystorePath={samlKeystorePingIdentitySSO.jks}`


`cas.authn.pac4j.saml[0].identityProviderMetadataPath={IDP Metadata URL from step 1}`

`cas.authn.pac4j.saml[0].maximumAuthenticationLifetime=2073600`

- In the lines referenced above, the `{placeholders}` should be updated to reflect your specific values as explained here. Save and close the file when you are finished.

- `cas.authn.pac4j.saml[0].keystorePassword={password}` - Create an alphanumeric password. Any value you want to enter.
  - `cas.authn.pac4j.saml[0].privateKeyPassword={password}` - Create an alphanumeric password. Any value you want to enter.
  - `cas.authn.pac4j.saml[0].serviceProviderEntityId=https://pam.yourorg.com/xtam/` - Replace this placeholder URL with your full https PAM login page URL ending with /xtam/.
  - `cas.authn.pac4j.saml[0].serviceProviderMetadataPath={pingidentitysso.xml}` - The full path and file name of the pingidentitysso.xml file that will be created after a PAM service restart later in this guide. For example, `C:/pam/content/keys/pingidentity.xml` (use forward slashes not backslashes).
  - `cas.authn.pac4j.saml[0].keystorePath={samlKeystorePingIdentitySSO.jks}` - Define a path and name for the PAM auto-generated key that will be created after a PAM service restart later in this guide. For example, `C:/pam/content/keys/samlKeystorePingIdentitySSO.jks` (use forward slashes not backslashes).
  - `cas.authn.pac4j.saml[0].identityProviderMetadataPath={IDP Metadata URL from step 1}` – This will be the full URL of the IDP Metadata URL from the PingIdentity Application temporarily saved to a file in the previous step. It will look similar to this example:  
<https://auth.pingone.com/GUID/saml20/metadata/GUID>
3. Restart the PAM service **PamManagement** (Windows) or **pammanager** (Linux).
  4. After the restart is complete, navigate to the PAM login page. Confirm that both files, `samlKeystorePingIdentitySSO.jks` and `pingidentitysso.xml`, were created in the location you defined.
  5. Now you can try your PingIdentity login by clicking the red **PingIdentitySSO** button on the PAM login page.

Log in to Imprivata Privileged Access Management



**Username:**

**Password:**

**Log in**

[? Forgot your password?](#)


For security reasons, please [log out](#) and exit your web browser when you are done accessing services that require authentication!

**Links to Additional Resources**

[Documentation](#)

[? Contact Imprivata Support](#)

**Or log in with:**

 **PingIdentitySSO**

# Considerations for SSO Users

Considerations for users logged in to the system using SSO Identity Providers.

- When integrating with SSO Identity Provider PAM expects integration with Active Directory that syncs with SSO IdP independently. PAM uses SSO IdP for authentication (including MFA) and login authorization (following SSO IdP rules). PAM uses AD to resolve group membership when permissions or workflow activities are granted to AD groups.
- All proxies that allow users to connect using native clients authenticate using Active Directory and PAM managed MFA (TOTP, Duo, Radius or even PAM native one).
- Some of the proxies (RDP, SQL but not SSH or WEB Sessions) require password hash stored in PAM. It is done automatically when users login to PAM directly. However, for SSO login when PAM does not know user passwords the only way to support this option is to let PAM to know the password (there is button Re-Enable RDP Proxy in the Properties of the user profile).
- For pass-through access (\$login in the user field) both proxy and WEB access pass the user password entered on the login form to the upstream endpoint. With SSO login, PAM does not know the user password so it cannot pass it through to the endpoint server. The solution is to Re-Enable RDP Proxy in the Properties of the user profile. When password is changed, it should be Re-Enabled again using the same strategy.

## Integration with Microsoft Azure AD Authenticator Push and OTP

The PAM server supports integration with Microsoft Azure AD Authenticator to provide second factor authentication through the use of the Microsoft Authenticator app (token and push).

### Functionality

- MS Azure AD MFA for the access to the Imprivata PAM WEB GUI is implemented by SSO integration of login screen with [Azure AD portal using SAML protocol](#).
- The following guide describes the configuration to enable Azure AD MFA for SSH, RDP Proxy connections made using native clients as well as for Workflow Requests requiring MFA configuration for requested actions.

### Requirements

Before you begin your integration, be sure you meet the following pre-requisites:

- A working Imprivata PAM deployment with the Federated Sign-In experience.
- PAM system configured to use [MFA for individual users or groups](#).
- If Users are created and managed in Azure AD, then a matching user must also exist in the back end AD or be created as a PAM Local User.



- If Users are synced from Active Directory to Azure AD, then you must also integrate PAM with the same [Active Directory](#).
- Users must already enroll their device prior to authenticating with PAM. Device enrollment is not currently supported using PAM.

To enable Azure AD MFA for a specific user or group perform the following steps

- Optionally: For the deployments using **sAMAccountName** (user vs user@domain.com) user naming convention, define MS Azure AD domain in the global parameter Administration > Settings > Parameters > Drivers > **Azure AD MFA Domain**.
- Assign mfa-azure ad MFA provider to a user or a group that require to use it.

## Configuring Azure

### *Register a New App*

1. Login to your Azure Portal (<https://portal.azure.com>), navigate to *Azure Active Directory* and select **App Registrations**.

2. Select **+ New Registration** and give it a meaningful name like “*pam-mfa*” or similar, press **Register**.

Microsoft Azure

Search resources, services, and docs (G+/)

Home >

App registrations

...

Azure Active Directory

Overview

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Custom security attributes (Preview)

Licenses

Azure AD Connect

Custom domain names

Mobile, MDM and MAM

<<

+ New registration

Endpoints

Troubleshooting

Refresh

Download

Preview

All applications

Owned applications

Deleted applications

Start typing a display name or application (client) ID to filter these r...

Add filters

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > >

## Register an application

\*

Name

The user-facing display name for this application (this can be changed later).

pam-mfa

✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only ( only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform

▼

e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- Retrieve the *Application (client) ID* from app registration overview page to use it in your PAM configuration.

Search (Cmd+/) <<

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

## Essentials

Display name	: pam-mfa	Client credentials
Application (client) ID	: 4[redacted]e	Redirect URIs
Object ID	: 1[redacted]325	Application ID URI
Directory (tenant) ID	: 3[redacted]42	Managed application
Supported account types : <a href="#">My organization only</a>		

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL)


Get Started Documentation

## Build your application with the Microsoft


The Microsoft identity platform is an authentication service, open-source libraries, and application standards-based authentication solutions, access and protect APIs, and add sign-in for your application

## Create an Access Policy

1. In your Azure Portal navigate to *Azure Active Directory*, then *Security* and finally **Conditional Access**.



# Security | Getting started

 Got feedback?

Getting started

Protect

Conditional Access

Identity Protection

Security Center

Verifiable credentials (Preview)

Manage

Identity Secure Score

Named locations

Authentication methods

Multifactor authentication

Certificate authorities


Report

Risky users

Risky workload identities (preview)

Risky sign-ins


Risk detections



## Documentation

Azure Active Directory offers a range of security features to pro

- [Azure AD Conditional Access](#)
- [Azure AD Identity Protection](#)
- [Azure Security Center](#)
- [Identity Secure Score](#)
- [Named locations](#)
- [Authentication methods](#)
- [Multifactor authentication](#)



## Security guidance

For a strong security posture, we recommend the following:

- [5 steps to secure your identity infrastructure](#)
- [Azure AD Password Guidance](#)
- [Azure AD Data Security Whitepaper](#)
- [How Password Hash Sync \(PHS\) works](#)

2. Select + **New policy** to create your new policy.

« [+ New policy](#) [+ New policy from template \(Preview\)](#) [What If](#) [Refresh](#)

[Overview \(Preview\)](#)

[Policies](#)

[Insights and reporting](#)

[Diagnose and solve problems](#)

**Manage**

[Named locations](#)

[Custom controls \(Preview\)](#)

[Terms of use](#)

[VPN connectivity](#)

[Authentication context \(Preview\)](#)

[Classic policies](#)

**Monitoring**

[Sign-in logs](#)

[Audit logs](#)

**Troubleshooting + Support**

[Virtual assistant \(Preview\)](#)

[New support request](#)

[Add filters](#)

3. Give your new policy some meaningful name like “pam-mfa” or similar.
4. Select affected by policy users/groups in **Users or workload identities**, for example *All users*:

## New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

pam-mfa



### Assignments

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

### Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

[Learn more](#)

What does this policy apply to?

Users and groups



Include

Exclude

☐ None

☒ All users

☐ Select users and groups

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☐ Users and groups



Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

Enable policy

Report-only

On

Off

Create

5. In the *Cloud apps or actions* select your newly created app registration:

## New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

pam-mfa



### Assignments

Users or workload identities ⓘ

[All users](#)

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

[0 conditions selected](#)

### Access controls

Grant ⓘ

[0 controls selected](#)

Session ⓘ

[0 controls selected](#)

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps



**Include**

Exclude

☐ None

☒ All cloud apps

☐ Select apps



Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal.

Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected.

Enable policy

Report-only

On

Off

Create

6. In the *Grant* section select **Require multi-factor authentication**



## New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

pam-mfa



### Assignments

Users or workload identities ⓘ

[All users](#)

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

0 conditions selected

### Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only

On

Off

Create

## Grant



Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multifactor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ  
[See list of approved client apps](#)

☐ Require app protection policy ⓘ  
[See list of policy protected client apps](#)

☐ Require password change ⓘ

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

Select

7. Ensure that **Enable policy** set to **On** and click **Create**. The result will be similar to this:

# New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

pam-mfa



## Assignments

Users or workload identities ⓘ

[All users](#)

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

[0 conditions selected](#)

## Access controls

Grant ⓘ

Enable policy

Report-only

On

Off



Don't lock yourself out! We recommend applying a policy to a small set of users first required. Please review the affected users and apps.



Exclude current user, | :onmicrosoft.com, from this policy.



I understand that my account will be impacted by this policy. Proceed an

Create

Overview (Preview) Policies Insights and reporting Diagnose and solve problems

Manage

Named locations Custom controls (Preview)

New policy New policy from template (Preview) What If Refresh Got feedback?

Search policies Add filters

Policy Name ↑↓	State ↑↓
pam-mfa	On

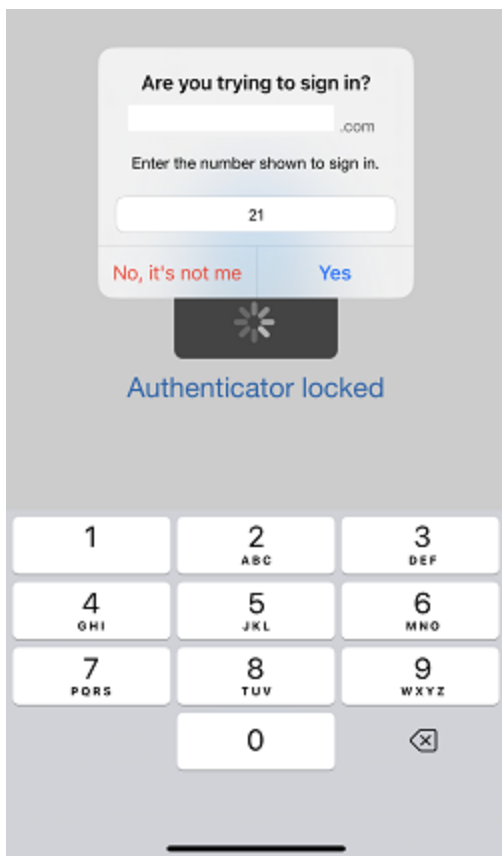
## Configuring your PAM System Properties:

1. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor and add this option to `catalina.properties` file and click **Save**:  
**`xtam.mfa.azuread.clientid=<your App ID>`**
2. If you also have Azure AD **Guest** users that will be required to authenticate with Azure MFA, then you must also add the following line that includes your *Azure tenant ID*. If you do not have Azure AD **Guest** users, then this parameter is not required:  
**`xtam.mfa.azuread.tenantid=<your Tenant ID>`**
3. Finally, **restart** your service PamManagement (Windows ) or pammanager (Linux) to complete your configuration.

## Azure MFA Number Matching

If MFA Number Matching is required in your Azure tenant, before their first use in PAM each user must manually enable Number Matching support. To enable, each user must login to PAM using their Azure AD SSO account, then navigate to Management > My Profile > Preferences and click the **Re-enable** button for the *RDP Proxy Access* parameter.

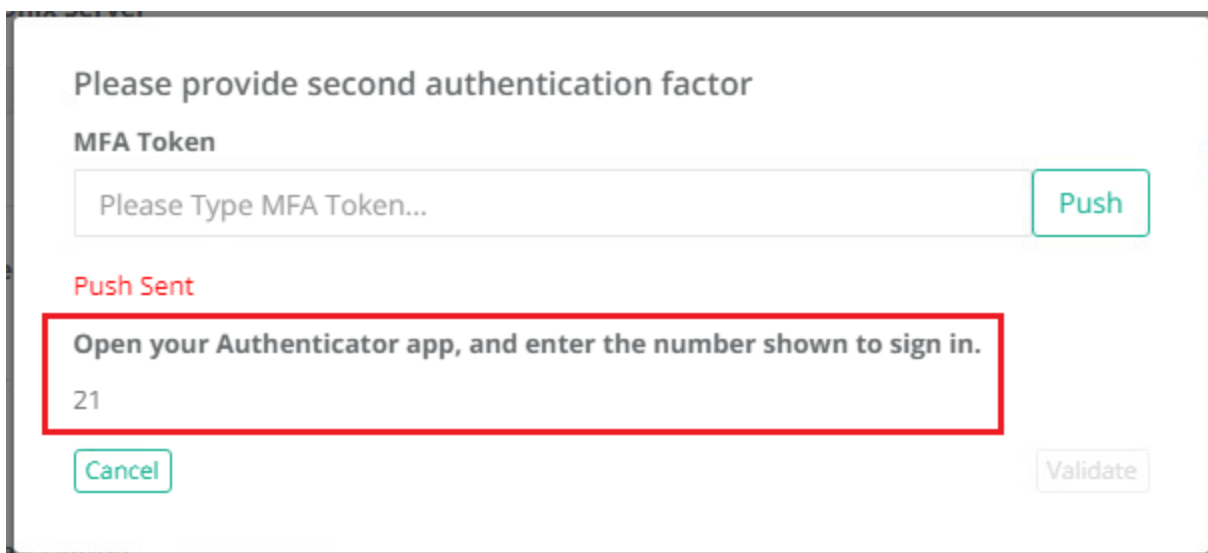
When prompted, the user must enter their valid password and click **Enable**. If the user's password is changed any time after this value has been provided, they must repeat this process, or their Azure MFA authentication will be denied.



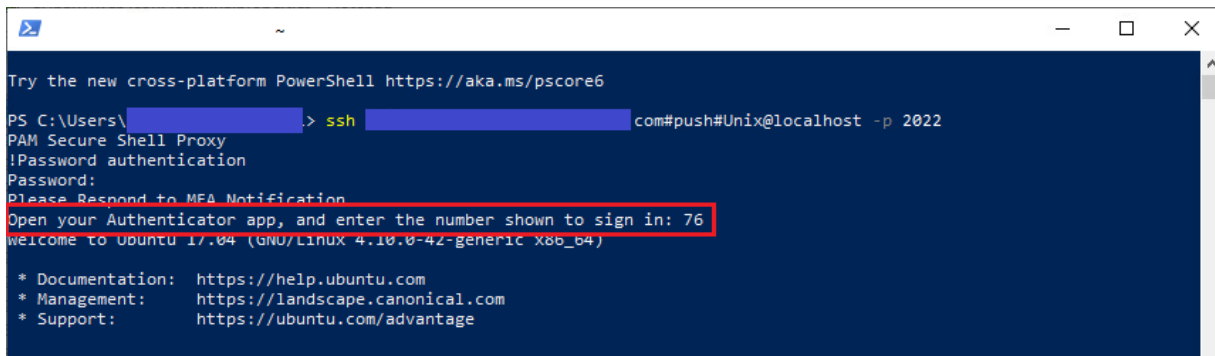
PAM native functionality supports Azure MFA Number Matching when:

- MFA is required in a Workflow Binding
- Authentication with the SSH Proxy.

For MFA in a Workflow Binding, the approved user will be presented with the Number in PAM after the *Push* button is clicked, that is then required to be used in the Microsoft Authenticator App.



For SSH Proxy authentication, the user will be presented with the *Number* in the proxy that is then required to be used in the Microsoft Authenticator App.

A terminal window with a dark blue background. The text shows a PowerShell prompt, an SSH command, and the output of a PAM Secure Shell Proxy. It prompts for a password and then displays an MFA notification: 'Please Respond to MFA Notification' and 'Open your Authenticator app, and enter the number shown to sign in: 76'. This line is highlighted with a red rectangle. Below this, it says 'welcome to ubuntu 17.04 (GNU/Linux 4.10.0-42-generic x86\_64)' and lists links for documentation, management, and support.

```
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\[redacted] > ssh [redacted] com#push#Unix@localhost -p 2022
PAM Secure Shell Proxy
!Password authentication
Password:
Please Respond to MFA Notification
Open your Authenticator app, and enter the number shown to sign in: 76
welcome to ubuntu 17.04 (GNU/Linux 4.10.0-42-generic x86_64)

* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:      https://ubuntu.com/advantage
```

Please note that these Numbers are time limited so if too much time has elapsed between when the number is generated and subsequently used in the Microsoft Authenticator App, MFA may be denied. The user must generate a new number if the current one has expired.

## To test the integration

- Use **user#push#record** when logging in to SSH or RDP Proxy sessions.
- Use **user#OTP#record** when logging in to SSH or RDP Proxy sessions.
- Use **user#record** when logging in to SSH Proxy sessions and follow MFA prompt to use push or OTP 2nd factor authentication.
- Click the **Push** button or provide OTP on the MFA configuration dialogue triggered by the MFA enabled workflow requests.

## Integration with OneLogin authentication

### System Configuration for SAML: OneLogin IdP Integration

PAM supports integration with OneLogin Identity Provider using SAML protocol to defer user authentication to OneLogin.

The following guide describes how to configure your OneLogin integration.

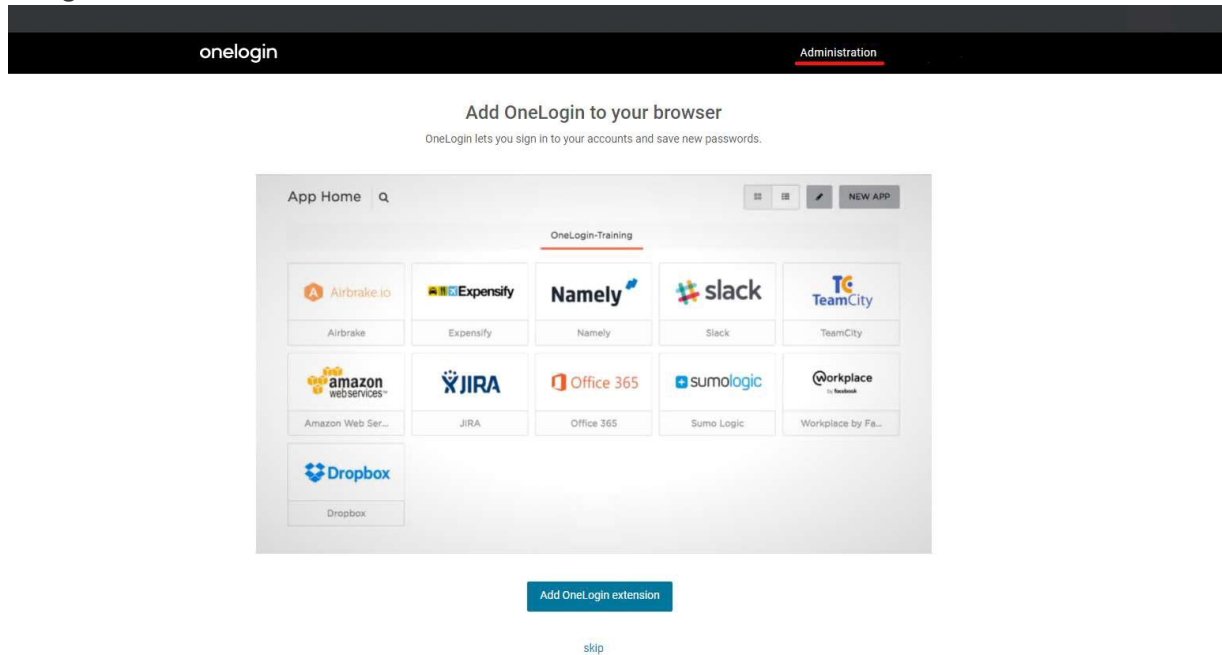
## Requirements

Before you begin your integration, be sure you meet the following pre-requisites:

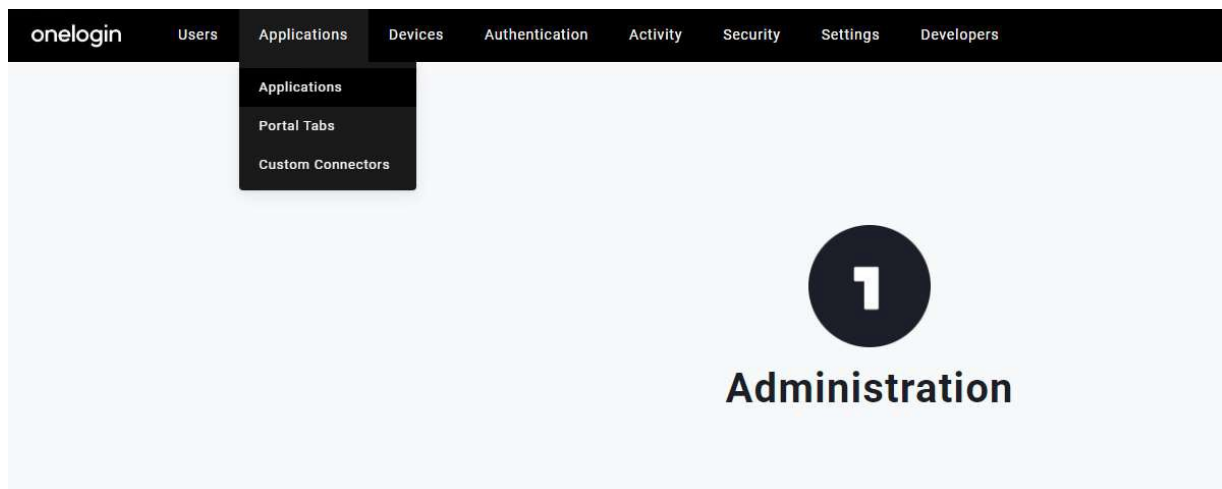
- A working PAM deployment with the [Federated Sign-In](#) experience.
- Access to your existing PAM host server. You will need to update a configuration file, certificates and restart services.
- Access to your OneLogin portal to configure your AuthPoint authentication services.
- If Users are created and managed in OneLogin, then a matching user must also be created as PAM Local User.
- If Users are synced from Active Directory to OneLogin, then you must also integrate PAM with the same Active Directory.

## Step 1: Begin the OneLogin Configuration

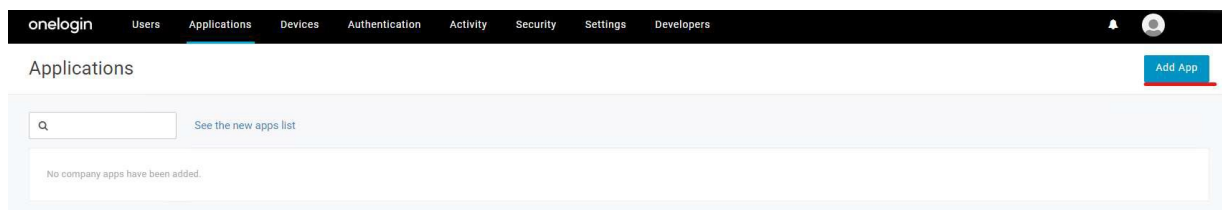
1. Login to your OneLogin account with admin account (<https://someorg.onelogin.com/portal/>)
2. Navigate to **Administration**.



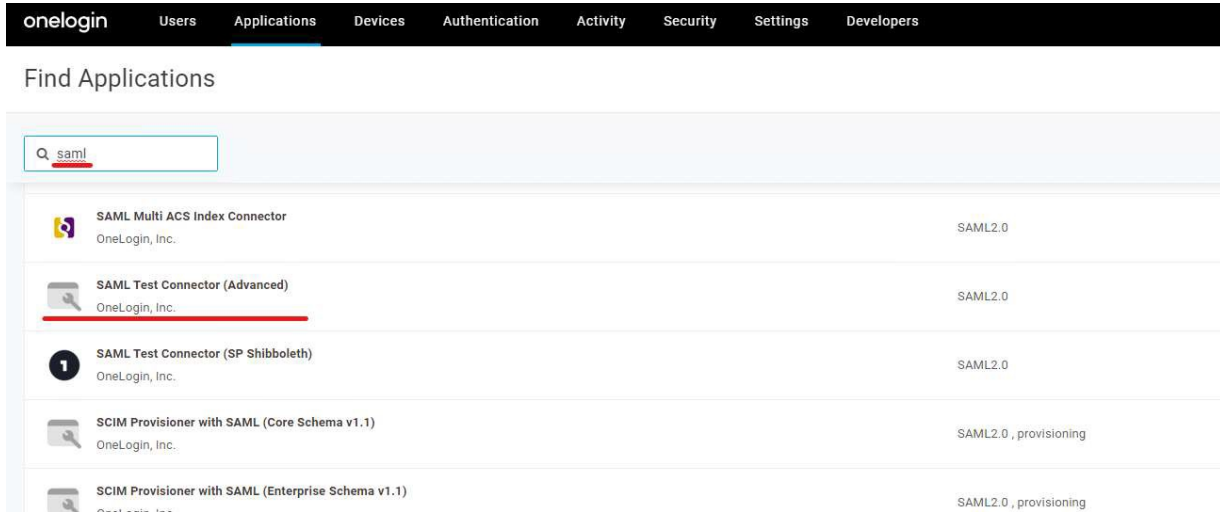
3. Go to Applications > Applications.



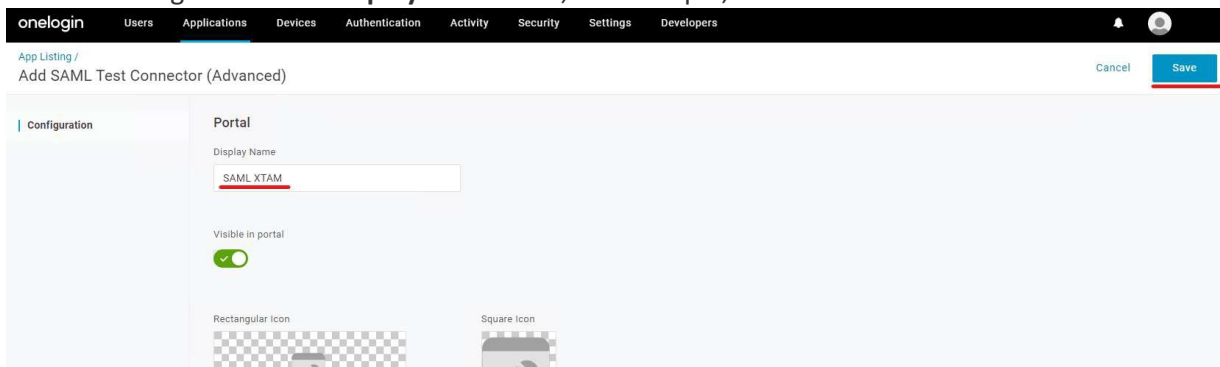
4. Click **Add App** button.



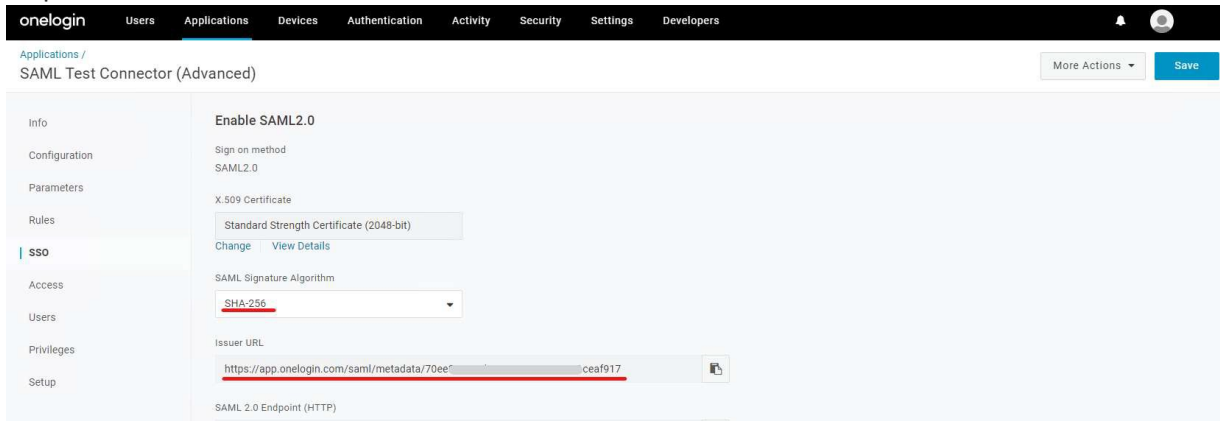
5. Navigate to Find Applications search for **saml** and choose **SAML Test Connector (Advanced)**.



6. Enter meaningful name in **Display Name** field, for example, **SAML PAM** and click **Save**.



7. Go to **SSO** page and select **SHA-256** for SAML Signature Algorithm. Copy **Issuer URL** for using it in next step. Click **Save**.



## Step 2: Perform the PAM Configuration

1. Login to your PAM host server.

On PAM server go to `$PAM_HOME/web/conf` folder. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor and add the following new section. Confirm that the

values for each parameter is accurate to your System deployment. Add new section with SAML provide configuration to `catalina.properties` with prepopulated data

# OneLogin SSO SAML

cas.authn.pac4j.saml[0].clientName=OneLoginSSO

cas.authn.pac4j.saml[0].keystorePassword=password

cas.authn.pac4j.saml[0].privateKeyPassword=password

cas.authn.pac4j.saml[0].serviceProviderEntityId={managed\_path}

cas.authn.pac4j.saml[0].serviceProviderMetadataPath=\$PAM\_HOME/content/keys/oneloginssso.xml

cas.authn.pac4j.saml[0].keystorePath=\$PAM\_HOME/content/keys/samlKeystoreOneLoginSSO.jks

cas.authn.pac4j.saml[0].identityProviderMetadataPath={Issuer URL From step 1.7}

cas.authn.pac4j.saml[0].maximumAuthenticationLifetime=2073600

2. When complete, save and close your `catalina.properties` file and restart **PamManagement** service.
3. After the service fully restarts, it could take 3-5 minutes to fully restart, the keystore file should appear in `samlKeystoreOneLoginSSO.jks` keystore and `oneloginssso.xml` metadata files should appear in `$PAM_HOME/content/keys`.

## Step 3: Complete the OneLogin Configuration

1. Return to your OneLogin portal.
2. In OneLogin application configuration go to **Configuration** page.

The screenshot shows the OneLogin portal interface. At the top is a navigation bar with tabs: onelogin, Users, Applications, Devices, Authentication, Activity, Security, Settings, and Developers. Below the navigation bar, the breadcrumb path is 'Applications / SAML Test Connector (Advanced)'. On the left is a sidebar menu with options: Info, Configuration (highlighted with a red underline), Parameters, Rules, SSO, Access, and Users. The main content area is titled 'Application details' and contains three input fields: 'RelayState', 'Audience (EntityID)', and 'Recipient'.

3. Enter values for all necessary fields that match those that were entered into the the `catalina.properties` file from the previous step:

**Audience (EntityID):** cas.authn.pac4j.saml[0].serviceProviderEntityId value from step 8

**Recipient:** https://pam.yourorg.com/cas/login?client\_name=OneLoginSSO

**ACS (Consumer) URL Validator:** ^https://pam.yourorg.com/cas/login\?client\_name=OneLoginSSO\$

**ACS (Consumer) URL:** https://pam.yourorg.com/cas/login?client\_name=OneLoginSSO

**Login URL:** https://pam.yourorg.com/xtam

**SAML signature element:** Assertion



onelogin Users Applications Devices Authentication Activity Security Settings Developers

Applications / SAML Test Connector (Advanced) More Actions Save

Info Configuration Parameters Rules SSO Access Users

Application details

RelayState

Audience (EntityID)  
https://xtam.yourorg.com

Recipient  
https://xtam.yourorg.com/cas/login?client\_name=OneLoginSSO

ACS (Consumer) URL Validator\*

onelogin Users Applications Devices Authentication Activity Security Settings Developers

Applications / SAML Test Connector (Advanced) More Actions Save

Info Configuration Parameters Rules SSO Access Users Privileges Setup

Application details

RelayState

Audience (EntityID)  
https://xtam.yourorg.com

Recipient  
https://xtam.yourorg.com/cas/login?client\_name=OneLoginSSO

ACS (Consumer) URL Validator\*  
\*https://xtam.yourorg.com/cas/login?client\_name=OneLoginSSO\$

ACS (Consumer) URL\*  
https://xtam.yourorg.com/cas/login?client\_name=OneLoginSSO

Single Logout URL

Login URL  
https://xtam.yourorg.com/xtam

onelogin Users Applications Devices Authentication Activity Security Settings Developers

Applications / SAML Test Connector (Advanced) More Actions Save

Info Configuration Parameters Rules SSO Access Users Privileges Setup

Application details

Login URL  
https://xtam.yourorg.com/xtam

SAML not valid before  
3

SAML not valid on or after  
3

SAML initiator  
OneLogin

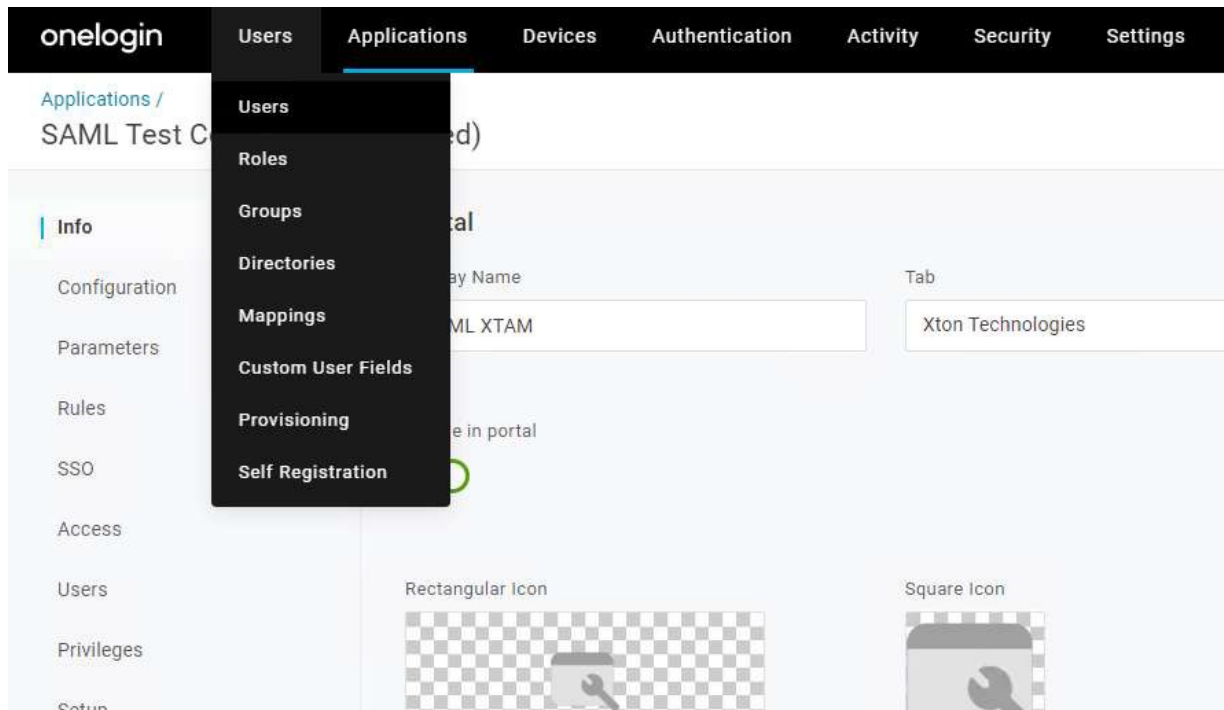
SAML nameID format  
Email

SAML issuer type  
Specific

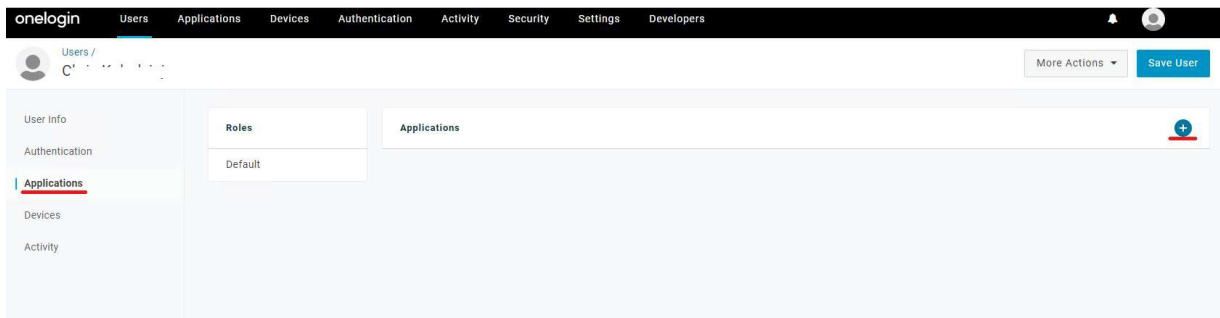
SAML signature element  
Assertion

Click **Save** button.

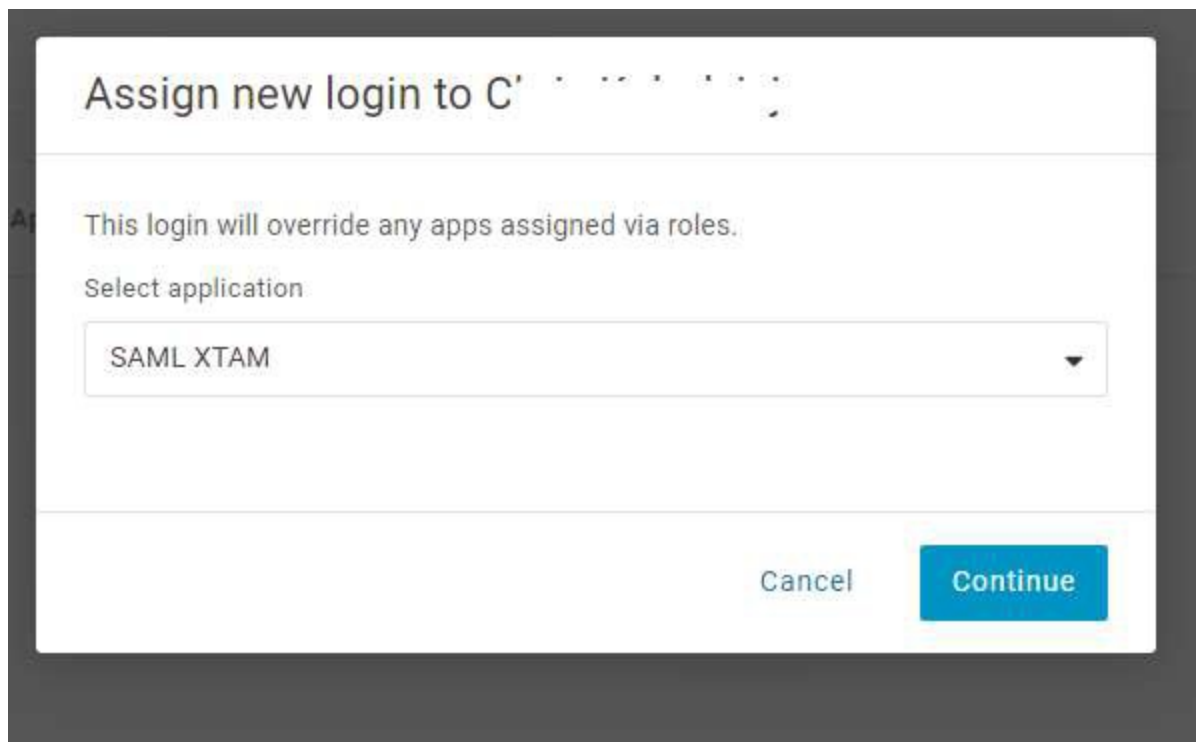
4. Navigate to Users > Users.



5. Select user that needs to login to the System using newly created application. Go to **Applications** and click **+** button.



6. From dropdown menu select your application click **Continue** and click **Save User**.



7. Finally, you can open your PAM login page, click the button named **OneLogin** and test the login process with the User that was created in the previous step.

## Integration with RADIUS based Providers

PAM supports integration with MFA providers that utilize the RADIUS Authentication protocol to provide secure login to its web portal only. If you are looking for a RADIUS integrated solution that supports both the PAM web portal and proxy authentication methods, then we recommend using [Imprivata Confirm ID](#).

This article will describe how to proceed with the configuration in PAM, but please note that you will need to know the specific values to use. If you do not know the specific configuration of your RADIUS based provider, please contact your Administrator or the Vendor for further assistance.

Pre-requisite: PAM must be deployed with and configured to use its [Federated Sign-In](#) component in order to integrate with multi-factor authentication providers.

1. Configure PAM with the Federated Sign-In module and ensure that it is working properly.
2. Log on to the PAM host computer.
3. Stop the **PamManagement** (Windows) or the **pammanager** (Linux) service. PAM will be offline until this procedure is completed.
4. Open the file `$PAM_HOME/web/conf/catalina.properties` and add the following lines to this file, inputting your MFA specific values (marked in red bold) where applicable:

```

1 cas.authn.mfa.globalProviderId=mfa-radius
2
3 cas.authn.mfa.radius.client.sharedSecret=secret
4 cas.authn.mfa.radius.client.authenticationPort=1812
5 cas.authn.mfa.radius.client.accountingPort=1813
6 cas.authn.mfa.radius.client/inetAddress=localhost
7 cas.authn.mfa.radius.server.protocol=CHAP (options include PAP, CHAP,
8   MSCHAPv1, MSCHAPv2, EAP_MD5, EAP_MSCHAPv2)
9   cas.authn.mfa.radius.name=XTAM-Trigger # This line should only be added
10  if your are using a Push based RADIUS provider. For example, if a user first
11  authenticates with their username and password and then receives a token to
12  their device, then add this line. Otherwise, do not include this line in your
13  configuration.

```

Please talk with your RADIUS or Network Administrator to learn what values should be set for the PAM configuration.

If you wish to enable different MFA providers for individual users or group, please read [this article](#) for additional information.

- When complete, **save and close** this file.
- Start the **PamManagement** (Windows) or the **pammanager** (Linux) service and try your RADIUS two-factor authentication login.

If you want to be able to send a command "push" in Radius integrations,

Open the file `$PAM_HOME/web/conf/catalina.properties` in text editor, locate the section that begins with `#CAS`, add the following line:

```
1 | cas.authn.mfa.radius.client.push=true
```

to this file and restart **PamManagement** (Windows) or the **pammanager** (Linux) service.

Instruction for update [Federated Sign-In](#) component from v5.2 to v6.5 is [here](#).

## Integration with ServiceNow

Privileged Access Management (PAM) Integration with ServiceNow Incident Activity.

PAM can be easily integrated with your ServiceNow tenants so that interactions within PAM records can be added to the corresponding ServiceNow Incidents activities.

Once the integration is properly configured, all you need to do in PAM is reference the ServiceNow (SN) Incident number in your access request form and the rest will be automated for you.

Review the remainder of this article to learn how to setup this easy integration as well as some screenshots detailing the process.

# Configuring your ServiceNow Integration

1. **Login** to your PAM host server.
2. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor and add the following new lines to the end:

```
xtam.integration.ticketing.pattern=SN#  
xtam.integration.ticketing.url=https://SERVICENOW-TENANT.service-now.com  
xtam.integration.ticketing.user=SERVICENOW-ADMIN  
xtam.integration.ticketing.password=SERVICENOW-PASSWORD  
xtam.integration.ticketing.script=ServiceNow Integration
```

- a. Defines the pattern that PAM will recognize as pertaining to a ServiceNow Incident number. Default is SN# meaning the user will refer to the SN incident number in PAM as *SN# INC0010009*
  - b. Defines your ServiceNow tenant URL.
  - c. Defines your ServiceNow administrator's username.
  - d. Defines your ServiceNow administrator's password.
  - e. Defines the PAM script that performs the integration procedure. You should not change this default value unless you created your own PAM script, then you should define your script's name here.
3. **Save** and close the file.
  4. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service to complete the integration.

## Testing PAM and ServiceNow Integration

Use the following procedure to both test your configuration as well as to understand how the two systems integrate.

1. **Login to ServiceNow** and create a new and find an existing Incident that can be used for testing. **Copy** the SN incident number.

Incident INC0010009

Subcategory: -- None --

Business service:

Configuration item:

Urgency: 2 - Medium

Priority: 3 - Moderate

Assignment group:

Assigned to:

\* Short description: Rebuild db indexes

Description: Rebuild database index on production web server (prod-abc123)

Related Search Results >

Notes | Related Records | Resolution Information

Watch list: ☐ ☐

Work notes list: ☐ ☐

Work notes:

☐ Additional comments (Customer visible)

Activities: 1

System Administrator

Field changes • 2019-04-30 07:04:58

Impact: 2 - Medium

Incident state: New

Opened by: System Administrator

Priority: 3 - Moderate

2. Login to **PAM** and navigate to a record that requires an access request (PAM Workflow) and click the **Request** button.
3. In the Access Request form's **Reason** field, enter a reason that includes the SN# pattern as well as the actual SN incident number. Note that the expected format is SN# space Incident Number. For example:

Rebuilding indexes as required in SN# INC0010009

### Request Access <sup>?</sup>

**Reason <sup>?</sup>**

Rebuilding indexes as required in SN# INC0010009

☒

**Requested Minutes <sup>?</sup>**

45

☐

**Requested From <sup>?</sup>**

2019-04-30

10

:

13

**Requested To <sup>?</sup>**

2019-05-01

10

:

13

**Workflow Template**

IT Dept Connect Approval (after hours)

☒

**Checkout Required <sup>?</sup>**

Cancel

Request

4. **Submit** the PAM request when done.
5. **Return** to the ServiceNow incident and view the activity. A new comment will have been generated detailing the access request.

© 2025 Imprivata, Inc. All Rights Reserved.

| 209

<

≡

Incident  
INC0010009

Follow

▼

Update

Resolve

Delete

↑

↓

Related Search Results >

Notes

Related Records

Resolution Information

Watch list

Work notes list

Work notes

Work notes

☐ Additional comments (Customer visible)

Post

Activities: 3

System Administrator

Additional comments • 2019-04-30 07:16:14

PAM Comment: User john requested access: Rebuilding indexes as required in SN# INC0010009

System Administrator

Field changes • 2019-04-30 07:16:14

Incident state   In progress was New

System Administrator

Field changes • 2019-04-30 07:04:58

Impact   2 - Medium  
Incident state   New  
Opened by   System Administrator  
Priority   3 - Moderate

Update

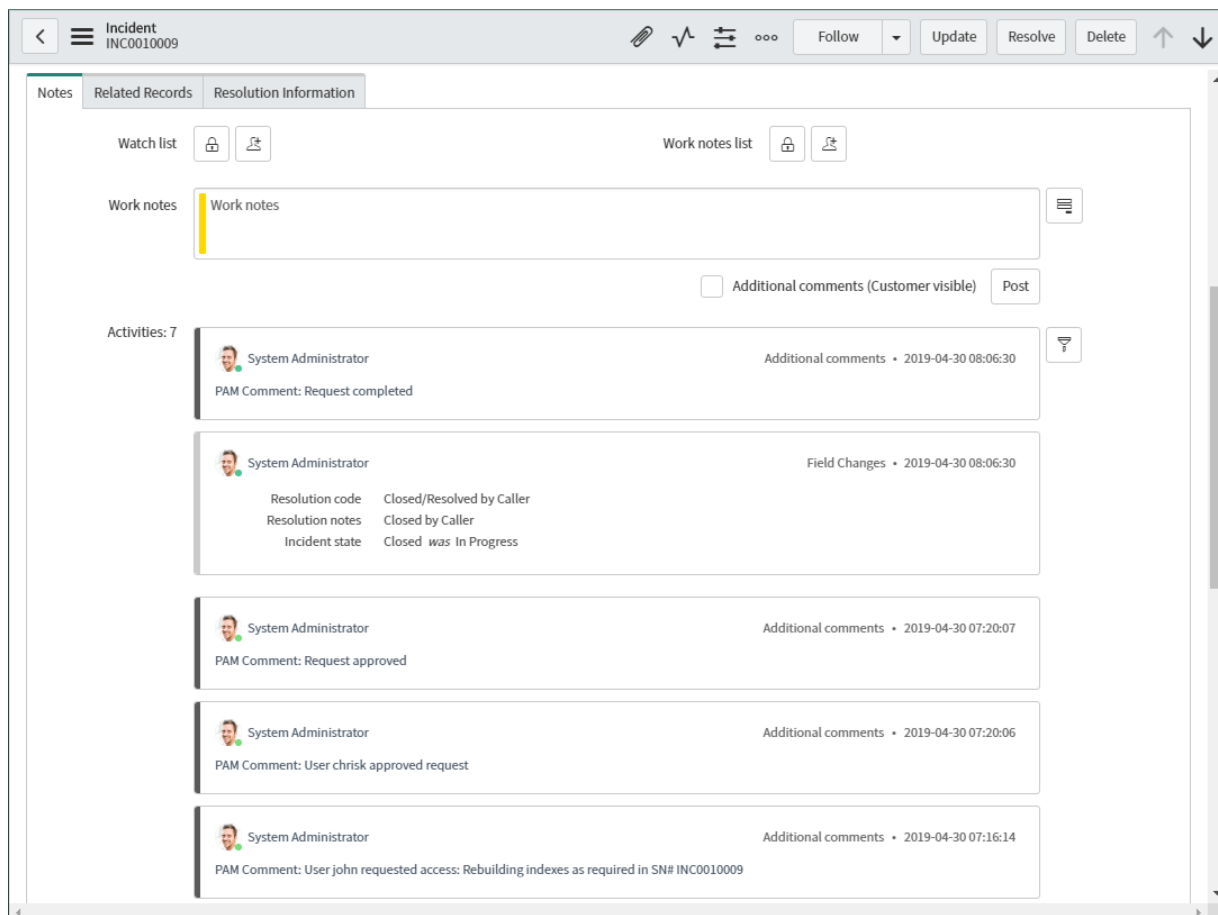
Resolve

Delete

Related Links

6. **Return** to PAM, approve the access request and continue testing the remaining functionality that has been approved via the Workflow. Afterwards, return to the SN incident to see each new activity comment.





## Integration with TOTP (MFA) Authentication

If you are already a user of Google Authenticator Multi-factor or Two-factor authentication and would like to configure PAM to use Google Auth, then please perform the following steps.

Please note that you will need to be able to access and modify files on the PAM host computer.

Contact your PAM System Administrator for assistance.

Pre-requisite: PAM must be deployed with and configured to use its [Federated Sign-In](#) component in order to integrate with multi-factor authentication providers.

1. Log on to the PAM host computer.
2. Open the file `$PAM_HOME/web/conf/catalina.properties`
3. Uncomment the following line only when a single global MFA for the entire PAM is desired:

```
1 | #cas.authn.mfa.globalProviderId=mfa-gauth
```

If you wish to enable different MFA providers for individual users or group, please read [this](#) article for additional information.

4. If you are using your own Database and not the PAM internal database, then modify the following lines. If you are using PAM's internal database, then skip this step.

```
1 | cas.authn.mfa.gauth.jpa.database.driverClass=org.apache.derby.jdbc.ClientDriver
2 | cas.authn.mfa.gauth.jpa.database.dialect=org.hibernate.dialect.DerbyTenSevenDialect
```

You can find the values that need to be replaced in bold above from this same `/catalina.properties` file in the #PAM Database section. In this example, we would copy the SQL database parameters below and use them to replace those of the Derby database above.

```
1 | hibernate.dialect=org.hibernate.dialect.SQLServer2012Dialect
2 | hibernate.connection.driver_class=com.microsoft.sqlserver.jdbc.SQLServerDriver
```

5. Optionally, you may modify the following lines to customize the branding of the Authentication page. Update the parameters; numbers and letters only, no spaces are allowed.

```
1 | cas.authn.mfa.gauth.issuer=Imprivata
2 | cas.authn.mfa.gauth.label=ImprivataPAM
```

6. When complete, **save** and **close** this file.
7. **Restart** the service PamManagement.

Once configured, refer to the following article [Google Authenticator – How to Login as a User for steps on how to use Google Authenticator MFA with PAM](#) from an end user's perspective.

## Integration with WatchGuard AuthPoint

### Configuration for PAM and WatchGuard AuthPoint MFA Integration

PAM supports integration with SAML providers like WatchGuard AuthPoint to allow their unique multi-factor authentication (MFA) solution to handle the second authentication method, enabling even greater security for your PAM deployment.

The following guide describes how to configure your PAM and WatchGuard AuthPoint integration.

## Requirements

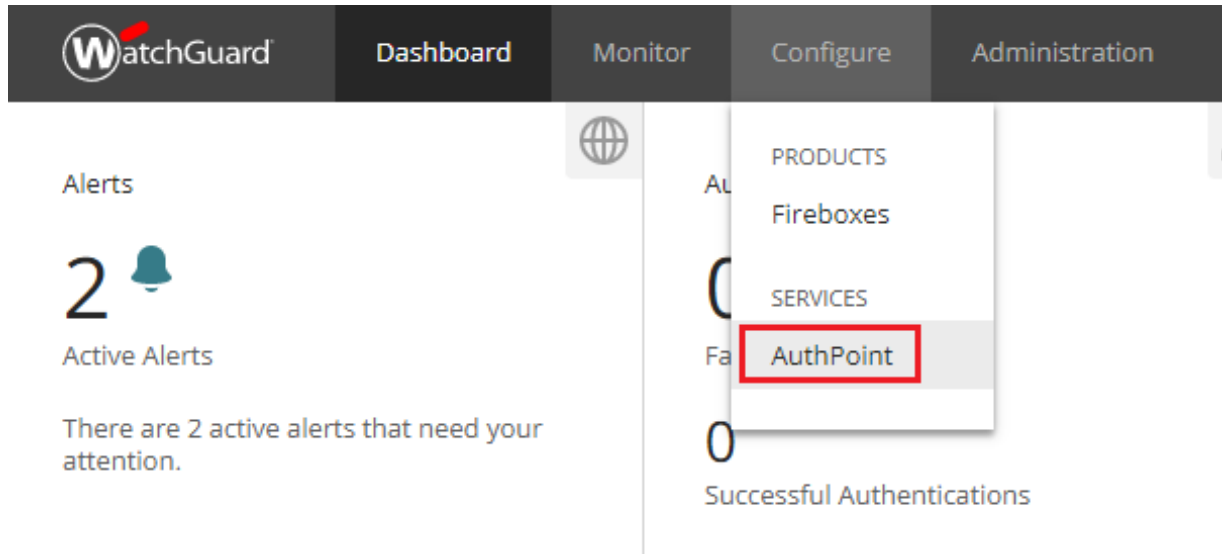
Before you begin your integration, be sure you meet the following pre-requisites:

- A working PAM deployment with the Federated Sign-In experience.
- Access to your existing PAM host server. You will need to update a configuration file, certificates and restart services.
- Access to your WatchGuard portal to configure your AuthPoint authentication services.

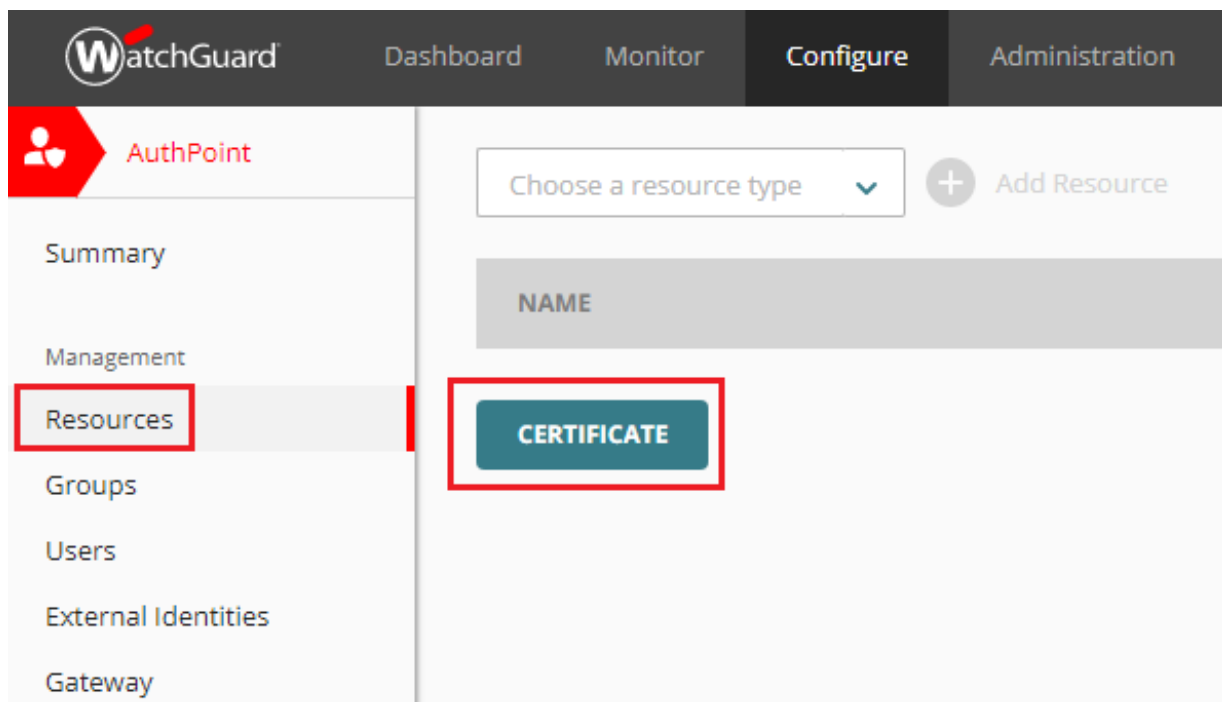
- If Users are created and managed in WatchGuard, then a matching user must also be created as an PAM Local User.
- If Users are synced from Active Directory to WatchGuard, then you must also integrate PAM with the same Active Directory.

## Step 1: Begin the AuthPoint Configuration

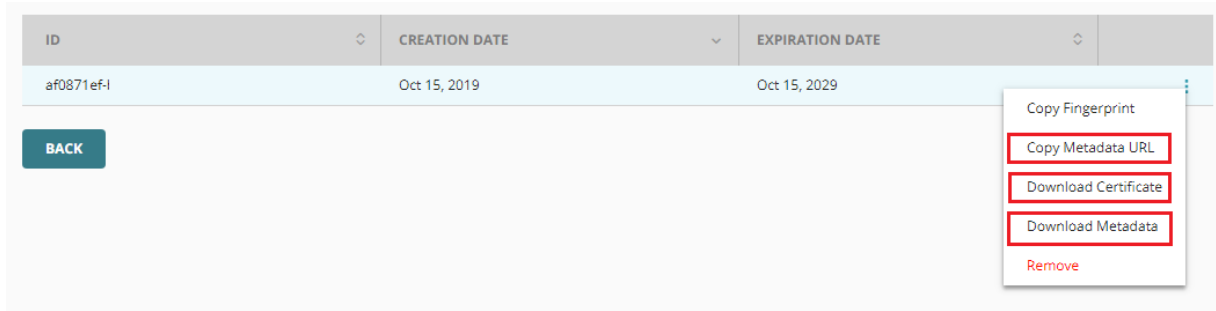
1. Login to your **WatchGuard** portal. This guide is built using the WatchGuard Cloud portal as available in October 2019.
2. Navigate to Configure > AuthPoint.



3. From the *AuthPoint* page, select the **Resources** option from the left navigation. From the *Resources* page, click the **CERTIFICATE** button to generate a certificate.



- When the certificate appears, click the menu on the right (three dots) and use both the **Download Certificate** and **Download Metadata** files. **Save** both files to a safe location as they will be needed in a future step.



- From the same menu (three dots), open the **Copy Metadata URL** option and save this URL. We will need this full URL in a future step.

## Step 2: Perform the Configuration

- Login to your PAM host server.
- Move or copy both the downloaded Certificate and Metadata files from step 1.4 to the `$PAM_HOME\content\keys` directory.
- Import the AuthPoint certificate to the PAM keystore using the following procedure:

- Open a prompt and navigate to the `$PAM_HOME` directory. You may need `sudo` or elevated permissions.
- Execute the following command:

For Windows, confirm the name of the `.cer` file and its location to be imported and used by PAM:

```
1 | bin\PamKeytool.cmd -import -alias xtauthpoint -file content\keys\wg-authpoint-saml-certificate-202910-base64.cer -keystore jre\lib\security\cacerts
```

For Unix or Linux, confirm the name of the `.cer` file and its location to be imported and used by PAM:

```
1 | bin/PamKeytool.sh -import -alias xtauthpoint -file content/keys/wg-authpoint-saml-certificate-202910-base64.cer -keystore jre/libsecurity/cacerts
```

- After the command is issued, you will be prompted for the keystore password. Enter the value `changeit` and press the Enter key to continue.
  - When prompted *Trust this certificate?* enter `y` and press the Enter key. You will receive the message *Certificate was added to keystore* when it has imported successfully.
- Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor and add the following new section. Confirm that the values for each parameter is accurate to your PAM deployment, particularly those in red.

# AutoPoint SSO SAML

cas.authn.pac4j.saml[0].clientName=AuthPoint

```
cas.authn.pac4j.saml[0].keystorePassword={enterSomePassword}
cas.authn.pac4j.saml[0].privateKeyPassword={enterSomePassword}
cas.authn.pac4j.saml[0].serviceProviderEntityId={managed_path}
cas.authn.pac4j.saml[0].serviceProviderMetadataPath=$PAM_HOME/content/keys/{metadata.xml from
step 1.4}
cas.authn.pac4j.saml[0].keystorePath=$PAM_HOME/content/keys/samlKeystoreAuthpoint.jks
cas.authn.pac4j.saml[0].identityProviderMetadataPath={metadata URL from step 1.5}
cas.authn.pac4j.saml[0].maximumAuthenticationLifetime=2073600
```

5. When complete, save and close your `catalina.properties` file.
6. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service. After the service fully restarts, it could take 3-5 minutes to fully restart, the keystore file should appear in `$PAM_HOME/content/keys/samlKeystoreAuthpoint.jks` or the location you defined in the catalina file.
7. Next, we will export the SAML certificate from PAM using the following procedure.
  - a. Open or reuse your existing prompt and navigate to the `$PAM_HOME` directory. You may need `sudo` or elevated permissions.
  - b. Execute the following command:

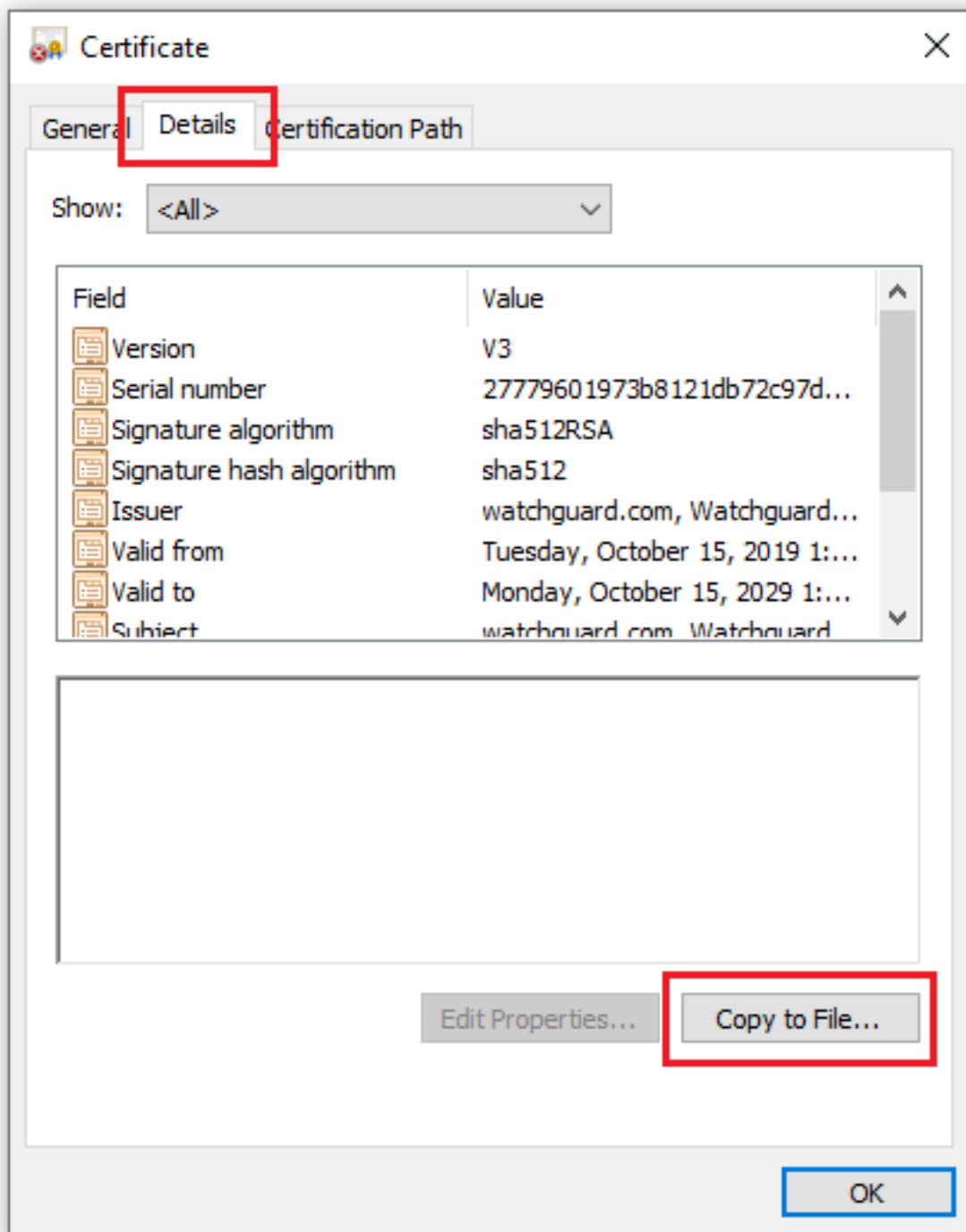
For Windows:

```
1 | bin\PamKeytool.cmd -keystore content\keys\samlKeystoreAdfs.jks -export -
  | alias saml2clientconfiguration -file content\keys\adfsxtam.cer
```

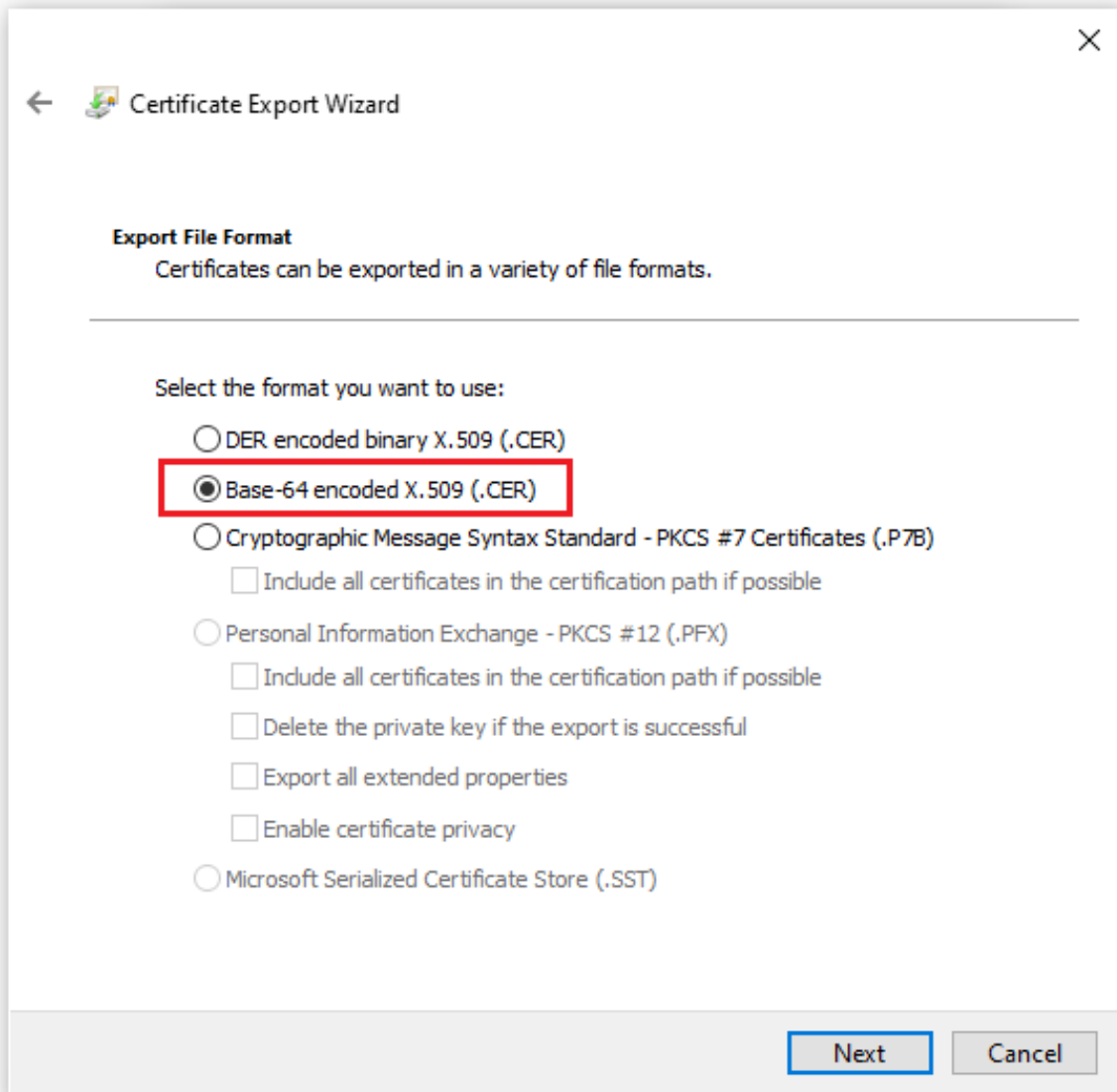
For Unix or Linux:

```
1 | bin/PamKeytool.sh -keystore content/keys/samlKeystoreAdfs.jks -export -
  | alias saml2clientconfiguration -file content/keys/adfsxtam.cer
```

8. Now we need to convert your exported certificate file to base-64 encoding. Use whatever method you are most comfortable with. In Windows, we believe the easiest method is the following:
  - a. Double click on your certificate file and click **Open** if you receive a security prompt.
  - b. From the *Certificate* dialog, switch to the *Details* tab and click the **Copy to File...** button.



- c. On the **Certificate Export Wizard** screen, select the format **Base-64 encoded X.509 (.CER)** option.

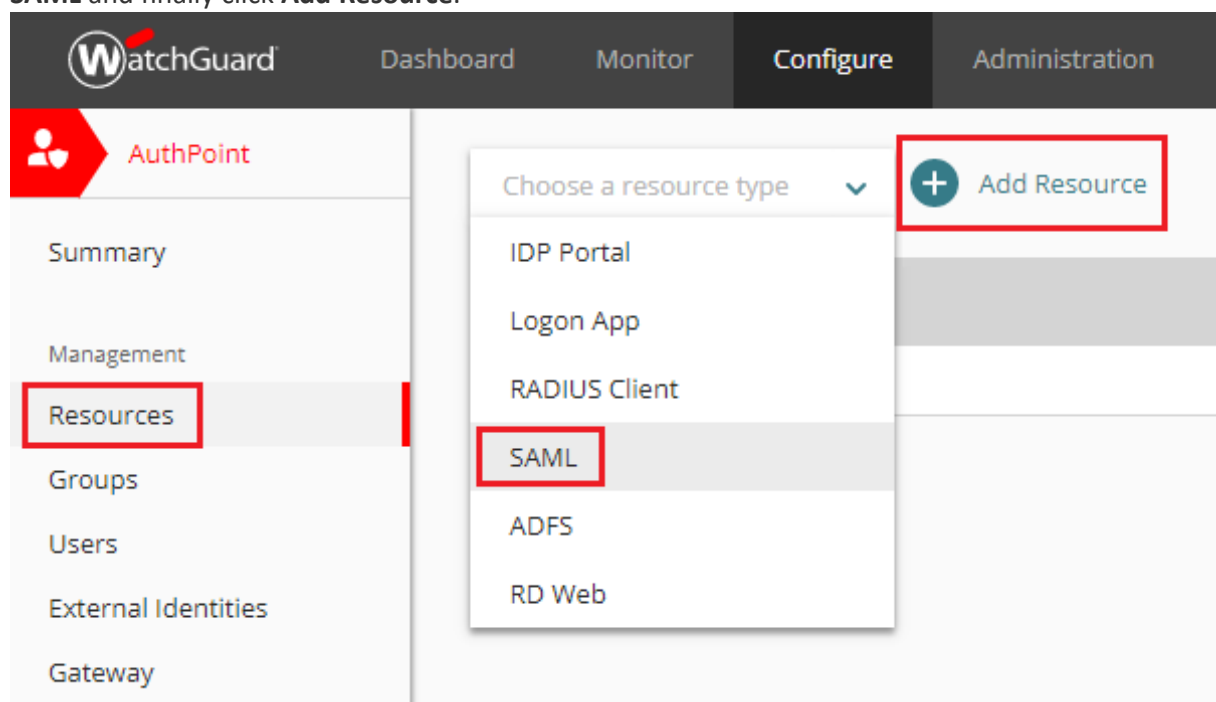


- d. Save this converted certificate file to `$PAM_HOME/content/keys`.

## Step 3: Complete the AuthPoint Configuration

1. Return to your WatchGuard portal.

2. From AuthPoint's **Resources** page, expand the Choose a resource type dropdown menu, select the option **SAML** and finally click **Add Resource**.





3. Enter values for all necessary fields that match those that were entered into the `catalina.properties` file from the previous step.

The screenshot shows the WatchGuard AuthPoint configuration interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configure' (selected), and 'Administration'. The left sidebar lists various configuration categories: Summary, Management, Resources (highlighted), Groups, Users, External Identities, Gateway, Hardware Tokens, General, Downloads, and Settings. The main content area is titled 'SAML' and contains the following fields:

- Name \***: Text input field containing 'Xtam integration'.
- Application Type (Integration Guide) \***: Dropdown menu set to 'Others'.
- Service Provider Entity ID \***: Text input field containing 'https://[redacted]:6443'.
- Assertion Consumer Service \***: Text input field containing 'https://[redacted]:6443/cas/login?client\_name=AuthPoint'.
- User ID sent on redirection to service provider**: Dropdown menu set to 'Email'.
- Logout URL**: Text input field containing 'Logout URL'.
- Signature Method**: Dropdown menu set to 'SHA-256'.
- SAML Version**: Dropdown menu set to '2.0'.
- Certificate**: Section with a 'CHANGE FILE' button, a trash icon labeled 'Remove file', and a toggle switch for 'Encryption enabled' which is turned on.
- AuthPoint Certificate \***: Dropdown menu showing 'af0871ef-[redacted] - Expiration date: Oct 15, 2029'.

At the bottom of the configuration area are two buttons: 'CANCEL' and 'SAVE'.

**Name:** Enter a meaningful name

**Application Type:** Others

**Service Provider Entity ID:** {managed\_path value from step 2.4}

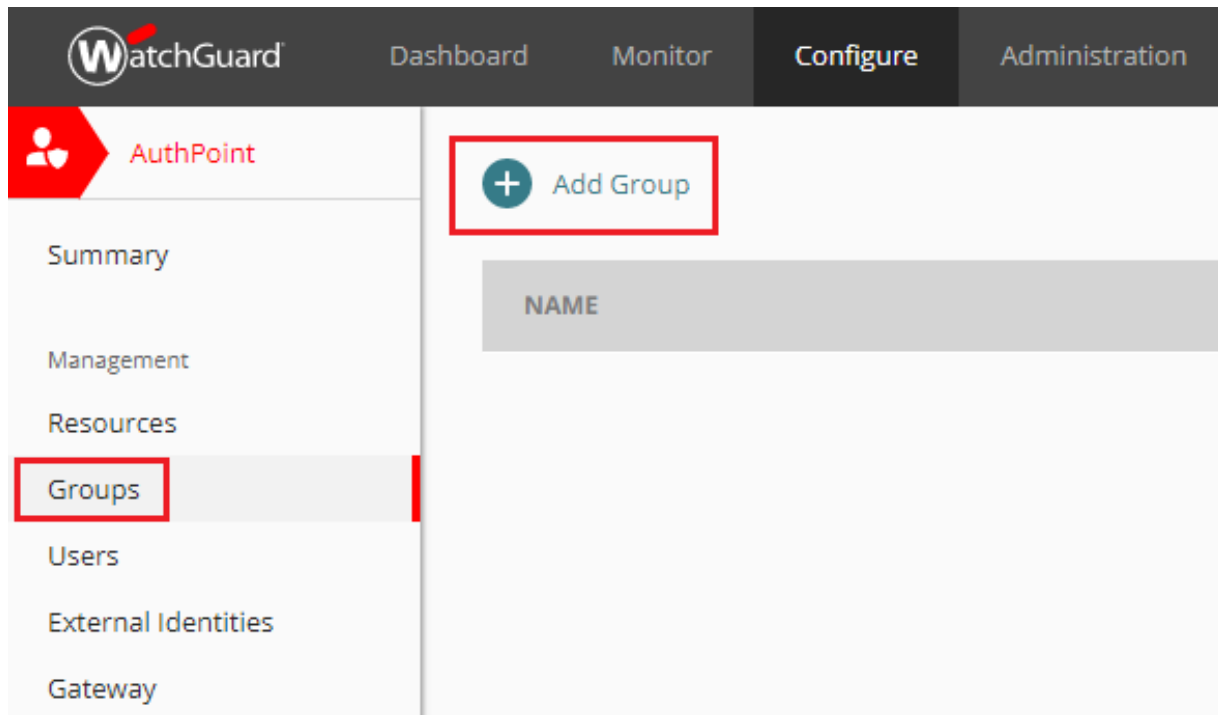
**Assertion Consumer Service:** {managed\_path value from step 2.4}/cas/login?client\_name=AuthPoint

**User ID sent on redirection to service provider:** Email

**Logout URL:** empty

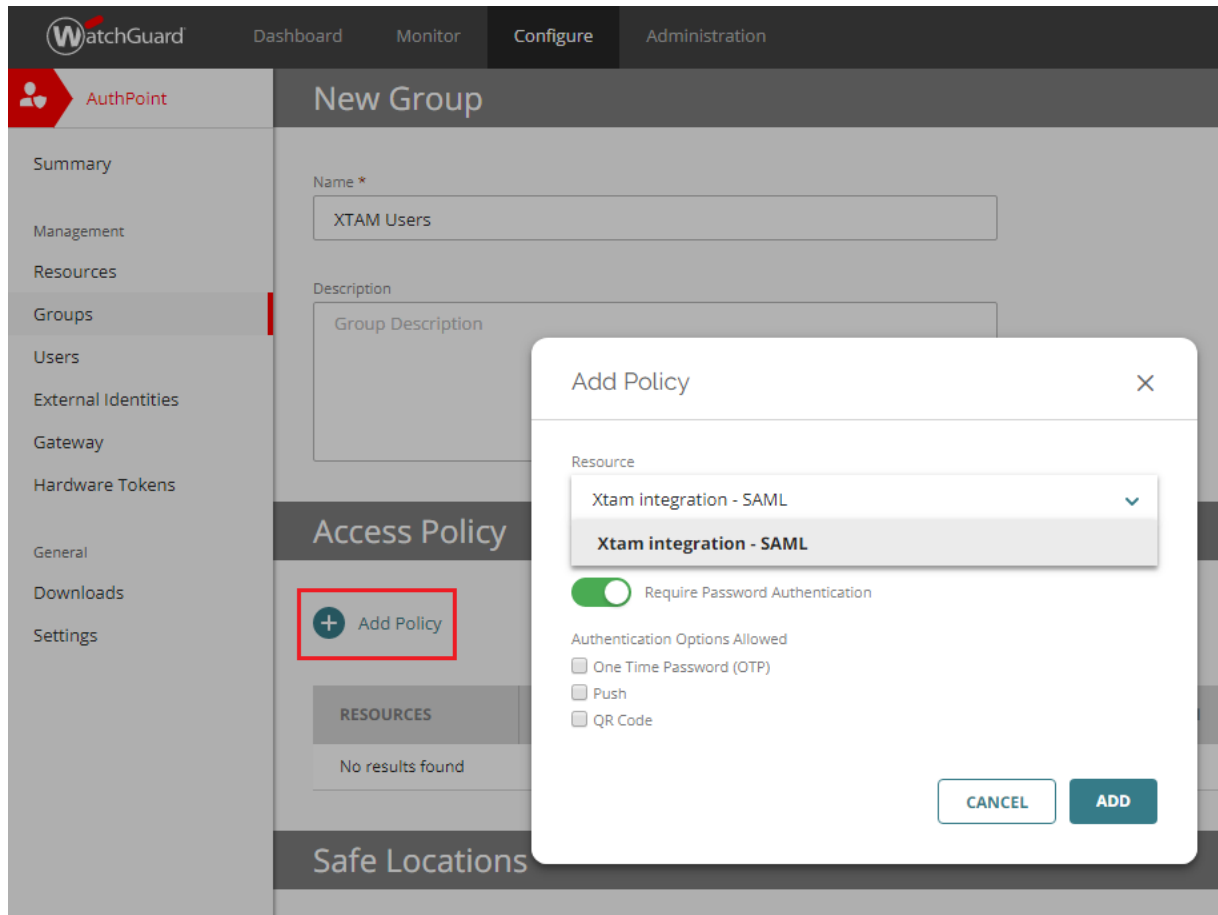
**Signature Method:** SHA-256

4. For the Certificate, click the **CHOOSE FILE** button and select your converted base-64 encoded certificate file from the previous step.
5. Click the slider so that **Encryption enabled** is turned on.
6. Click the **SAVE** button to complete the resource creation.
7. Next, navigate to the AuthPoint's *Groups* page and click the **Add Group** button.



8. Enter a meaningful Name (required) for this new Group and a description (optional).

9. Now for this Group, click the **Add Policy** button, select the *Resource* we created in the previous step from the dropdown and finally configure your security policies as desired. Click **ADD** to complete the creation of your policy.



10. Next, navigate to the AuthPoint's Users page and click the **Add User** button.

WatchGuard

DashboardMonitorConfigureAdministration

AuthPoint

Summary

Management

Resources

Groups

Users

External Identities

Gateway

+

Add User

USER NAME	NAME
-----------	------

11. Fill out all required fields as needed for this new User. For the *Group* parameter, select the Group that was created in the previous step. Click the **SAVE** button to create this new user.

The screenshot shows the WatchGuard AuthPoint interface for creating a new user. The top navigation bar includes 'Dashboard', 'Monitor', 'Configure', and 'Administration'. The left sidebar lists various configuration areas, with 'Users' currently selected. The 'New User' form includes the following fields and options:

- First Name \***: Text input containing 'John'.
- Last Name**: Text input containing 'Smith'.
- User Name \***: Text input containing 'jsmith'.
- LDAP**: A toggle switch that is currently turned off.
- Email \***: Text input containing 'jsmith@example.com'.
- Group \***: A dropdown menu with 'Xtam access' selected.
- Show Address**: A button with a plus icon.
- CANCEL** and **SAVE**: Buttons at the bottom of the form.

12. Finally, you can open your PAM login page, click the red button named **AuthPoint** and test the login process with the User that was created in the previous step. *Remember that an identical User account must also be created on PAM's Local Users page.*

## Integration with YubiKey

If you are already a user of YubiKey Multi-factor or Two-factor authentication and would like to configure PAM to use YubiKey, then please perform the following steps.

Please note that you will need to be able to access and modify files on PAM host computer. Contact your System Administrator for assistance.

Pre-requisite: PAM must be deployed with and configured to use its Federated Sign-In component in order to integrate with multi-factor authentication providers. For YubiKey MFA Integration, download this [Federated Sign-in](#) Module and follow the guide linked above for configuration.

#### [Step 1. Register your YubiKey to get Yubico API Keys](#)

#### [Step 2. Configure Integration with YubiKey](#)

## Step 1. Register your YubiKey to get Yubico API Keys

1. Open your browser to <https://upgrade.yubico.com/getapikey/>
2. Enter your **email address** into the required field.
3. Enter your key's OTP or touch your YubiKey to populate the **YubiKey OTP** field.
4. **Check the box** to accept the Yubico Terms and Conditions.

5. Click the **Get API Key** button.

https://upgrade.yubico.com/getapikey/

Search DuckDuckGo

# yubico

## YUBICO GET API KEY

Here you can generate a shared symmetric key for use with the Yubico Web Services. You need to authenticate yourself using a Yubikey One-Time Password and provide your e-mail address as a reference.

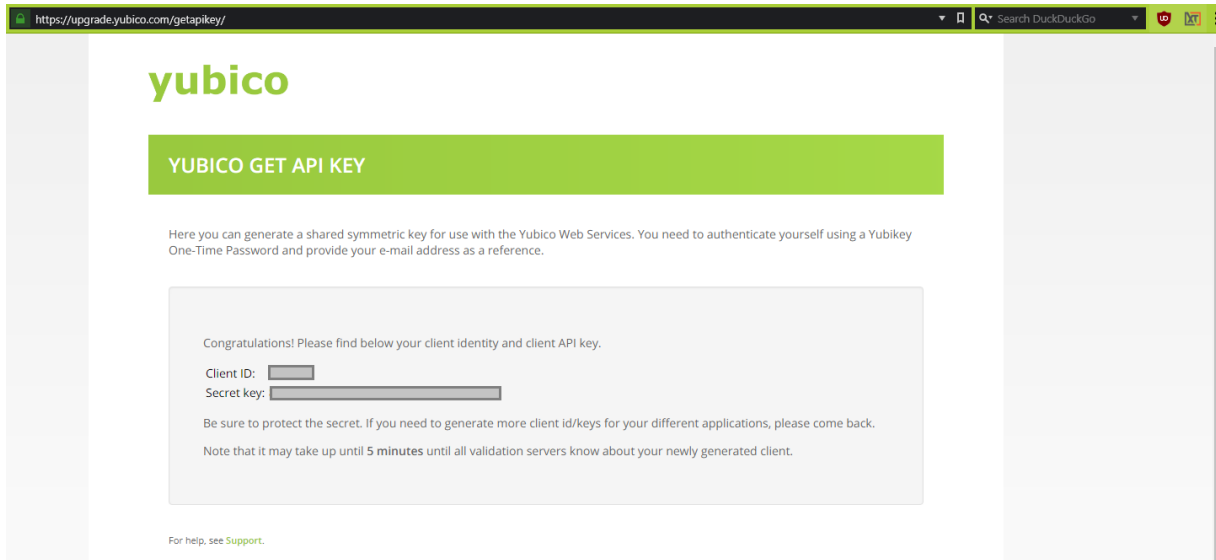
Your email address:

YubiKey OTP:

☒ I've read and accepted the [Terms and Conditions](#)

For help, see [Support](#).

6. The Yubico website will now display your client identity and client API keys. Save this information to a safe location or do not close your web browser. You will need both the *Client ID* and *Secret key* values in the next step.



## Step 2. Configure Integration with YubiKey

1. Log on to PAM host computer.
2. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor.
3. In this file, scroll down to the section labeled **# YubiKey**. If you do not have this section, copy and paste the entire section below to the bottom of your file.

```
1 | # YubiKey
2 | # Get your API clientId and secretKey here:
   | https://upgrade.yubico.com/getapikey/
3 |
4 | #cas.authn.mfa.globalProviderId=mfa-yubikey
5 | cas.authn.mfa.yubikey.clientId=clientId
6 | cas.authn.mfa.yubikey.secretKey=SecretKey
7 | cas.authn.mfa.yubikey.name=XTAMYubiKey
8 |
9 | cas.authn.mfa.yubikey.jpa.dataSourceName=java:comp/env/jdbc/PamDB
10 | cas.authn.mfa.yubikey.jpa.driverClass=org.apache.derby.jdbc.ClientDriver
11 | cas.authn.mfa.yubikey.jpa.dialect=org.hibernate.dialect.DerbyTenSevenDialect
12 | cas.authn.mfa.yubikey.jpa.dataSourceProxy=true
13 | cas.authn.mfa.yubikey.jpa.ddlAuto=update
```

4. Uncomment the following line only when a single global MFA for the entire PAM is desired:

```
1 | #cas.authn.mfa.globalProviderId=mfa-yubikey
```

If you wish to enable different MFA providers for individual users or group, please read [this article](#) for additional information.



5. Add your Client ID and Secret Key from Step 1 to the following lines:

```
1 | cas.authn.mfa.yubikey.clientId=clientId
2 | cas.authn.mfa.yubikey.secretKey=SecretKey
```

6. If you are using your own Database and not the PAM internal database, then modify the following lines. If you are using PAM's internal database, then skip this step.

```
1 | cas.authn.mfa.gauth.jpa.database.driverClass=org.apache.derby.jdbc.ClientDriver
2 | cas.authn.mfa.gauth.jpa.database.dialect=org.hibernate.dialect.DerbyTenSevenDialect
```

7. You can find the values that need to be replaced in bold above from this same `/catalina.properties` file in the #PAM Database section. In this example, we would copy the bolded SQL database parameters below and use them to replace those of the Derby database above.

```
1 | hibernate.dialect=org.hibernate.dialect.SQLServer2012Dialect
2 | hibernate.connection.driver_class=com.microsoft.sqlserver.jdbc.SQLServerDriver
```

8. When complete, **save and close** this file.  
9. Restart the service **PamManagement** (Windows) or **pammanger** (Linux).

This configuration will enable YubiKey as the global MFA provider in the System for all user logins. YubiKey MFA supports connection for users who using native clients such as PuTTY, mstsc, MobaXTerm, Secure CRT, Royal TS, WinSCP, scp, etc via SSH Proxy or RDP Proxy. If you wish to configure additional MFA providers or to enable YubiKey only for selected users or groups, then please see our [MFA Configuration Guide article](#) for more information.

## Advanced Deployments

### Changing Web GUI Port Number

To avoid a possible conflict on the standard https port of 443, PAM is installed to use port 6443 for its web GUI (<https://server:6443/xtam>).

If you want to change this port to something other than 6443, like the standard https port 443, then please follow the steps described in this article.

Before changing the port to 443 make sure that there is no other software running on this port on the operating system (such as MS IIS or Apache HTTPD Server) to avoid port conflicts. If something else is already running on this port, then PAM will fail to start.

## Windows

For Windows deployments:

1. Login to PAM host server and open the file `$PAM_HOME/web/conf/server.xml` in a text editor.
2. Search for the exact value **port="6443"**. There will be only one matching occurrence of this exact value in the file.

```

74      <!-- BEGIN: SELF SIGNED SSL -->
75      <Connector SSLEnabled="true" ciphers=
"TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA25
6" clientAuth="false" honorCipherOrder="true" keystoreFile="{xtam.cert.path}" keystorePass="{xtam.cert.password}" keystoreType="JKS" maxThreads="200"
port="6443" protocol="com.pam.config.Http11NioEncryptedProtocol" proxyPort="443" scheme="https" secure="true" sslEnabledProtocols="TLSv1.2+TLSv1.3"
sslProtocol="TLSv1.2"/>
76      <!-- END: SELF SIGNED SSL -->

```

3. Change this value from **port="6443"** to **port="443"**.
4. Save and close the file.
5. Restart the **PamManagement** service.

When the service fully restarts, your PAM server will be listening on port 443 (<https://server:443/xtam> or simply <https://server/xtam>).

## Linux with root account

For Linux deployments installed and run with root account:

1. Login to PAM host server and open the file `$PAM_HOME/web/conf/server.xml` in a text editor.
2. Search for the exact value **port="6443"**. There will be only one matching occurrence of this exact value in the file.

```

74      <!-- BEGIN: SELF SIGNED SSL -->
75      <Connector SSLEnabled="true" ciphers=
"TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA25
6" clientAuth="false" honorCipherOrder="true" keystoreFile="{xtam.cert.path}" keystorePass="{xtam.cert.password}" keystoreType="JKS" maxThreads="200"
port="6443" protocol="com.pam.config.Http11NioEncryptedProtocol" proxyPort="443" scheme="https" secure="true" sslEnabledProtocols="TLSv1.2+TLSv1.3"
sslProtocol="TLSv1.2"/>
76      <!-- END: SELF SIGNED SSL -->

```

3. Change this value from **port="6443"** to **port="443"**.
4. Save and close the file.
5. Restart the **pammanager** service.

## Linux with a non-root user account

For Linux deployments installed and run with a non-root user account:

Because PAM was deployed and running with a non-root account, Linux will not allow PAM to be bound to low number port such as 443. In this case, there are two options:

**First** is to follow the documentation of your operating system and disable this behavior so that Linux will allow a non-root user to bind to the port 443.

We do not recommend this option for production deployments, but for non-production deployments like test, trial or 'proof of concept' environments this may be considered.

**Second** is to leave PAM on its default port 6443 and configure a third party load balancer (revers proxy) to listen on the port 443 and pass through the HTTP traffic to the PAM server.

The below article describes the configuration of Apache HTTPD proxy server to act as a load balancer for two PAM nodes, but the same concept with a single node will serve a single node deployment. You can also use any other load balancer too such as an **F5**.

[Load Balancer Configuration for Apache HTTP Server with Sticky Sessions](#)

It's worth noting again, regardless of which option applies to your deployment, before changing the port to 443 make sure that there is no other software running on this port on the operating system (such as MS IIS or Apache HTTPD Server) to avoid port conflicts. If something else is already running on this port, then PAM will fail to start.

## Deployment Architecture to Scale Session Manager

This article discusses different deployment architecture scenarios to scale Privileged Access Management (PAM) utilizing multiple session manager components.

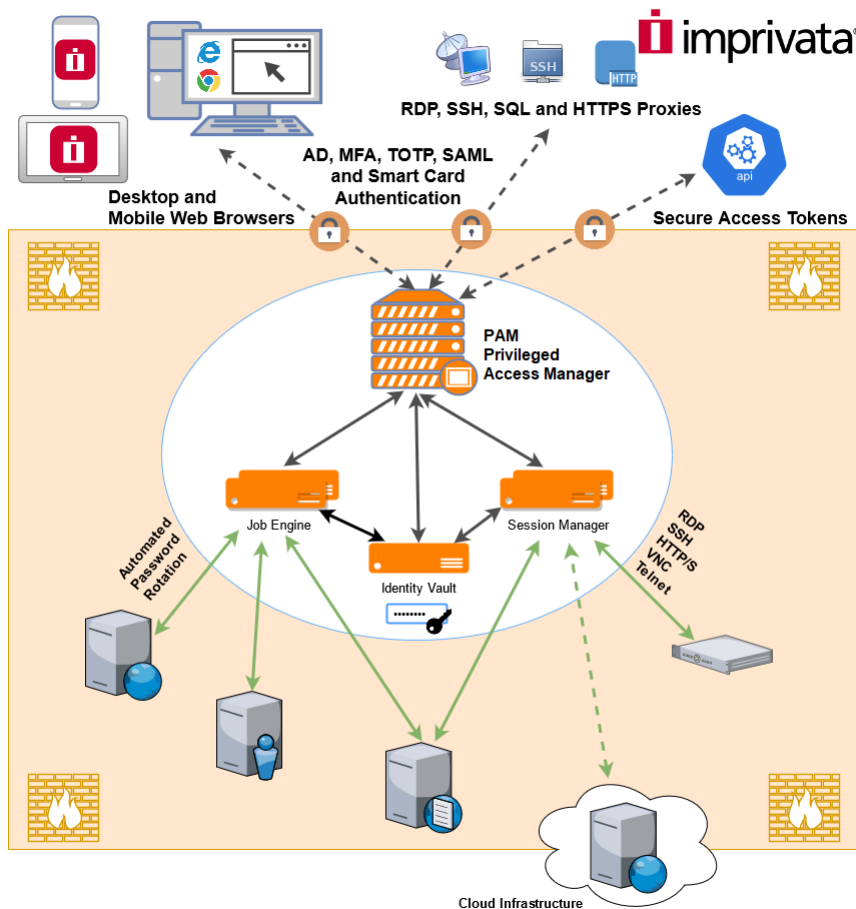
### Component Architecture

PAM contains several components. When PAM is deployed on a single host all components are installed on the same server and they communicate between each other inside this server.

One of these components is Session Manager.

PAM communicates with Session Manager using PAM proprietary protocol through the port 4822.

Session Manager, in turn, communicates with remote computers using RDP, SSH, Telnet or VNC protocols depending of the remote computer.



Session Manager can be installed on a separate host than PAM WEB application.

Then PAM can be instructed to use this Session Manager instead (or together) with the one installed on the PAM computer.

This way, RDP (or SSH) session will be established from Session Manager server to a remote server and PAM will communicate with Session Manager server using port 4822 (the port should be opened in Session Manager Server firewall).

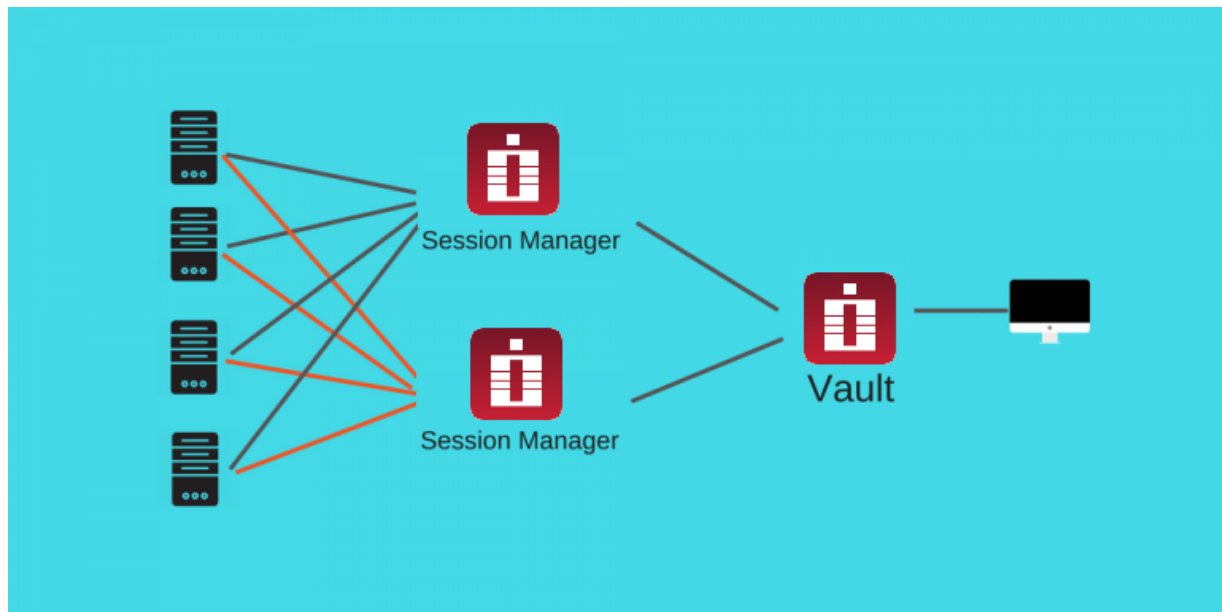
This architecture is not specifically related to RDP. Any protocol will work in the same way.

## Session Manager Deployment

There are two applications of this deployment:

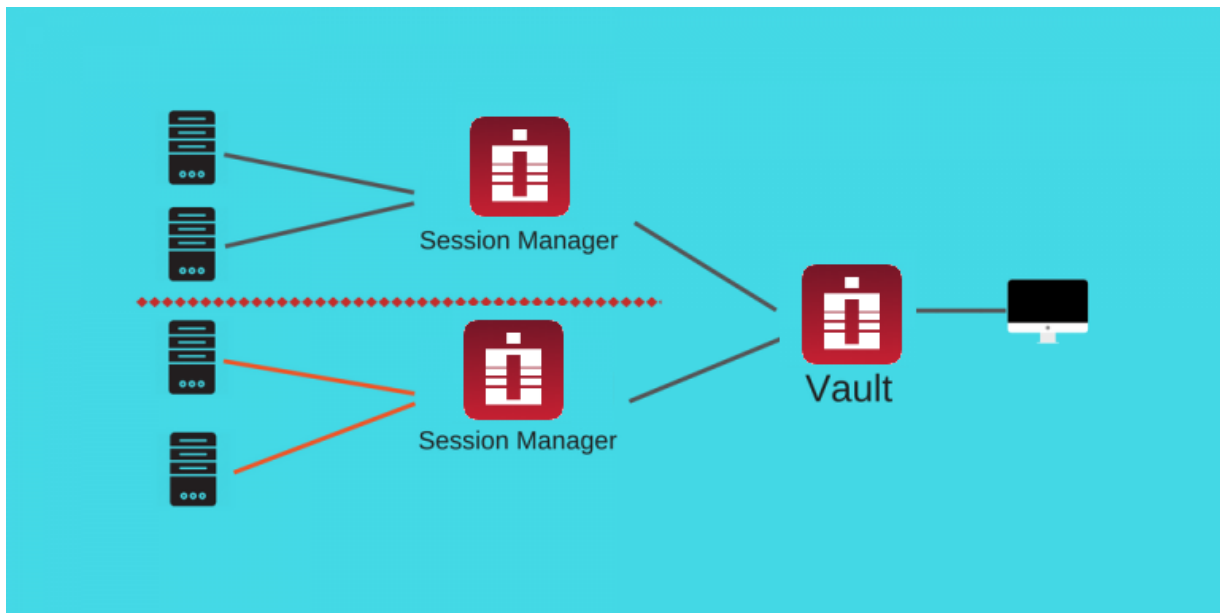
### 1. Performance optimization.

PAM can automatically load balance sessions between multiple Session Managers (there could be more than two) each time selecting one with least number of currently active sessions. This architecture also supports [high availability requirement](#).



### 2. Network isolation.

PAM could be configured to select a specific session managers group out of several configured groups (called Proximity Groups) to serve remote computers located on a specific PAM Vault, in specified IP range or in a specific domain. For example, computers from the network 10.0.0.x/24 could be served by SERVER SM1 or SERVER SM2 (balanced) while computers from the network 10.1.1.x/24 could be served by balanced session managers SERVER SM3 or SERVER SM4.



For the end user there will be no visible differences – the sessions will open as usual.

## Configuring

Practically, to support this scenario install Session Manager as an individual application on the Session Manager host.

To do that,

1. Run the regular installer on this host but only select one option: Session Manager.
2. The installer at some point will ask about certificates.
3. In a test environment ignore it leaving the communication channel between PAM and Session Manager over the port 4822 insecure.

Alternatively,

1. Bring file `certbundle.zip` from `$PAM_HOME` folder of PAM WEB application host. These certificates are generated during the installation and they keep the communication channel encrypted.
2. Open the PAM GUI, navigate to the menu Administration / Settings / Proximity Groups, **edit** *Default Group* and **add a new server** (host, port 4822).
3. Make sure that port 4822 is accessible from PAM server.
4. After saving the configuration PAM will check connection automatically displaying whether the communication channel is established (blue), failed (crossed-out) and whether it is secured (green).

Optionally,

1. **Remove** *localhost* or **keep it** so PAM will load balance between localhost and an external one.
2. Add more proximity groups for remote servers in specific IP ranges of with specific domain masks.

Each proximity group might contain multiple session managers so PAM will load balance between them inside a group.

Using Proximity Groups with multiple session managers is the way that PAM scales for large or busy environments.

## Double-Hop SSH and RDP Proxy Configuration

Configuring PAM for Double-Hop Remote SSH Proxy, SSH Tunnel and RDP Proxy Sessions.

In order to configure PAM to support a double-hop SSH or RDP Proxy, you will need to deploy more than just a single Session Manager component to your remote server.

Please review the article [Deployment Architecture to Scale Session Manager](#) that discusses the reasons to deploy remote session manager nodes.

Additional components are required for a successful SSH Proxy, SSH Tunnel or RDP Proxy remote connection.

### Configuring components

This article describes the process of deploying and configuring PAM components to setup this Double-Hop scenario.

1. On the [remote Session Manager node server](#) only, run the PAM Setup Installer (Windows or Linux) and select the following components only:
  - Internal Database
  - Directory Service
  - Job Engine
2. Choose the same *Destination Folder* where PAM is currently deployed on this server. We will be adding components to your existing deployment, not creating a new instance.
3. Enter a password for your new pamadmin account on this remote node. It is not required, but if you happen to know the password of this account from your main node(s), then you can use the same here. Otherwise, create a new password and be sure to save it somewhere safe.
4. Do not enable a Federated Connection ("Enable SSO") when asked.
5. Establishing an [Active Directory integration](#) with this node is not required. Simply leave it blank and continue.
6. Save all the installation and password details to a file in save location and **Finish** the installation.
7. The new required components are now installed to your existing node. Next, we will need to enter the new parameters to your remote Session Manager's configuration file.
  - a. On this remote Session Manager node, open the `$PAM_HOME/web/conf/catalina.properties` file in a text editor and add the following (or confirm the parameters if they already exist):
    - **xtam.http.proxy=true**
    - **xtam.http.proxy.port=8081**

- The proxy port defined above, 8081, should match the value in Administration > Settings > Parameters > HTTP Proxy Port on the main PAM node. If you have different value, use that one.
- Please note that this port will need to be opened between the main node and your remote node just as the standard 4822 port is currently configured for remote sessions.

- **cas.tgc.crypto.signing.key=<THE VALUE OF THIS KEY FROM THE MAIN NODE>**

- The value of cas.tgc.crypto.signing.key should be the same as the value of this key in the main node's `$PAM_HOME/web/conf/catalina.properties` file. This parameter might already exist in the remote node file. In this case change its value to match with the value on the main node. Watch for trailing and leading spaces that should be removed. This is the shared key for service authentication.

- Save and close the `catalina.properties` file on the Session Manager node.
- Restart the new **PamManagement** / **pammanager** service running on this remote node.
- Once the remote node is back online (about 3-5 mins), test your SSH/RDP Proxy or Tunnel session.

## Troubleshooting Steps

1. Check that the port (default: 8081) defined in the `catalina.properties` file on the remote node matches the value in the in Administration > Settings > Parameters > HTTP Proxy Port on the main PAM node.
2. Check that the port (default: 8081) defined in the `catalina.properties` file on the remote node is accessible from the main PAM node (telnet from main PAM node to check).
3. Check that Proximity group on the main node GUI for the destination server matches the address on the remote node.
4. Check the value of `cas.tgc.crypto.signing.key` property in `$PAM_HOME/web/conf/catalina.properties` matches between main and remote nodes.

## Front-End Server Architecture

This article discusses front-end server architecture to make Privileged Access Management available from the outside of the corporate network.

## Front-end Architecture for Production Deployment

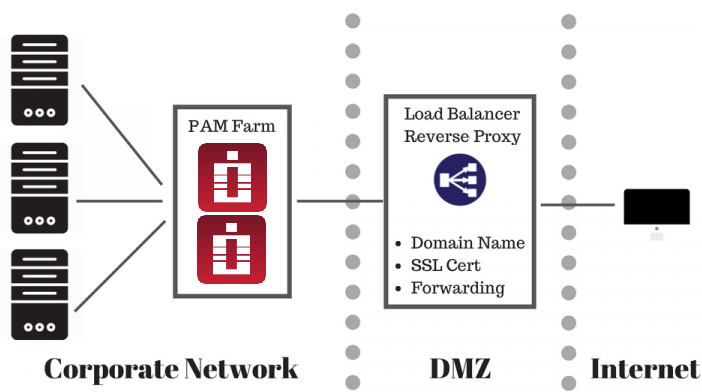
For the production deployment of PAM that could be accessed from the outside of the network we usually recommend to install a reverse proxy (load balancer) on the computer in DMZ to handle the inbound HTTPS traffic with SSL certificates.

This reverse proxy will forward all requests to the PAM server inside the network.

HTTPS configuration with SSL certificate is optional for the trial use to test application functionality.

However, if testing with SSL is desirable or for the production use the pre-requisite is to have a fully qualified domain name (FQDN) resolvable to the PAM reverse proxy computer in DMZ (for example pam.company.com) and an SSL certificate for this FQDN signed by an internet certificate authority trusted by browsers accessing PAM.

In this example PAM will be accessed at <https://pam.company.com/xtam/>.

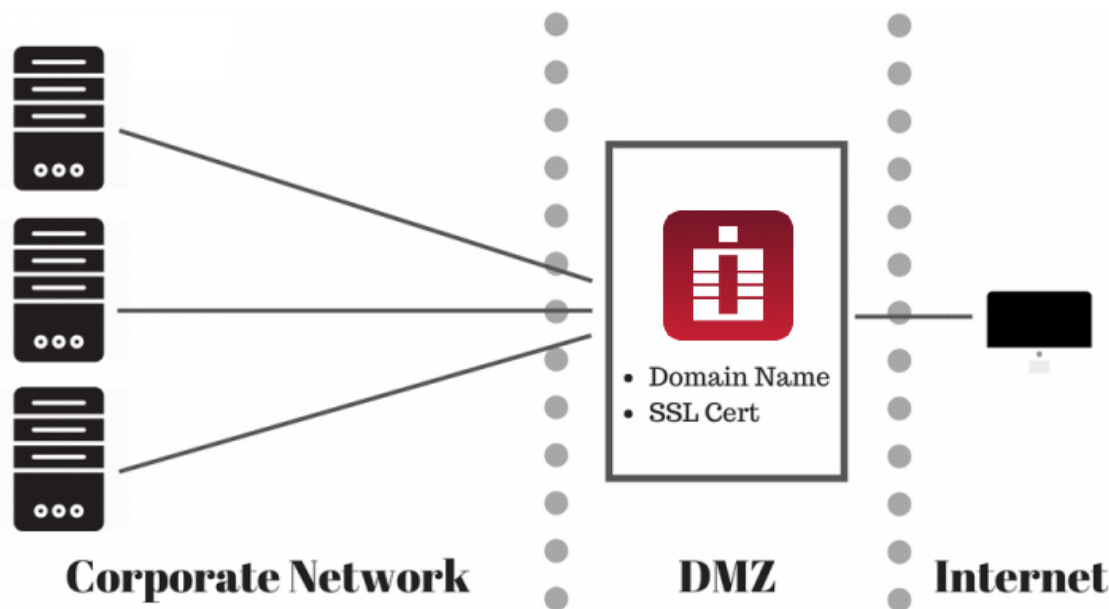


## Front-end Architecture for Test or Trial Deployment

The alternative way to test the external setup is to install PAM itself at the computer in DMZ, [optionally load there a trusted SSL certificate](#) mentioned earlier and switch it to bind directly to HTTP(s) port.

It is slightly easier to do and will demonstrate PAM functionality for the trial purposes.





The discussion below assumes two-server setup with one computer with reverse proxy at DMZ and the other one with PAM behind the firewall.

PAM licensing does not count load balancer / reverse proxy computer as a node to purchase.

## Additional Considerations

When forwarding WEB traffic from a reverse proxy to PAM server using HTTPS protocol make sure that PAM uses trusted certificate or disable certificate check on the load balancer or direct the traffic on the unsecured HTTP port (PAM listens an unprotected HTTP protocol on the port 8080 for test purposes).

Below is an article to [replace generated self-signed certificate of PAM server with the one trusted by the load balancer](#).

Note that PAM server and [load balancers](#) could be installed on similar or on different operating systems (for example, Windows hosting PAM server and Unix hosting the reverse proxy / load balancer). Also, it is possible to utilize existing load balancer in case the one is already in place (for example F5).

If you plan for your users to only use WEB GUI and WEB Sessions then standard HTTPS at port 443 with SSL is enough.

Make sure to enable sticky sessions on the load balancer because RDP and SSH sessions are stateful.

Consider enabling Web sockets since they bring better performance for WEB Sessions (some load balancer might require them enabled separately).

If you plan for your users to use native clients (Putty, mstsc, etc) then you need to open (and load balance) PAM Proxy ports (default are 3388 for RDP proxy, 2022 for SSH Proxy, 8081 for HTTP Proxy).

Keep in mind that there is a constant background port scanning noise in the Internet targeting all ports and all protocols. These events appear in the Audit Log as failed logins with IP address and a user. Deployments might implement white list filtering expected visitors on the [load balancer](#). Deployments might also implement black listing abusers reported in the audit log. Both white and black listing is expected to be on the load balancer side.

## High Availability Configuration for PAM Deployments

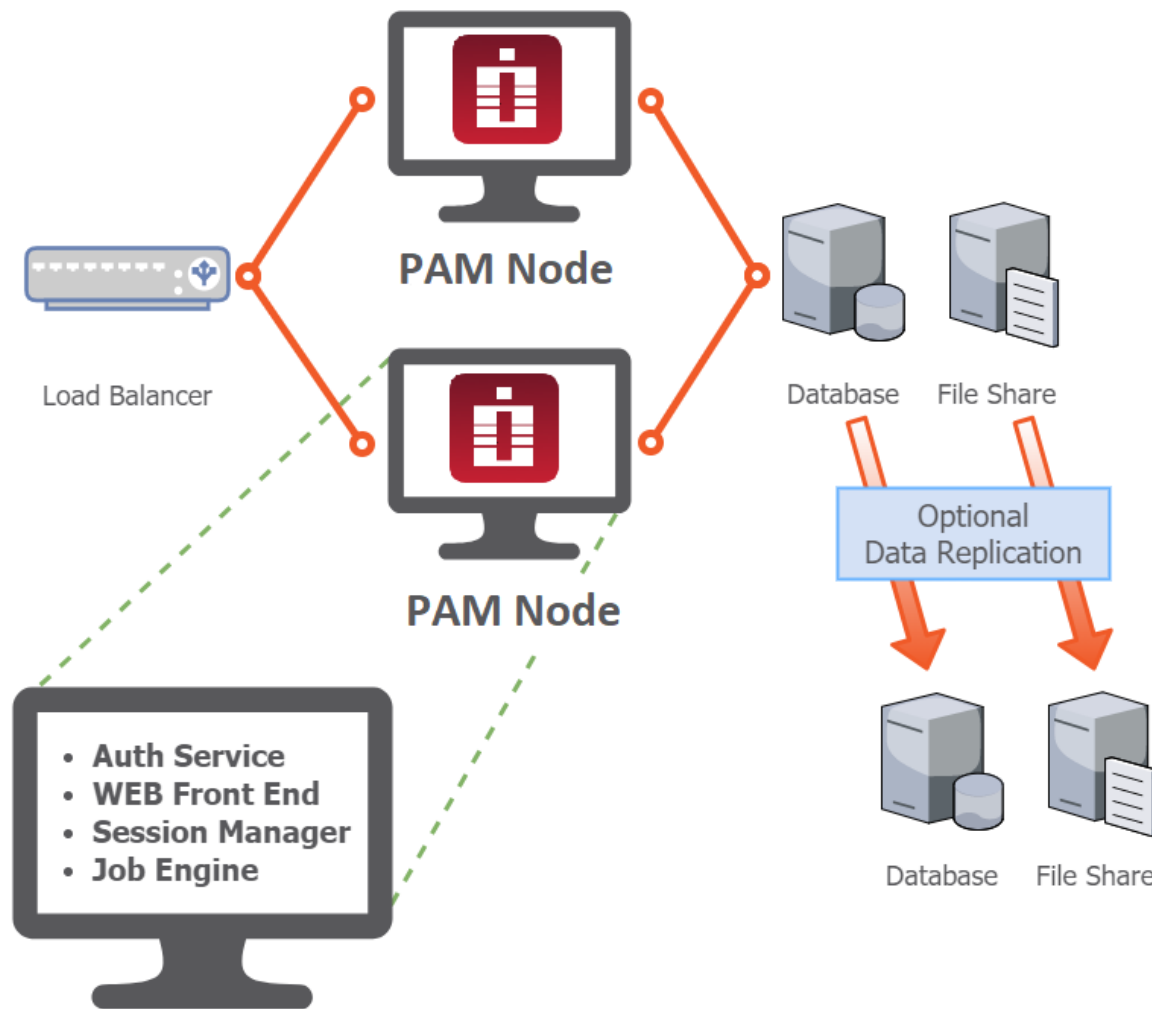
PAM High Availability (HA) option is deployed using two or more PAM nodes with the same software connected to a single database and balancing HTTP traffic using a [Load Balancer](#) or Virtual IP technologies.

PAM HA option allows the system to continue operating in case one of the nodes malfunctions. In addition to that, PAM HA option when deployed using [a load balancer scenario](#) improves overall system performance by splitting the load across multiple nodes.

### High Availability Option Concepts

Below is a basic network diagram that should provide a visual of the following content in this article.

It demonstrates a load balanced instance of PAM, using two PAM nodes with a replicated external database and file share.



High availability farm could be deployed to either a series of Unix or Windows servers, using load balancer to distribute traffic between nodes.

**Server 1:** Hosts Database server. Both PAM nodes A and B will be configured to use this external Database instance as their database.

**Server 2:** Load Balancer. See considerations about selecting a [load balancer](#) below. SSL certificate will be deployed to [Load Balancer](#) for security. Read more about advanced network load balancer deployments in [Front-End Server Architecture](#) article.

**Server 3:** Hosts PAM node A.

**Server 4:** Hosts PAM node B.

The following describes the basic configuration of each server, not the order of operations in which they should be deployed.

Database server should be setup before PAM nodes A and B for example.

## High Availability Option Setup

### 1. Database Server

Install or use an existing Database server. The PAM *Internal Database* is not supported for High Availability deployments. You must use one of the supported [External Database](#) options.

Both PAM nodes will be configured with identical database parameters.

### 2. Load Balancer

[Load Balancer](#) could be used for HA configurations. In this case, Load Balancer has to support sticky sessions (session affinity) in any form (cookie based or IP based) because PAM back end protocols (RDP, SSH) are stateful.

PAM has an option for WEB Sessions (users see RDP screens or SSH terminals in WEB Browser Window) or sessions using native clients ([PuTTY](#), [MS RDP](#), [HTTP proxy](#), etc).

If you plan to use native clients then the load balancer has to support TCP-level balancing (HTTP proxy sessions to WEB Portals run through non-HTTP protocol).

WEB Sessions and WEB GUI could be supported by HTTP-only load balancer.

To illustrate this idea – some TCP level [Load Balancers](#) do not support sticky sessions for multi-zone balancing.

To resolve it, some of our clients use both HTTP Load Balancer for WEB Browsing and WEB Sessions and TCP Load Balancer on different IP and QNAME for native clients while some other clients choose to host PAM nodes in the same zone to use a single TCP LB.

Some TCP Load Balancer (such as F5) do support sticky sessions for multi-zone hosting though.

PAM does not mandate any of these solutions – just be aware about the requirements and check with LB vendor if needed.

Also, you can change LB some time later.

Single node PAM deployment (such as for staging or test areas) could be operated without LB.

PAM can terminate [SSL](#) connection itself, switched to listen on default port 443 (if OS supports it) and serve both WEB GUI, WEB and native sessions.

Multi-node PAM deployments could also operate in standby mode providing HA but not a load distribution.

In this case two PAM nodes could operate on different URLs or use Virtual-IP shifters such as MS NLB or Keealived.

### 3. PAM node A

Install Windows Server and assign a static IP. Reference this IP when configuring the Server Farm in your load balancer.

Run **XtamSetup.exe** and choose the following options:

- Directory Service
- Application GUI
- Job Engine
- Session Manager
- [Federated Sign-In](#) (optional)

When prompted for a database connection, enter the values for your Database server instance.

Configure your AD integration using AD server, user and password.

Complete installation and save your password information to a file.

#### 4. PAM node B

Install Windows Server and assign a static IP. Reference this IP when configuring the Server Farm in your load balancer.

Run **XtamSetup.exe** and choose the following options:

- Directory Service
- Application GUI
- Job Engine
- Session Manager
- [Federated Sign-In](#) (optional).

When prompted for a database connection, enter the values for your Database server instance.

Configure your AD integration using AD server, user and password.

Complete installation and save your password information to a file.

Update the PAM master password on node B with the one from node A by issuing the following command from the command line in \$PAM\_HOME folder:

for Windows:

```
1 | bin\PamDirectory SetMasterPassword web MASTER PASSWORD FROM NODE A
```

for Linux:

```
1 | bin/PamDirectory.sh SetMasterPassword web MASTER PASSWORD FROM NODE A
```

Rather than entering the master password into the command, you can instead use a – (dash character). When this command is executed with a dash, you will be prompted to enter the password.

```
bin\PamDirectory SetMasterPassword web –
bin/PamDirectory.sh SetMasterPassword web –
```

Synchronize keys for SSH, RDP and HTTP Proxies

```
$PAM_HOME/content/keys/sshd.keypair
```

```
$PAM_HOME/content/keys/certificate_rdp.cer
```

```
$PAM_HOME/content/keys/keystore_rdp.p12
```

```
$PAM_HOME/content/keys/certificate.cer
```

```
$PAM_HOME/content/keys/keystore.p12
```

## 5. Setup Federated Sign-In Component in Multi-Node configuration

When using [Federated Sign-In](#) Component for the user authentication, synchronize this module on both nodes by copying the following parameters from `$PAM_HOME/web/conf/catalina.properties` file from PAM Node A to PAM Node B and restart management service on the Node B:

```
1 | cas.ticket.registry.jpa.crypto.signing.key=VALUE
2 | cas.ticket.registry.jpa.crypto.encryption.key=VALUE
3 |
4 | cas.tgc.crypto.encryption.key=VALUE
5 | cas.tgc.crypto.signing.key=VALUE
6 |
7 | cas.webflow.crypto.signing.key=VALUE
8 | cas.webflow.crypto.encryption.key=VALUE
```

## 6. Configure MFA for a Multi-Node Deployment

To support multifactor authentication (MFA) the MFA token on both nodes needs to be synchronized by copying the following parameter's value from the `$PAM_HOME/web/conf/catalina.properties` file on PAM Node A to PAM Node B.

Restart the PAM management service on Node B to finish.

```
1 | xtam.cas.mfa.token=VALUE
```

All token and key settings specific to each MFA provider should be synced between nodes.

## 7. Setup Local User Directory Replication

When using PAM local users and groups, setup up replication between local user directory services on Nodes A and B.

1. On PAM Node A, open a command prompt and navigate to the PAM installation directory.
2. Execute the following command replacing the values with those of PAM Node B:
  - **{ads.remote.server}** : The host name or IP of PAM Node B (make sure port(s) 10636 and 10389 are open)
  - **{ads.remote.password}** : The "Directory Password" of PAM Node B that was generated during installation

for Windows:

```
1 | bin\PamDirectory.cmd ADSReplicate web {ads.remote.server}
   | {ads.remote.password}
```

for Linux:

```
1 | bin/PamDirectory.sh ADSReplicate web {ads.remote.server}
   | {ads.remote.password}
```

3. On PAM Node B, open a command prompt and navigate to the PAM installation directory.
4. Execute the following command replacing the values with those of PAM Node A:
  - **{ads.remote.server}** : The host name or IP of PAM Node A (make sure port(s) 10636 and 10389 are open).
  - **{ads.remote.password}** : The “Directory Password” of PAM Node A that was generated during installation

for Windows:

```
1 | bin\PamDirectory.cmd ADSReplicate web {ads.remote.server}
   | {ads.remote.password}
```

for Linux:

```
1 | bin/PamDirectory.sh ADSReplicate web {ads.remote.server}
   | {ads.remote.password}
```

5. Wait a few minutes for the replication to complete, restart **PamDirectory** Service on PAM Nodes A and B and then refresh your browser.

## Saving to a Shared Network Drive

By default, PAM saves its content (Session Video Recordings, Exports and Temporary files) to a directory in its installation location `$PAM_HOME/content` and the `$PAM_HOME` variable resolves to the *local* install location. Each PAM node will access the Content storage based on its own resolution of the location.

When using multiple nodes, best practice is to use a network share that is accessible by all nodes using that address.

When a user has connected to a specific node and launched an RDP session, and this is recorded, this recording will be stored in the **Content Location** address that the local node resolves to.

When an administrator wants to view the recording, the PAM node that the administrator is log into will try and accessed the recordings also using the **Content Location** address based on its own resolution.

If the default **Content Location** address is still used, the administrator will only be able to view recordings that were recorded by that node.

Trying to view a recording that is in a separate storage location will exhibit the behaviour where the recording just will not play.

No error will be seen.

If nodes are in separate datacentres, it is recommended to use a network share that is locally accessible from each node, but is replicated between datacentres. An example of this is Microsoft DFS.

Configuring PAM to Save Content to a *Shared, Network Drive or Path*.

If you would like to change this path to a shared, network location, please perform the following steps:

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Parameters.
3. Update the path in the following parameters as needed: **Content Location**, **Export Location** and **Temporary Location**.
4. Network locations should be defined like this: `//server/share`
5. Click the **Save** button next to each parameter that has been modified.

For Windows deployments, because PAM is run using the “Local System” account, ensure that this Local System account on the PAM host server has *Read/Write* access to your shared, network drive. If it does not, then the save will fail due to an Access Denied exception.

To test this configuration change, establish a remote session with the recording option enabled and confirm that both directories and the resulting video file (stored as a `.zip` file) are created in your new location or create an **Export** to ensure the export (stored as a `.zip` file) is created in your new location.

## Load Balancer Configuration

### Load Balancer Configuration

This article describes the Load Balancer configuration to serve as a front end for two PAM nodes with sticky sessions options enabled.

Please review the article [Deployment Architecture to Scale Session Manager](#) that discusses the reasons to deploy remote session manager nodes.

#### *Pre-requisites*

- Load Balancer should operate on Layer 4 (tcp) for proxies and the application Layer 7 for *http/https* processing.
- Sticky sessions should be *enabled* on the Load Balancer.

Follow the links to configure a Load Balancer enabled for:

[Apache HTTP Server with Sticky Sessions](#)

[HTTPS Load Balancer in a Linux deployment of PAM](#)

[NGINX](#).

If you have any questions as for the Load Balancer configuration, please them the Support team:

<https://support.imprivata.com/communitylogin>.

### Apache HTTP Server with Sticky Sessions

This article discusses the details of the Apache HTTP Server Load Balancer configuration to serve as a front end for two PAM nodes with sticky sessions options enabled. Please refer to the following [diagram for the deployment](#).

Apache HTTPS server in this example utilizes the module **mod\_ssl**. Make sure to install this module and enable it in the Apache server configuration.



For SELinux allow HTTPS server to connect using the command:

```
1 | setsebool -P httpd_can_network_connect 1
```

The reverse proxy configuration is summarized in the SSL Virtual Host specification file below:

```
1 <VirtualHost *:80>
2     ServerName xtam-cos-farm.yourdomain.com
3     Redirect / https://xtam-cos-farm.yourdomain.com/xtam/
4     Redirect /xtam/ https://xtam-cos-farm.yourdomain.com/xtam/
5 </VirtualHost>
6
7 <VirtualHost *:443>
8     SSLEngine on
9     SSLProxyEngine on
10
11     # followed 2 directives were set for being able to use self-signed
certificates on farm nodes
12     SSLProxyCheckPeerCN off
13     SSLProxyCheckPeerName off
14
15     ServerName xtam-cos-farm.yourdomain.com
16
17     <Proxy balancer://xtam-https-balancer>
18         BalancerMember https://<hosta-address>:6443 route=hosta
19         BalancerMember https://<hostb-address>:6443 route=hostb
20         ProxySet lbmethod=byrequests
21         ProxySet stickysession=JSESSIONID
22     </Proxy>
23
24     <Proxy balancer://xtam-ws-balancer>
25         BalancerMember ws://<hosta-address>:6443 route=hosta
26         BalancerMember ws://<hostb-address>:6443 route=hostb
27         ProxySet lbmethod=byrequests
28         ProxySet stickysession=JSESSIONID
29     </Proxy>
30
31     ProxyPass / balancer://xtam-https-balancer/
32     ProxyPassReverse / balancer://xtam-https-balancer/
33
34     ProxyPass /xtam/websocket-tunnel balancer://xtam-ws-balancer/xtam/websocket-
tunnel
35     ProxyPassReverse /xtam/websocket-tunnel balancer://xtam-ws-
balancer/xtam/websocket-tunnel
36
37     SSLCertificateFile /etc/ssl/certs/cert-name.crt
38     SSLCertificateKeyFile /etc/pki/tls/private/private_key.key
39 </VirtualHost>
```

On the PAM nodes modify Engine tag in `$PAM_HOME/web/conf/server.xml` file. This tag should include `jvmRoute` attribute identifying this node for the Apache server. Use **hostb** on the second PAM node `server.xml` file.

Note that load balancer configuration above references both `hosta` and `hostb` identifiers using route attribute of Proxy node description. You can use different identifiers but they have to match between the node `server.xml` and load balancer configuration files.

```
1 | <Engine name="Catalina" defaultHost="localhost" jvmRoute="hosta">
```

## Debian and Ubuntu Linux Load Balancer

### Objective

The objective of this guide is to configure a HTTPS enabled load balancer for a single server PAM system on a Linux host computer.

Note that there are multiple architectures and products that can be used for load balancing of WEB applications all involving different configuration files and mechanisms to obtain and deploy a SSL certificate.

This guide will describe one of the methods to illustrate components and files required in the process.

### Pre-requisites

- OS Debian / Ubuntu with Apache HTTP Server installed.
- URI for PAM setup that might be used as a managed path for PAM SSO Server (such as <https://pam.-company.com>) so that an external computer can access the PAM server using this URL.
- SSL certificate from a trusted Certificate Authority. Note that the certificate should be trusted by all client and server side system components (browsers and WEB containers) in order for the SSO server to work.

The certificate contains the following files:

- The certificate (the guide assumes the name `cert.crt`)
- Server private Key (the guide assumes the name `private.key`)
- Optional: CA bundle certificate (the guide assumes the name `ca-bundle.crt`)
- Optional: Certificate chain file (the guide assumes the name `server-ca.crt`)

### Configuration

1. **Check Apache HTTP Server with `httpd` and `mod_ssl` packages installed.** These packages might not be installed on a default Ubuntu distribution.

To **install** the packages use the following commands:

```
1 | apt-get install apache2
2 | a2enmod ssl proxy proxy_http proxy_wstunnel
3 | a2ensite default-ssl
4 | service apache2 restart
```

2. **Copy** the certificate files into the `/etc/apache2/ssl/` directory. **Change** the permissions of the private key so only root can access it using these commands:

```
1 | chown root /etc/apache2/ssl/private.key
2 | chmod 600 /etc/apache2/ssl/private.key
```

3. **Add** the SSL and Load Balancer configuration to the Apache HTTP Server.

**Edit** the file `/etc/apache2/sites-enabled/default-ssl.conf` and locate the line:

```
1 | VirtualHost _default_:443
```

- a. **Add** the load balancer configuration after this line:

```
1 | ProxyPass /xtam/websocket-tunnel ws://127.0.0.1:8080/xtam/websocket-tunnel
2 | ProxyPassReverse /xtam/websocket-tunnel
  | ws://127.0.0.1:8080/xtam/websocket-tunnel
3 |
4 | ProxyPass /xtam/ http://127.0.0.1:8080/xtam/
5 | ProxyPassReverse /xtam/ http://127.0.0.1:8080/xtam/
6 |
7 | ProxyPass /cas/ http://127.0.0.1:8080/cas/
8 | ProxyPassReverse /cas/ http://127.0.0.1:8080/cas/
```

- b. **Add** the SSL certificates to the same file:

Locate line starting with `SSLCertificateFile`, **uncomment** it and **add the path** to the certificate:

```
1 | SSLCertificateFile /etc/apache2/ssl/cert.crt
```

Locate line starting with `SSLCertificateKeyFile`, **uncomment** it and **add the path** to the private key:

```
1 | SSLCertificateKeyFile /etc/apache2/ssl/private.key
```

Optionally, locate line starting with `SSLCACertificateFile`, **uncomment** it and **add the path** to the chain file:

```
1 | SSLCACertificateFile /etc/apache2/ssl/ca-bundle.crt
```

Optionally, locate line starting with `SSLCertificateChainFile`, **uncomment** it and **add the path** to the chain file:

```
1 | SSLCertificateChainFile /etc/apache2/ssl/server-ca.crt
```

- c. **Save and close** the file.

4. **Restart** the Apache HTTP Server.

```
1 | service apache2 restart
```

# HTTPS Load Balancer in a Linux deployment of PAM

Configuring an HTTPS secured load balancer can be achieved by performing the steps outlined in the following guides.

Please note that our guides will assume a single node PAM deployment with Apache HTTP.

[For Red Hat or CentOS, please review this guide](#)

[For Debian or Ubuntu, please review this guide](#)

## Red Hat and CentOS Linux Load Balancer

Configuring a load balancer in Red Hat or CentOS Linux for PAM deployments.

### Objective

The objective of this guide is to configure a HTTPS enabled load balancer for a single server PAM system on a Linux host computer.

Note that there are multiple architectures and products that can be used for load balancing of WEB applications all involving different configuration files and mechanisms to obtain and deploy a [SSL certificate](#).

This guide will describe one of the methods to illustrate components and files required in the process.

### Pre-requisites

- OS Red Hat / CentOS with Apache HTTP Server installed.
- URI for PAM setup that might be used as a managed path for PAM SSO Server (such as <https://pam.company.com>) so that an external computer can access the PAM server using this URL.
- SSL certificate from a trusted Certificate Authority. Note that the certificate should be trusted by all client and server side system components ([browsers](#) and [WEB containers](#)) in order for the [SSO](#) server to work. The certificate contains the *following files*:

- The certificate (the guide assumes the name `cert.crt`)
- Server private Key (the guide assumes the name `private.key`)
- Optional: CA bundle certificate (the guide assumes the name `ca-bundle.crt`)
- Optional: Certificate chain file (the guide assumes the name `server-ca.crt`).

### Configuration

1. **Check `httpd` and `mod_ssl` packages** are installed and enabled in the Apache HTTP Server. They are enabled in the default CentOS setup but this should be confirmed.

To do that, check the file `/etc/httpd/conf.modules.d/00-proxy.conf` and **uncomment** the following lines:

```
1 | LoadModule proxy_module modules/mod_proxy.so
2 | LoadModule proxy_http_module modules/mod_proxy_http.so
3 | LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so
```

If these lines are not present then **install** *httpd* and *mod\_ssl* with the following command:

```
1 | yum install httpd mod_ssl
```

2. **Copy** the certificate files into the `/etc/pki/tls/certs/` directory and change permissions of the private key so only root can access it using these commands:

```
1 | chown root /etc/pki/tls/private/private.key
2 | chmod 600 /etc/pki/tls/private/private.key
```

3. **Add** the SSL and Load Balancer configuration to the Apache HTTP Server.

Edit the file `/etc/httpd/conf.d/ssl.conf` and locate the line:

```
1 | VirtualHost _default_:443
```

- a. **Add the load balancer configuration** after this line:

```
1 | ProxyPass /xtam/websocket-tunnel ws://127.0.0.1:8080/xtam/websocket-tunnel
2 | ProxyPassReverse /xtam/websocket-tunnel
  | ws://127.0.0.1:8080/xtam/websocket-tunnel
3 |
4 | ProxyPass /xtam/ http://127.0.0.1:8080/xtam/
5 | ProxyPassReverse /xtam/ http://127.0.0.1:8080/xtam/
6 |
7 | ProxyPass /cas/ http://127.0.0.1:8080/cas/
8 | ProxyPassReverse /cas/ http://127.0.0.1:8080/cas/
```

- b. **Add the SSL certificates** to the same file:

Locate the line starting with *SSLCertificateFile*, **uncomment** it and **add the path** to the certificate:

```
1 | SSLCertificateFile /etc/pki/tls/certs/cert.crt
```

Locate the line starting with *SSLCertificateKeyFile*, **uncomment** it and **add the path** to the private key:

```
1 | SSLCertificateKeyFile /etc/pki/tls/private/private.key
```

Optionally, locate the line starting with *SSLCACertificateFile*, **uncomment** it and **add the path** to the chain file:

```
1 | SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
```

Optionally, locate the line starting with `SSLCertificateChainFile`, **uncomment** it and **add the path** to the chain file:

```
1 | SSLCertificateChainFile /etc/pki/tls/certs/server-ca.crt
```

c. **Save and close** the file.

4. **Change** the setting for the Apache HTTP Server by issuing this command:

```
1 | /usr/sbin/setsebool -P httpd_can_network_connect 1
```

5. **Restart** the Apache HTTP Server:

```
1 | service httpd restart
```

## NGINX Configuration

Centos:

```
1 | yum install nginx
2 | setsebool -P httpd_can_network_connect 1
```

Ubuntu:

```
1 | apt install nginx
```

### *Nginx config for reverse proxy:*

You should name it a name such as `xtam.conf` or something similar and put it in `/etc/nginx/conf.d/`

```
1 | map $http_upgrade $connection_upgrade {
2 |     default      upgrade;
3 |     ''           close;
4 | }
5 |
6 | server {
7 |     listen 80;
8 |     server_name xtam.yourdomain.com;
9 |     # redirect all HTTP requests to HTTPS
10 |    location / {
11 |        return 301 https://$server_name$request_uri;
12 |    }
13 | }
14 |
15 | server {
16 |     listen 443 ssl http2;
17 |     ssl_protocols TLSv1.3 TLSv1.2;
18 |     ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384
19 | EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH
EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4";
    server_name xtam.yourdomain.com;
```

```

20     ssl_certificate      /etc/pki/tls/certs/cert.crt;
21     ssl_certificate_key  /etc/pki/tls/private/private_key.key;
22
23     location / {
24         proxy_set_header Host $host;
25         proxy_set_header X-Real-IP $remote_addr;
26         proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
27         proxy_pass https://xtam.yourdomain.com:6443;
28         proxy_buffering off;
29     }
30
31     # Websocket configuration
32     location /xtam/websocket-tunnel {
33         proxy_pass https://xtam.yourdomain.com:6443;
34         proxy_http_version 1.1;
35         proxy_set_header Upgrade $http_upgrade;
36         proxy_set_header Connection $connection_upgrade;
37     }
38 }

```

On SELinux-enabled systems you can get *"502 Bad gateway error"* when trying to access your reverse-proxied address with followed errors in `/var/log/nginx/error.log`: *"connect() to <some\_ip\_here:6443> failed (13: Permission denied) while connecting to upstream"*

You need to check if such port is allowed `http_port_t`:

```
1 | semanage port -l | grep http_port_t
```

If it's not, allow it by issuing the followed command:

```
1 | semanage port -a -t http_port_t -p tcp 6443
```

## Nginx config for web load balancer

You should name it a name such as `xtam_lb.conf` or something similar and put it in `/etc/nginx/conf.d/`

```

map $http_upgrade $connection_upgrade {
    default      upgrade;
    ""           close;
}

upstream backend_web {
    hash $remote_addr;
    server xtamcentoshosta:6443;
    server xtamcentoshostb:6443;
}

```

```

server {
    listen 80;
    server_name xtam-farm.yourdomain.com;
    # redirect all HTTP requests to HTTPS
    location / {
        return 301 https://$server_name$request_uri;
    }
}

server {
    listen 443 ssl http2;
    server_name xtam-farm.yourdomain.com;
    ssl_certificate      /etc/pki/tls/certs/cert.crt;
    ssl_certificate_key  /etc/pki/tls/private/private_key.key;

    location / {
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_pass https://backend_web;
    }

    # Websocket configuration
    location /xtam/websocket-tunnel {
        proxy_pass https://backend_web;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection $connection_upgrade;
        proxy_set_header Host $host;
    }
}

```

### *Nginx additional config for tcp load balancer for proxies:*

On Centos distributions streams section does not exists in `/etc/nginx/nginx.conf`.

To continue with this manual you should add following to the end of `/etc/nginx/nginx.conf`:

```

1 | stream {
2 |     include /etc/nginx/conf.d/*.tcp;
3 | }

```

Place `xtam.tcp` file to `/etc/nginx/conf.d/`:

```

1 | upstream http_proxy {
2 |     hash $remote_addr;
3 |     server xtamcentoshosta:8081;
4 |     server xtamcentoshostb:8081;
5 | }
6 |
7 | upstream ssh_proxy {
8 |     hash $remote_addr;
9 |     server xtamcentoshosta:2022;

```



```

10 |     server xtamcentoshostb:2022;
11 | }
12 |
13 | upstream rdp_proxy {
14 |     hash $remote_addr;
15 |     server xtamcentoshosta:3388;
16 |     server xtamcentoshostb:3388;
17 | }
18 |
19 | server {
20 |     listen 8081;
21 |     proxy_pass http_proxy;
22 | }
23 |
24 | server {
25 |     listen 2022;
26 |     proxy_pass ssh_proxy;
27 | }
28 |
29 | server {
30 |     listen 3388;
31 |     proxy_pass rdp_proxy;
32 | }

```

On SELinux-enabled systems, by default, the SELinux configuration does not allow NGINX to listen (bind()) to TCP or UDP ports other than the default ones that are allow-listed in the **http\_port\_t** type.

You can check this by running the following command:

```
1 | semanage port -l | grep http_port_t
```

So you'll need to add proxy ports to this type:

```

1 | semanage port -a -t http_port_t -p tcp 2022
2 | semanage port -a -t http_port_t -p tcp 3388
3 | semanage port -a -t http_port_t -p tcp 8081

```

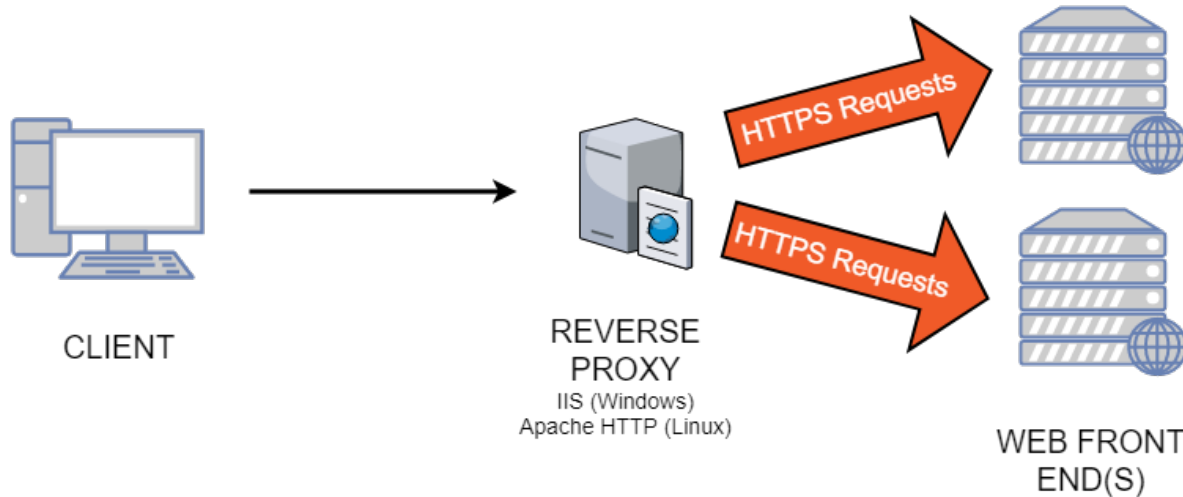
You can get the following error: *"ValueError: Port tcp/8081 already defined"*, in such case you should use slightly modified command for that port:

```
1 | semanage port -m -t http_port_t -p tcp 8081
```

# Securing Traffic Between a Load Balancer and PAM

Although some people consider securing the internal traffic inside PAM server farm an unnecessary overkill, others may consider it a potential security vulnerability.

Regardless of either position, the PAM solution does provide a rather straightforward process to secure the traffic between a load balancer and your PAM web container(s).



Before you begin, please consider the following:

- This applies to deployments where one or more PAM nodes are configured behind a load balancer (as shown in the graphic above) or it could be used to secure external traffic to the PAM server without the use of a load balancer.
- This requires that you have possession of a SSL certificate from a trusted CA. One is required if it is configured for wildcards, however multiple may be necessary if the URL is explicitly defined.
- If your security certificates are packaged in a format different than PFX, please contact our Support Team <https://support.imprivata.com/communitylogin> for additional assistance.
- If your PAM instance was deployed prior to April 2, 2018, please contact our Support Team <https://support.imprivata.com/communitylogin> for additional assistance.
- If you are unsure if this is necessary for your deployment, please consult with your security or IT department.

## Pre-requisites

1. A deployed PAM instance that is accessible from a load balancer, not configured to use localhost. Your PAM instance should be using a URL like <https://pam.company.com:8080/xtam>.
2. Your Load Balancer (Microsoft IIS or Apache HTTPD Server) is configured to pass external traffic to PAM server using re-write rules to HTTP port 8080.
3. Trusted SSL certificate file in PFX format and its associated password for your domain name like in item 1

above. In our example, that certificate would be for *pam.company.com* or *\*.company.com*.

**Note:** If you are using Apache, then the `.pfx` file will need to be converted from individual certificate and private key files.

## Configuring your PAM Web Container(s) to accept HTTPS Traffic

1. Login to the server that is hosting your PAM server.
2. Open a command window and navigate to `$PAM_HOME`. This is the installation folder for PAM.
3. Next, we will need to encrypt your SSL certificate password by using the command below. This will generate your encrypted certificate password that will be used in a later step.
  - a. For Windows, substitute your SSL certificate password with `{PASSWORD}` and issue this command:

```
1 | bin\PamDirectory Encrypt {PASSWORD}
```

- b. For Unix, substitute your SSL certificate password with `{PASSWORD}` and issue this command:

```
1 | bin/PamDirectory.sh Encrypt {PASSWORD}
```

4. Open the file `$PAM_HOME/web/conf/server.xml`. Locate this line in the file:

```
1 | <!-- Define an AJP 1.3 Connector on port 8009 -->
```

Immediately before that line, paste the following text:

```
1 | <Connector
2 |     keystoreFile="PATH_TO_CERTIFICATE.pfx" keystorePass="ENCRYPTED_OR_
   | CLEAR_PASSWORD"
3 |     protocol="com.pam.config.Http11NioEncryptedProtocol"
4 |     port="8443" maxThreads="200"
5 |     scheme="https" secure="true" SSLEnabled="true" proxyPort="443"
6 |     clientAuth="false" sslProtocol="TLS" keystoreType="PKCS12"/>
```

5. In the above pasted text, replace

`keystoreFile="PATH_TO_CERTIFICATE.pfx"` with your SSL certificate location;

keystorePass="ENCRYPTED\_OR\_CLEAR\_PASSWORD" with your encrypted password from step 3, that includes everything in the output except *Ok*:

6. Save and close this `server.xml` file.
7. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service.
8. When the service is running again (takes ~ 60 seconds), check the PAM server availability to server SSL traffic from the load balancer server using a URL similar to this: <https://pam.company.com:8443/xtam/>
9. Re-write your load balancer rules referenced in **Pre-requisite #2** to access the downstream PAM server using the HTTPS protocol. When finished, restart IIS or Apache.
10. Test PAM accessibility from all available locations, internally and optionally externally, to ensure communication and functionality is working as it was previously.
11. *(Optional)* You may now disable the connector on port 8080 also configured in the `server.xml` file. The disabled connector will look like this:

```
<!--  
    <Connector port="8080" protocol="HTTP/1.1"  
        connectionTimeout="20000" secure="true"  
        redirectPort="8443" />  
-->
```

12. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service.

## PAM Health Check Page

PAM Status or Health Check Page.

PAM comes with a default status or healthcheck page that can be used by systems like Load Balancers to determine if the application is online or offline.

The health check page includes information like **Host Name**, **Current Time** and **Operating System**.

If the page does not load or respond, then the application can be considered to be offline.

The PAM health check page can be accessed from `$PAM_URL/healthcheck`.

For example, <https://xtam.company.com/xtam/healthcheck>

- The health check process attempts to directly connect to the endpoint of the following components: SSH, RDP, HTTP Proxy, all integrated LDAP servers and also verifies the other nodes check-in times.

- The results of the health check are reported on the node monitoring page and also posted on the [Audit Log](#).
- In addition to the notifications about the failed components posted to the audit log on the Warning level, the system also posts periodic (once an hour) heartbeat audit log messages on the Information level confirming the expected operation of system components and integrated user directories.
- Administrators can subscribe to the audit log *Health Check* events or to SIEM system messages to receive notifications about failure in the system components or heartbeat stream to confirm normal operation.

## Multi-Replication of Directory Services Nodes (3+)

When deploying PAM to three or more nodes, its internal directory services can be setup for replication to support several scenarios.

In this guide, we will walk-through a few of these scenarios and provide the commands to enable this configuration.

To begin, we will use the example of a three node deployment and we will label the Directory Services on each as NodeA, NodeB and NodeC for illustrative purposes.

You will need to provide the hosts for each node (IP, hostname, etc.), the Directory Password that was generated during installation of each node and they must be reachable on your network.

The first scenario will describe the deployment where all nodes will replicate to each other. Meaning NodeA > NodeB, NodeA > NodeC, NodeB > NodeA, NodeB > NodeC and NodeC > NodeA, NodeC > NodeB.

Beginning on NodeA, we will configure the replication to NodeB and NodeC using the following command from `$PAM_HOME`:

for Windows deployments:

```
1 | bin\PamPamDirectory.cmd ADSReplication web {replicationContainerSlot}
   | {ads.server.NodeB} {ads.password.NodeB}
```

for Linux deployments:

```
1 | bin/PamDirectory.sh ADSReplication web {replicationContainerSlot}
   | {ads.server.NodeB} {ads.password.NodeB}
```

**{replicationContainerSlot}** – This will define the position of the replication within the node configuration. Value should begin at one.

**{ads.server.NodeB}** – This will define the hostname of the remote Directory Services node that is being replicated to.

**{ads.password.NodeB}** – This will define the Directory Password of the remote Directory Services node that is being replicated to.

Using the above as guidance, our commands executed from NodeA would look like this (assuming a Windows deployment):

```
1 | bin\PamDirectory.cmd ADSReplication web 1 xtamNodeB AYhK8QvjPFKXc8
```

```
1 | bin\PamDirectory.cmd ADSReplication web 2 xtamNodeC haqVYk5p3y23L2
```

Then on NodeB, we will configure replication with NodeA and NodeC:

```
1 | bin\PamDirectory.cmd ADSReplication web 1 xtamNodeA 7tEEed8H95aJsS8
```

```
1 | bin\PamDirectory.cmd ADSReplication web 2 xtamNodeC haqVYk5p3y23L2
```

And finally, on Node C we will configure replication with NodeA and NodeB:

```
1 | bin\PamDirectory.cmd ADSReplication web 1 xtamNodeA 7tEEed8H95aJsS8
```

```
1 | bin\PamDirectory.cmd ADSReplication web 2 xtamNodeB AYhK8QvjPFKXc8
```

Once replication is successfully configured on each node, the process will begin shortly.

Additional commands are available to display a list of already configuration replication pairs and to delete a replication target from the source node.

To list the replication targets on a node:

```
1 | bin\PamDirectory.cmd ADSReplication web list
```

To delete a replication target on a node:

```
1 | bin\PamDirectory.cmd ADSReplication web {replicationContainerSlot} delete
```

The other scenario we will describe is one where you want to setup a Master-Slave replication deployment where NodeA is the master and will be replicated to NodeB and NodeC, common use case might be for the purposes of replicating production to a staging or test environment.

Meaning NodeA > NodeB and NodeA > NodeC only.

In this deployment scenario, we will only be executing the replication commands from NodeB and NodeC as they are taking data from NodeA.

On NodeB,

```
1 | bin\PamDirectory.cmd ADSReplication web 1 xtamNodeA 7tEEd8H95aJsS8
```

And on NodeC,

```
1 | bin\PamDirectory.cmd ADSReplication web 1 xtamNodeA 7tEEd8H95aJsS8
```

Once configured, you can use the list command to verify the replication targets:

```
1 | bin\PamDirectory.cmd ADSReplication web list
```

And you can use the delete parameter to remove a replication target (i.e. delete NodeA from the configuration on NodeB):

```
1 | bin\PamDirectory.cmd ADSReplication web 1 delete
```

## Troubleshooting

If services need to be restarted for troubleshooting, they should be done so in this order:

1. Stop PamManagment or pammanager.
2. Stop PamDirectory or pamdirectory.
3. Start PamDirectory or pamdirectory.
4. Start PamManagement or pammanager.

## Transparent Perimeter deployment

Transparent Perimeter deployment option provides access to closed isolated networks behind firewall based on the reverse tunnel architecture.

The option improves security of the isolated network under management by allowing external parties to access assets inside the network with no requirements to open ports in the network firewall.

Transparent Perimeter deployment is a useful addition to an MSP looking to manage client networks with no interference with the network perimeter.

The option is also useful for organizations accessing on-premises or multi-cloud data-centers using cloud-deployed Master PAM cluster.

The Transparent Perimeter feature complements the existing Remote Node deployment scenario that requires a firewall rule to open the port in the isolated network to provide secure encrypted Master Node connectivity to the Remote Node.

For Windows 10 hosts the optional feature OpenSSH Service should be enabled following [these instructions](#).

## Remote Worker Nodes for multiple Master Nodes

Remote Worker Nodes are able to service multiple Master Nodes.

This option allows organizations to architect efficient access network servicing assets hosted at the same cloud datacenter to independent clients.

This function is useful for an MSP providing access to assets of multiple clients hosted at the same datacenter to several internal or external groups managing those assets.

In this case, one single remote node cluster inside the datacentres will serve all groups each with the independent master nodes interested to manage these assets.

The function also provides MSP with the cost-efficient option to gradually migrate managed assets from multiple clients datacenters into a hosted cloud location reusing the access infrastructure of a hosted cloud network.

Use the following configuration on the remote node to configure multiple master node connections.

- `xtam.remote[0].enabled` = **Flag to enable master node configuration for multi-master node deployment**
- `xtam.remote[0].url` = **Master node URL in multi-master node deployment**
- `xtam.remote[0].user` = **Master node user in multi-master node deployment**
- `xtam.remote[0].password` = **Master node password in multi-master node deployment**
- `xtam.remote[0].token` = **Master node password token in multi-master node deployment to use instead of user and password**

Note that the index in the master node configuration allows specifying multiple connections.

Also, note that the default configuration is given by `xtam.remote.*` parameters are still necessary and used to designate a primary master node connection to serve as a main monitoring point for the remote node.

## Transparent Perimeter

The Transparent Perimeter feature might be used to provide low level traffic connectivity to networks with high security requirements or to quickly investigate test scenarios.

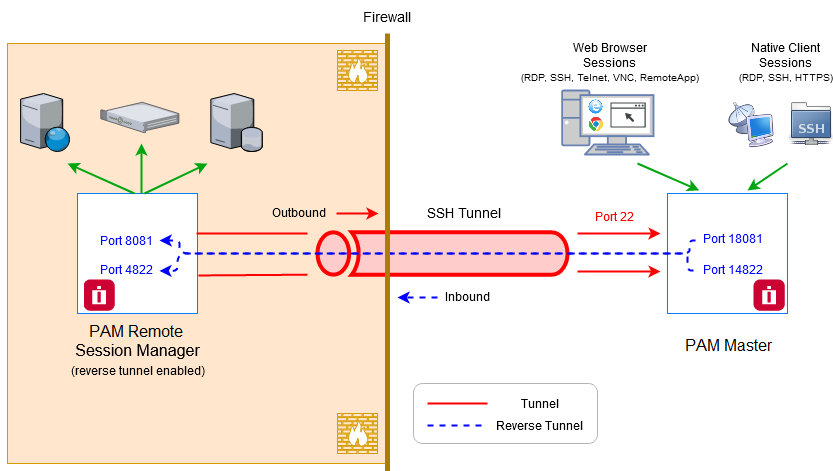
This deployment scenario requires hosts of PAM Master nodes to provide [SSH Tunneling](#) capability for the remote node.

In this configuration, PAM Remote Node deployed to the closed isolated network builds and maintains reverse SSH tunnels back to the master nodes using configured port on the master node.

It allows administrators to configure Session Manager Proximity Group in PAM Master node for the localhost port exposing remote session manager inside the isolated network.



## PAM Transparent Perimeter Deployment



Note that in order for a user to be able establish a connection from Session Manager node (remote node) to the PAM master node, a user should be part of OS local account. Whatever user is listed in **xtam.reverse.tunnel[0].remoteUser** in `catalina.properties` should be added in OS level on the master nodes (not PAM).

The configuration for the reverse tunnels is performed using the following properties on the remote node in `$PAM_HOME/web/conf/catalina.properties` file:

- `xtam.reverse.tunnel[0].remoteHost`=Master node host for SSH connection
- `xtam.reverse.tunnel[0].remotePort`=Master node port for SSH connection
- `xtam.reverse.tunnel[0].remoteUser`=Master node user for SSH connection
- `xtam.reverse.tunnel[0].remotePassword`=Master node user password or Private Key password for SSH connection
- `xtam.reverse.tunnel[0].remoteKey`=Path to master node Private Key for SSH connection as an alternative for remoteUser
- `xtam.reverse.tunnel[0].forwardHost`=Session manager host in the isolated network in the local isolated network space
- `xtam.reverse.tunnel[0].forwardPortLocal`=Session manager port in the isolated network
- `xtam.reverse.tunnel[0].forwardPortRemote`=Session manager port on the master node to use in the proximity group
- `xtam.reverse.tunnel[0].forwardBindingAddress`=Binding address on the master node to expose the port to other interfaces
- `xtam.reverse.tunnel[0].aliveInterval`=Sets the server keep-alive interval property in milliseconds. If 0 is specified, no keep-alive message will be sent. The default interval is 10000.
- `xtam.reverse.tunnel[0].aliveCountMax`=Sets the number of keep-alive messages which may be sent without receiving any messages back from the server. If this threshold is reached while keep-alive messages are being sent, the connection will be disconnected. The default value is 20

Note that index in **xtam.reverse.tunnel** configuration allows to specify multiple tunnels maintained by the remote node. Reverse tunnel [SSH connection](#) could be established using user / password or user / private key (optionally with password).

In addition to reverse tunnel, the node is capable to establish and to maintain forward tunnel to the master node to limit all traffic from the remote node to the master node to SSH tunnel **port 22** including HTTPS traffic from remote worker to the master node as well as reverse traffic from the master node to remote session managers.

The option further simplifies remote network requirements for the remote node configuration.

The configuration for the forward tunnels is performed using the following properties on the remote node in `$PAM_HOME/web/conf/catalina.properties` file:

- `xtam.forward.tunnel[0].remoteHost`=Master node host for SSH connection
- `xtam.forward.tunnel[0].remotePort`=Master node port for SSH connection
- `xtam.forward.tunnel[0].remoteUser`=Master node user for SSH connection
- `xtam.forward.tunnel[0].remotePassword`=Master node user password or Private Key password for SSH connection
- `xtam.forward.tunnel[0].remoteKey`=Optional path to master node Private Key for SSH connection as an alternative for `remoteUser`
- `xtam.forward.tunnel[0].forwardHost`=Host in the master node network to forward tunnel to
- `xtam.forward.tunnel[0].forwardPortLocal`=Forwarded port on the remote node to map as a master node port
- `xtam.forward.tunnel[0].forwardPortRemote`=Master node port to forward traffic to (usually 443)
- `xtam.forward.tunnel[0].forwardBindingAddress`=Binding address on the remote node to expose the port to other interfaces
- `xtam.forward.tunnel[0].aliveInterval`=Sets the server keep-alive interval property in milliseconds. If 0 is specified, no keep-alive message will be sent. The default interval is 10000
- `xtam.forward.tunnel[0].aliveCountMax`=Sets the number of keep-alive messages which may be sent without receiving any messages back from the server. If this threshold is reached while keep-alive messages are being sent, the connection will be disconnected. The default value is 20.

Note that index in **xtam.forward.tunnel** configuration allows to specify multiple tunnels maintained by the remote node. Forward tunnel [SSH connection](#) could be established using user / password or user / private key (optionally with password).

Also note that for proper HTTPS configuration the remote node DNS resolution of the master node name should be defined for the local host of the remote node.

## Silent Installer for Linux Platforms

The [silent installer](#) for Linux platforms accepts command line parameters as configuration options for the specific deployment replacing interactive communication with the user using the options provided in the command line.

With all options required to complete the installation specified in the command line the installer completes automatically without operator attention.

The options also include destination location and the file to store generated credentials.

Command line parameters could be used to supplement interactive installation or to facilitate automated deployment.

The silent installer option is useful for deployment automation and repeat-ability in large environments, elastic provisioning of new systems in cloud or closed data-center environments and cleaner separation of system ownership, administration and deployment roles by limiting exposure of sensitive system keys and passwords.

Silent installer for Linux platforms includes the following parameters:

- **-eula** – Accept EULA
- **-db** – install embedded database
- **-nodb Oracle | MSSQL | MySQL | PostgreSQL SERVER USER PASSWORD** – connect to external database
- **-dir** – install Directory Services
- **-nodir SERVER PASSWORD** – connect to external Directory Services
- **-gui** – install the application GUI
- **-nogui** – install the application without GUI component
- **-worker** – install the application Worker process
- **-noworker** – install the application without Worker process
- **-session** – install session manager
- **-nosession** – install the application without session manager
- **-cas** – install Federated Sign-In Module
- **-casversion CAS52 | CAS65** - version of Federated Sign-In Module
- **-nocas** – install the application without Federated Sign-In Module
- **-ldap SERVER@domain USER PASSWORD** – connect to LDAP during installation
- **-noldap** – do not connect to LDAP during installation
- **-sso MANAGED-PATH** – configure SSO access through Managed Path
- **-nosso** – disable SSO access
- **-folder** – automatically confirm current folder
- **-admin LOGIN FIRST\_NAME LAST\_NAME PASSWORD | GENERATE** – initial system administrator
- **-location INSTALLATION\_FOLDER** – installation folder
- **-output FILE** – file output for generated keys and passwords
- **-help** – prints this message

Below is the **example** of command line arguments to automatically install the system with default options selected into the folder `$PAM_HOME` (for example, `/opt/pam`), create system administrator user with generated password and save the generated passwords and keys into the file `pam.info`:

```
1 | ./XtamSetup.sh -eula -db -dir -gui -worker -session -noldap -admin pamadmin  
System Administrator GENERATE -nocas -nosso -folder -location /opt/pam -output  
pam.info
```

## Silent Installer for Windows Platforms

The Windows PowerShell installation script includes command line options to define installation choices. The script also allows silent deployment options combination.

The [silent installer](#) option is useful for deployment automation and repeatability in large environments, elastic provisioning of new systems in cloud or closed data-center environments and cleaner separation of system ownership, administration and deployment roles by limiting exposure of sensitive system keys and passwords.

The PowerShell installer for Windows platforms includes the following parameters:

- **-eula** – Accept EULA
- **-db** – install embedded database
- **-nodb** – connect to external database
- **-dbType** **Oracle| MSSQL| MySQL| PostgreSQL**
- **-dbServer** **SERVER**
- **-dbUser** **USER**
- **-dbPassword** **PASSWORD**
- **-dir** – install Directory Services
- **-nodir** – connect to external Directory Services
- **-dirServer** **SERVER**
- **-dirPassword** **PASSWORD**
- **-gui** – install the application GUI
- **-nogui** – install the application without GUI component
- **-worker** – install the application Worker process
- **-noworker** – install the application without Worker process
- **-session** – install session manager
- **-nosession** – install the application without session manager
- **-cas** – install Federated Sign-In Module
- **-casversion** **CAS52 | CAS65** - version of Federated Sign-In Module
- **-nocas** – install the application without Federated Sign-In Module
- **-ldap** – connect to LDAP during installation
- **-ldapServer** **SERVER**
- **-ldapUser** **USER**
- **-ldapPassword** **PASSWORD**
- **-noldap** – do not connect to LDAP during installation
- **-sso** – configure SSO access through Managed Path
- **-managedPath** **MANAGED-PATH**
- **-nosso** – disable SSO access
- **-mp** **MASTER-PASSWORD** – install with provided master password instead of generated one
- **-folder** – automatically confirm current folder
- **-admin** **LOGIN** – initial system administrator
- **-adminFirst** **FIRST\_NAME** – first name of the initial system administrator
- **-adminLast** **LAST\_NAME** – last name of the initial system administrator
- **-adminPassword** **PASSWORD|GENERATE** – password of the initial system administrator
- **-location** **INSTALLATION\_FOLDER** – installation folder
- **-output** **FILE** – file output for generated keys and passwords
- **-help** – prints this message
- **-certBundle** - path to the certificate bundle for remote session manager deployments

To install the software to the current folder from **PowerShell** prompt run the script as:

```
1 | & .\XtamSetup.ps1
```

To install the software to the specified existing location folder from **Windows** command line prompt run the script as:

```
1 | PowerShell -File XtamSetup.ps1 -location c:\pam
```

Below is the **example** of command line arguments to *automatically* install the system with default options selected into the folder `$PAM_HOME` (for example, `c:\pam`), create system administrator user with generated password and save the generated passwords and keys into the file `pam.info`:

```
1 | & .\XtamSetup.ps1 -location c:\pam -eula -db -dir -gui -worker -session -nocas -  
  | nosso -noldap -folder -admin pamadmin -adminFirst System -adminLast Admin -  
  | adminPasswd INITIAL-PASSWORD -output pam.info
```

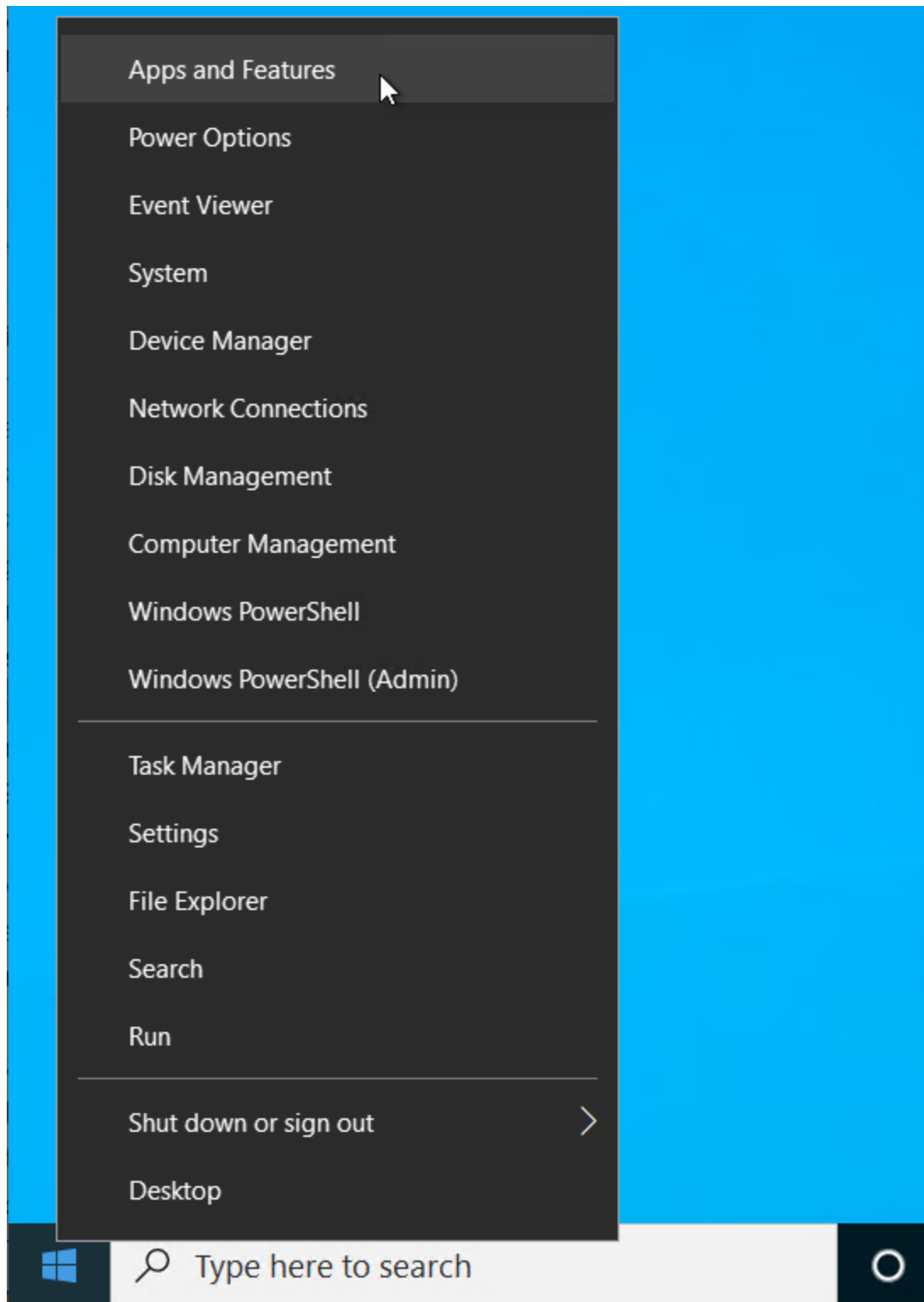
## Deploying OpenSSH Service on Windows 10+ Hosts

### Pre-requisites

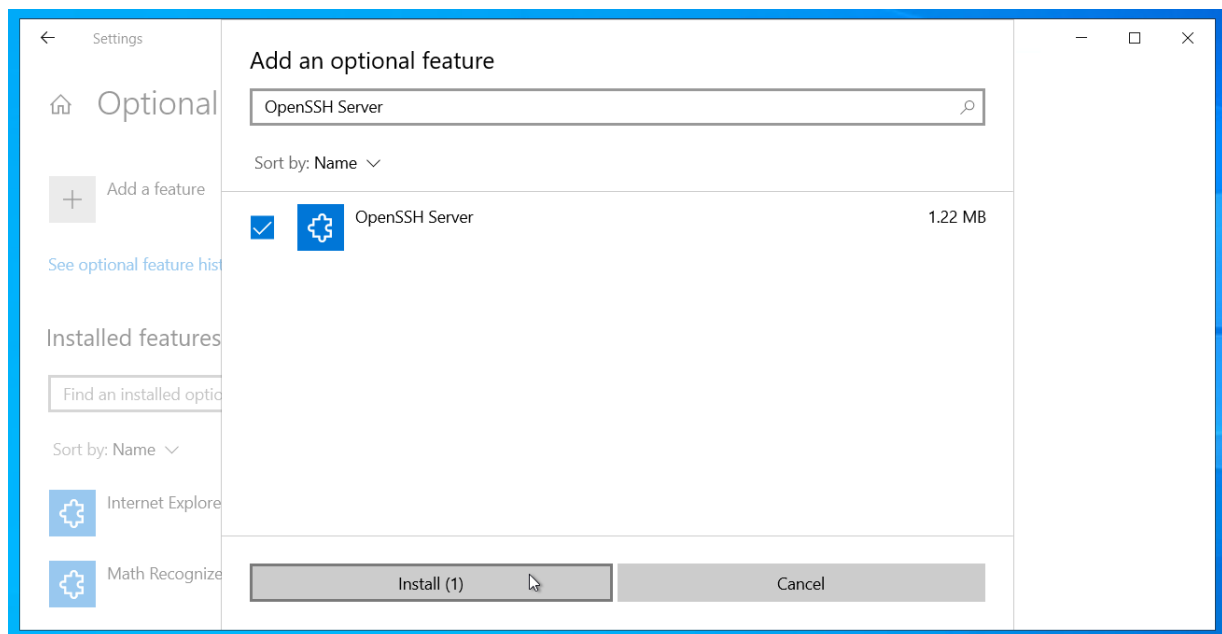
- The host is running Windows 10 (version 1809 or greater) or Windows 11.
- The user is signed in as an account that is a member of the built-in Administrator group.

## Deploying OpenSSH Service

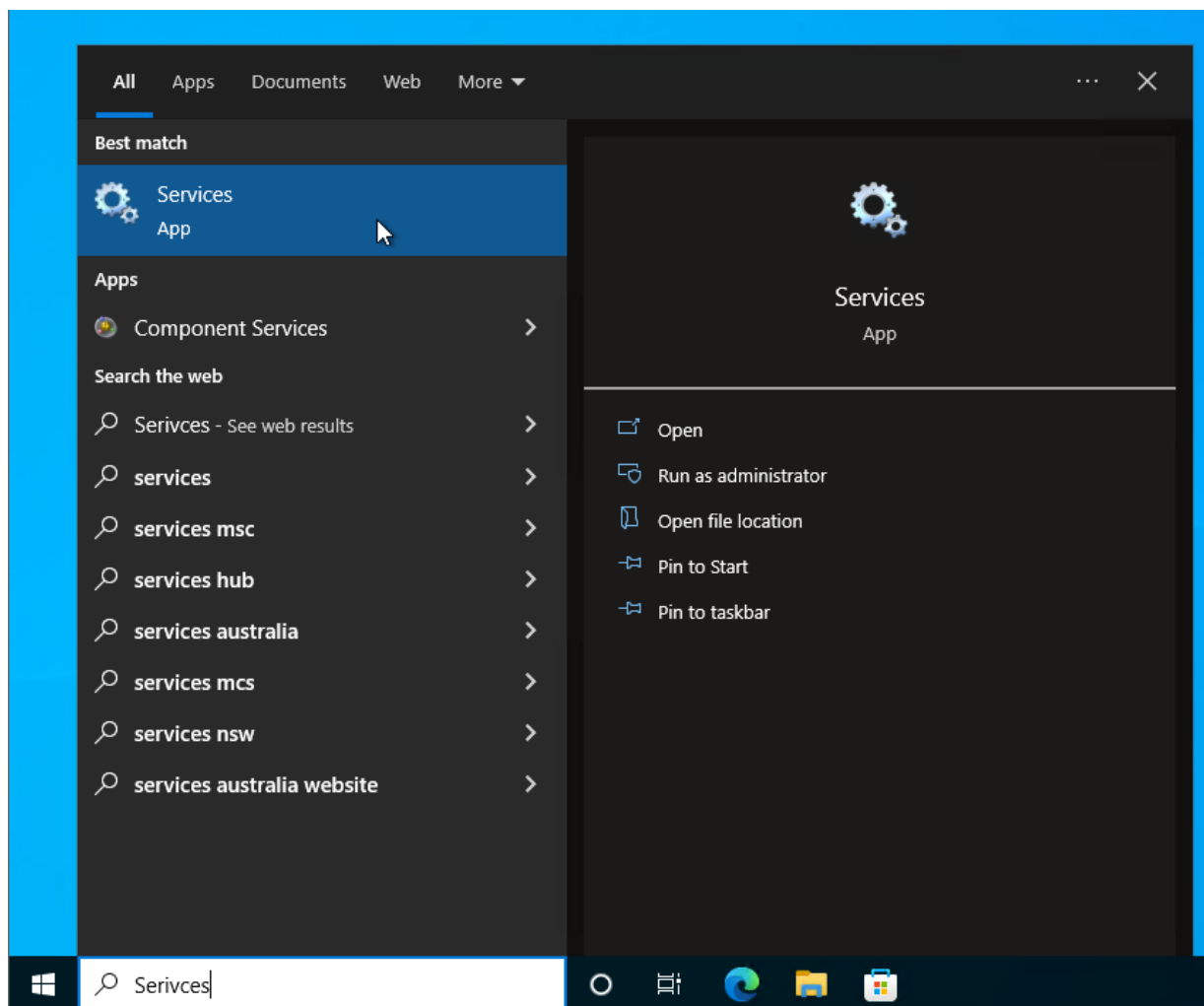
1. On Windows 10+ host, right-click Windows left button, go to **Apps and Features**.



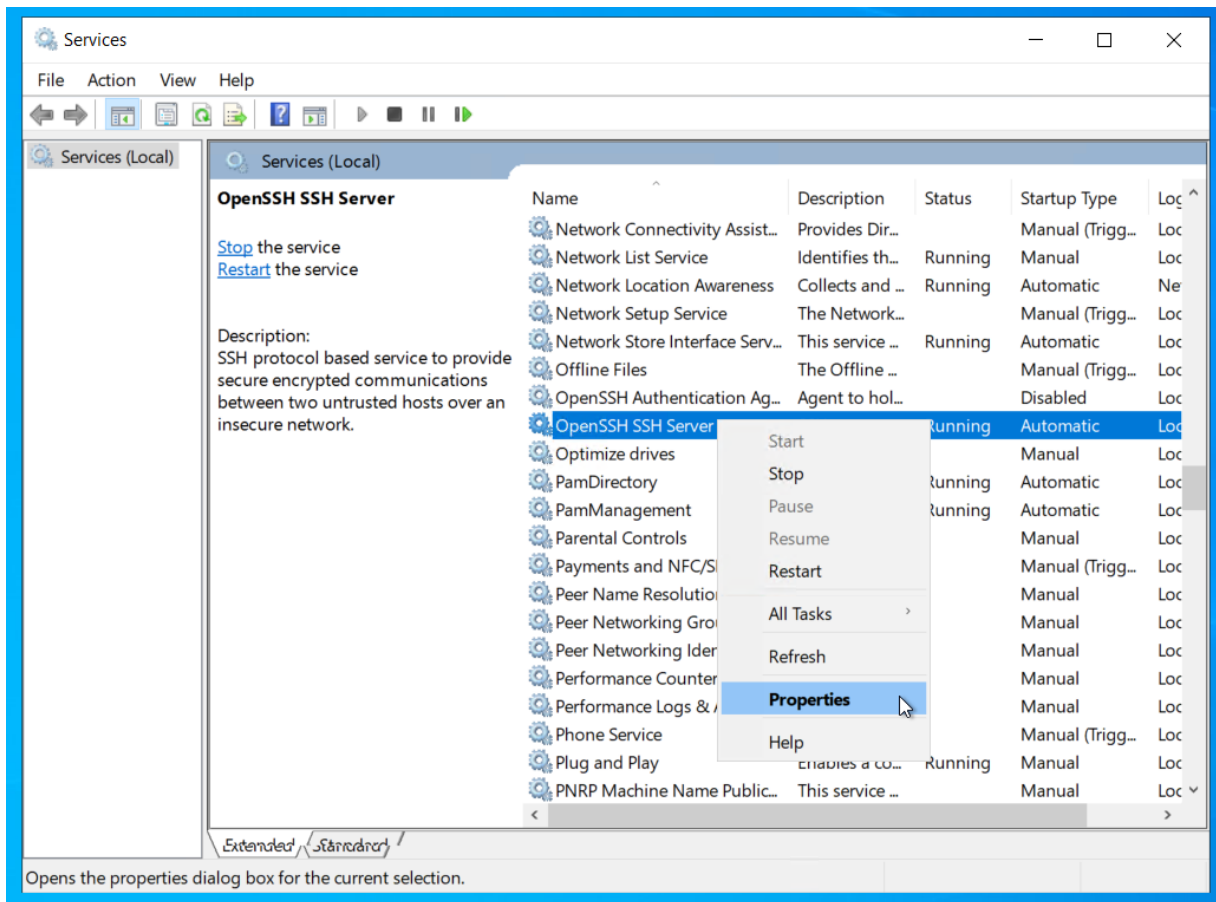
2. Under Add a feature select **OpenSSH Server**.



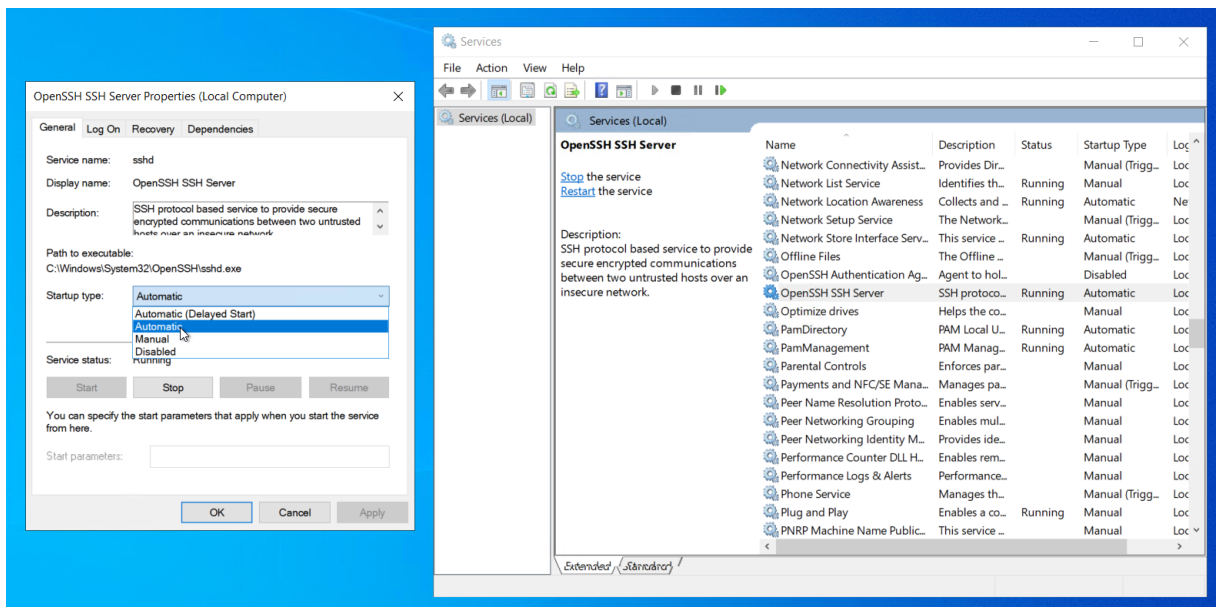
3. Using Windows search tool search and select **Services**.



4. Search and right-click **OpenSSH SSH Server**, and click **Properties**.

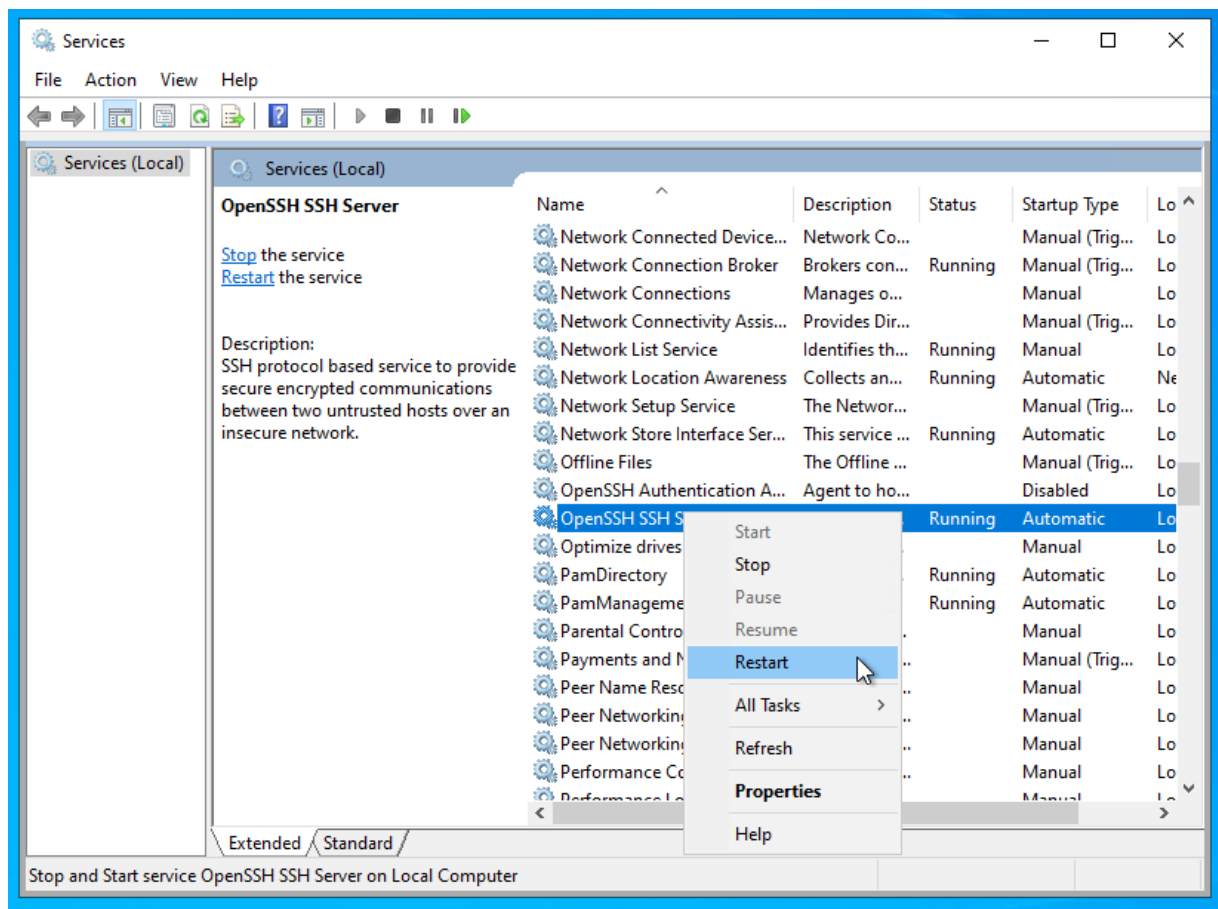


- Under **Startup type**, select **Automatic** and press **OK**.



- Restart the *OpenSSH SSH Server* service by right-clicking the service and press **Restart**.





## Update Local Directory to TLS 1.2

Use the following procedure to update the PAM Local Directory to restrict the accepted cryptographic protocol to TLS v1.2.

Please note that all new PAM deployments beginning on August 9, 2020 will have TLS 1.2 only enabled by default. For existing PAM deployments prior to August 9, 2020, this procedure can be used if required.

1. Login to PAM host server and first stop the **PamManagement** (Windows) or **pammanager** (Linux) service. Then stop the **PamDirectory** (Windows) or **pamdirectory** (Linux) service.
2. Open the file `$PAM_HOME/ds/instances/default/conf/ou=config/ads-directoryserviceid=default/ou=servers/ads-serverid=ldapservice/ou=transports/ads-transportid=ldaps.idif` in a text editor.
3. Add the following line to the end of the file:

```
1 | ads-enabledProtocols: TLSv1.2
```

4. **Save and close** this file.
5. Start the **PamDirectory** (Windows) or **pamdirectory** (Linux) service.
6. Start the **PamManagement** (Windows) or **pammanager** (Linux) service.

# Session Connection Failed Error 519

Session Error: 519 - The remote server does not appear to exist, cannot be reached over the network or the account is locked. In most cases, this server is the remote desktop server. PAM | Production Web Server - pam\itadmin@10.0.0.23:10023

Show Keyboard

English (US) ▼

Clipboard

File Browser

Show Participants

Full Screen

–

100%

+

Press Esc to close toolbar

If you are attempting to Connect to a remote host, but you are receiving the 519 error code, then this typically means that PAM was unable to connect with the remote host using the parameters from the record.

**To troubleshoot this issue, please evaluate and try the following suggestions.**

1. Ensure that both the **username** and **password** entered into the record are accurate. Incorrect passwords and typos will generate this error.
2. Assuming it is a Windows host using a local account, try removing the domain from the username. Rather than using **contoso\localuser** try entering just **localuser** or vice versa.
3. Try pinging the remote host from the PAM host to ensure it is found and responding.
4. If you entered the Host as a computer name, try replacing it with the host's IP address instead.
5. On the remote host, ensure that the **RDP port** (3389) is open and that you can connect to it.
6. Make sure the username in this record has permissions on the host to connect remotely.
7. Make sure the username in this record is not locked or disabled.
8. Update to the latest available version of PAM.

If you are experiencing this error or any connectivity error when attempting a connection with *all* your records, then ensure the **PamSession** or **pamsession** service is running on your PAM host server. If it is running, try restarting it to resolve the issue.

If you are still having issues after trying the above, please gather your PAM logs and send them the Support team: <https://support.imprivata.com/communitylogin>.

[More session connection error codes here.](#)

## Login Connection Failed Error 404

Page Not Found (404) error when attempting to login to PAM.

### Troubleshooting

- Ensure that [Load Balancer](#) persistence settings are correct.
- Update to the latest PAM version. There have been cache-control changes made to login pages to ensure that content is not cached.
- Have the user clear browser history, cache and cookies for the last 24 hours.

## Switch PAM from IP to Name URL Access

Update PAM from IP-based to Named URL Access.

If your current version of PAM is accessible from an IP-based URL and you want to switch this to a Named-based URL, then the following guide walks you through the required steps.

In this guide we will use the IP of **10.1.2.3** as our example, the Name as **pam.company.com** and port 443. You should use your specific values in place of our example.

Therefore we will be switching from `https://10.1.2.3/xtam` to `https://pam.company.com/xtam`

1. Create a DNS record A for `pam.company.com` with the value **10.1.2.3**.
2. Obtain a SSL certificate (in `.pfx` or `.jks` format) for the host name **pam.company.com**, one that all browsers in your company will trust. Replace your old SSL certificate, which will no longer be trusted because it lacks the host `pam.company.com` in its subject, with your new SSL certificate. Use the steps in [this article to replace your SSL certificate in PAM](#).
3. Change PAM's configuration to accept the host `pam.company.com` instead of the IP address. This is done by opening the file `$PAM_HOME/web/conf/catalina.properties` and changing the following properties. If they do not currently exist, search the file, then add them manually as shown below. **Save and close** the file when complete.

```
1 cas.managed.path=https://pam.company.com
2 cas.server.name=https://pam.company.com
3 cas.server.prefix=https://pam.company.com/cas
4 cas.view.defaultRedirectUrl=https://pam.company.com/xtam/
```

The above configuration assumes you are accessing PAM using port 443. If you are using a different port like 6443 or another, then be sure to add the port number to all the paths like this example `https://pam.company.com:6443`

4. (Optional) If you are currently accessing PAM using port 6443 and wish to switch to another port, like 443, then complete this step. If you do not wish to change the port or have already done so previously, you skip this step. Open the file `$PAM_HOME/web/conf/server.xml` in a text editor. Search this document for your current port number (i.e. 6443) and replace it with your new port number (i.e. 443). There will be two places in this `.xml` file that will need to be updated.
5. Import your new SSL certificate into the PAM keystore. There are several ways to do this, please choose the one that works best for you.
  - a. If you are already on the latest version of PAM (or more recent than May 1, 2020), then perform the procedure above and restart the **PamManagement** (Windows) or **pammanager** (Linux) service. After the restart, wait about 5 minutes and then restart the same service one more time. PAM will import the new certificate during the first restart and will use it after the second restart.
  - b. If you are on a version of PAM between January 1, 2020 and May 1, 2020, then perform the procedure above and restart the **PamManagement** (Windows) or **pammanager** (Linux) service. After the restart, wait about 5 minutes and then execute the following command from `$PAM_HOME` (you will need Administrator or sudo permissions)  
for Windows:

```
1 | bin\PamDirectory.cmd SSLImport pam.company.com 443
```

for Linux:

```
1 | bin/PamDirectory.sh SSLImport pam.company.com 443
```

If the command returns any trust errors, follow the prompts to import all certificates into the PAM store, one by one. Afterward, run the same command again to confirm that no trust errors remain.

- c. For all versions of PAM, you can use the *PamKeyTool.cmd* command to import your SSL certificate. This procedure is described in [this article](#).

6. Finally, your PAM instance will now be accessible from your new named URL. Open your login page (<https://pam.company.com/pam>) and confirm it is working as expected.

## Session Manager Not Connecting

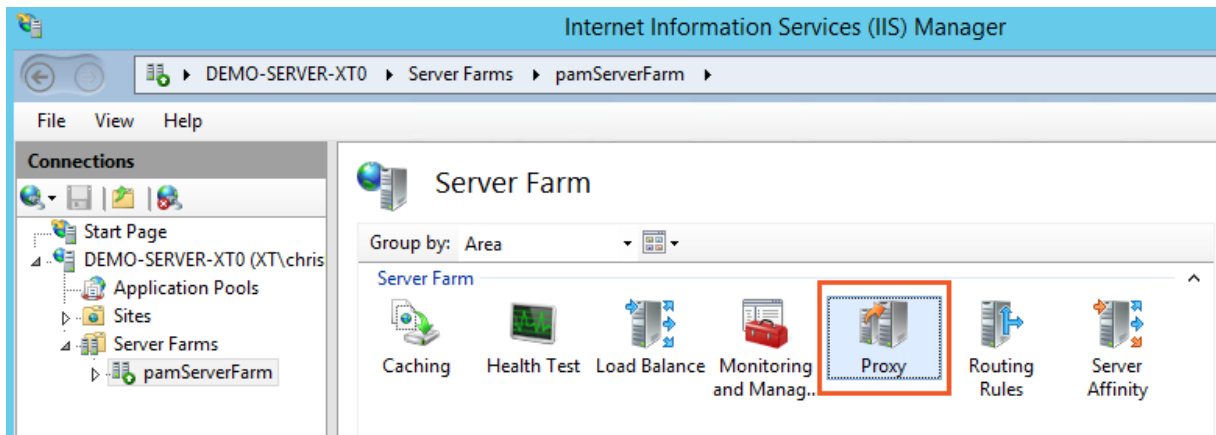
I can't connect to a session and the process is stuck on Connecting to Session Manager.

What should I do?

If a user attempts to establish a session and the browser displays the message "Connecting to Session Manager", but it does not connect to the host, then please try the following suggestions.

## IIS Buffer configuration

1. Login to the computer where Privileged Access Management is running.
2. Open its Internet Information Services (IIS) Manager.
3. Navigate down the menu to Server Name > Server Farms and select **pamServerFarm**.
4. On the *pamServerFarm* "Server Farm" page, open the **Proxy** section.



5. Locate the Buffer Setting section and make the following changes:
- Response buffer (KB): 1
  - Response buffer threshold (KB): 0

Buffer Setting

Response buffer (KB):

Response buffer threshold (KB):

6. Restart IIS and try to establish the session again.

If you have any codes in your connection status, [check for their meaning](#).

## Session Connection Errors Codes

If you are attempting to Connect to a remote host and receiving a connection error code, then this typically means that PAM was unable to connect with the remote host by one of the reasons. We use a common set of numeric status codes. These codes denote success or failure of operations, and can be rendered by user interfaces in a human-readable way.

### 0 (SUCCESS)

The operation succeeded. No error.

### 256 (UNSUPPORTED)

The requested operation is unsupported.

### 512 (SERVER\_ERROR)

An internal error occurred, and the operation could not be performed.

### 513 (SERVER\_BUSY)

The operation could not be performed because the server is busy.

### 514 (UPSTREAM\_TIMEOUT)

The upstream server is not responding. In most cases, the upstream server is the remote desktop server.

### 515 (UPSTREAM\_ERROR)

The upstream server encountered an error. In most cases, the upstream server is the remote desktop server.

### 516 (RESOURCE\_NOT\_FOUND)

An associated resource, such as a file or stream, could not be found, and thus the operation failed.

### 517 (RESOURCE\_CONFLICT)

A resource is already in use or locked, preventing the requested operation.

## 518 (RESOURCE\_CLOSED)

The requested operation cannot continue because the associated resource has been closed.

## 519 (UPSTREAM\_NOT\_FOUND)

The upstream server does not appear to exist, or cannot be reached over the network. In most cases, the upstream server is the remote desktop server. [Troubleshooting](#).

## 520 (UPSTREAM\_UNAVAILABLE)

The upstream server is refusing to service connections. In most cases, the upstream server is the remote desktop server.

## 521 (SESSION\_CONFLICT)

The session within the upstream server has ended because it conflicts with another session. In most cases, the upstream server is the remote desktop server.

## 522 (SESSION\_TIMEOUT)

The session within the upstream server has ended because it appeared to be inactive. In most cases, the upstream server is the remote desktop server.

## 523 (SESSION\_CLOSED)

The session within the upstream server has been forcibly closed. In most cases, the upstream server is the remote desktop server.

## 768 (CLIENT\_BAD\_REQUEST)

The parameters of the request are illegal or otherwise invalid.

## 769 (CLIENT\_UNAUTHORIZED)

Permission was denied, because the user is not logged in. Note that the user may be logged into PAM, but still not logged in with respect to the remote desktop server.

## 771 (CLIENT\_FORBIDDEN)

Permission was denied, and logging in will not solve the problem.

## 776 (CLIENT\_TIMEOUT)

The client (usually the user of PAM or their browser) is taking too long to respond.

## 781 (CLIENT\_OVERRUN)

The client has sent more data than the protocol allows.

## 783 (CLIENT\_BAD\_TYPE)

The client has sent data of an unexpected or illegal type.

## 797 (CLIENT\_TOO\_MANY)

The client is already using too many resources. Existing resources must be freed before further requests are allowed.

## Hardening Protocols and Ciphers

To restrict protocols and ciphers that the PAM Server uses for SSL to TLS 1.2+ please perform the following procedure.

By default, new and recent deployments of PAM only use TLS 1.2, but this article can still apply if the protocol needs to be modified for specific purposes.

1. Login to PAM host server with an account that has permissions to modify files and restart services. Both will be required for the successful completion of this activity.
2. Make a backup copy of the file `$PAM/web/conf/server.xml`. We will be making a few updates to this file and if anything goes wrong, you can restore this copy from backup.
3. Open the file `$PAM/web/conf/server.xml` in a text editor.
4. In the file, locate the Connector definition for the port that PAM listens. In our example, this is port 6443 but it may be different in your instance. In this definition the following changes will be made:
  - Change the current `sslProtocol="TLS"` to `sslProtocol="TLSv1.2"`
  - Add the attribute `sslEnabledProtocols` for enabled protocols one line after `sslProtocols`:

```
sslEnabledProtocols="TLSv1.2+TLSv1.3"
```

- Add the attribute for enabled *ciphers* one line after `sslEnabledProtocols`:

```
ciphers="TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256"
```

Here is how the default Connection definition looks when using **port 6443** (your port may be different):

```
1 <Connector
2     keystoreFile="${xtam.cert.path}"
3     keystorePass="${xtam.cert.password}"
4     protocol="com.pam.config.Http11NioEncryptedProtocol"
5     port="6443" maxThreads="200" proxyPort="443"
6     scheme="https" secure="true" SSLEnabled="true"
7     sslProtocol="TLS"
8     clientAuth="false" keystoreType="JKS"/>
```

And here is how the updated Connection definition will look when using port 6443 (your port may be different):

```
1 <Connector
2     keystoreFile="${xtam.cert.path}"
```

```

3      keystorePass="${xtam.cert.password}"
4      protocol="com.pam.config.Http11NioEncryptedProtocol"
5      port="6443" maxThreads="200" proxyPort="443"
6      scheme="https" secure="true" SSLEnabled="true"
7      sslProtocol="TLSv1.2"
8      sslEnabledProtocols="TLSv1.2+TLSv1.3"
9      ciphers="TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_
AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_DHE_RSA_
WITH_CHACHA20_POLY1305_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_
RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_
WITH_AES_128_GCM_SHA256"
10     honorCipherOrder="true"
11     clientAuth="false" keystoreType="JKS"/>

```

5. After you have made and confirmed your changes, **save and close** this file.
6. Finally, restart the **PamManagement** (Windows) or **pammanager** (Linux) service to complete the procedure.

This change will make the PAM SSL termination only operate on these enabled protocols. If PAM is accessed through a load balancer, similar changes should be made on the load balancer according to its documentation.

## Configuring the SSH Proxy Security Algorithms

To select specific Key Exchange, Message Authentication Code (MACs) and Cipher algorithms used by the SSH Proxy client connection and to remove weak algorithms the SSH Proxy is using to negotiate connections use the global parameters mentioned below.

Located in Administration > Settings > Parameters:

- SSH Proxy Ciphers
- SSH Proxy Key Exchange Algorithms
- SSH Proxy Macs

Please review the **Context Help** button for each option in the PAM interface for descriptions.

## Session Relay Node Architecture and Deployment

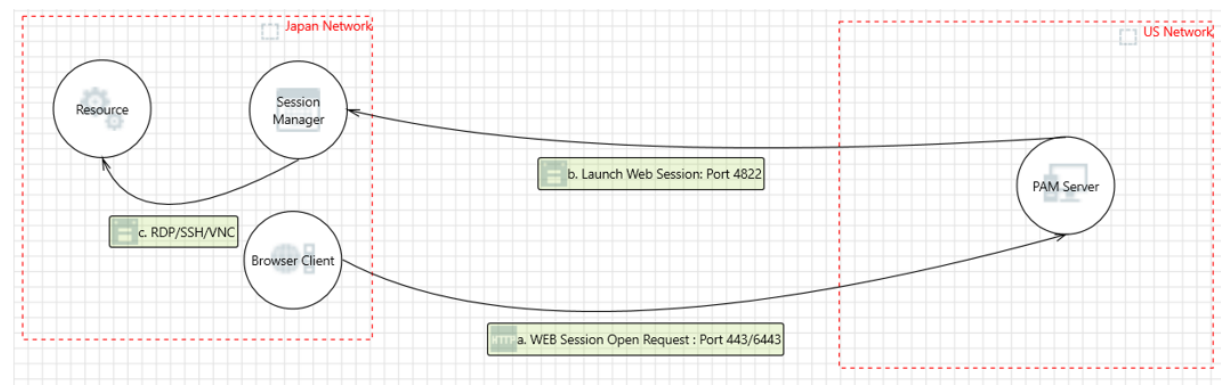
A Session Relay Node is designed to reduce potential heavy network traffic that may be apparent in deployments where remote sessions, between a user and a remote host, span geographies. In multi-region deployments and under certain circumstances, a user's remote session in such deployments could exhibit a performance decrease that results in latency during their session.

This could be caused by how PAM communicates between its components via network connectivity. In a multi-node PAM deployment where remote sessions are being utilized, the network traffic routes from the user's device through the PAM Master Node to the Session Manager (which may also be remotely located) and finally, to the destination host.



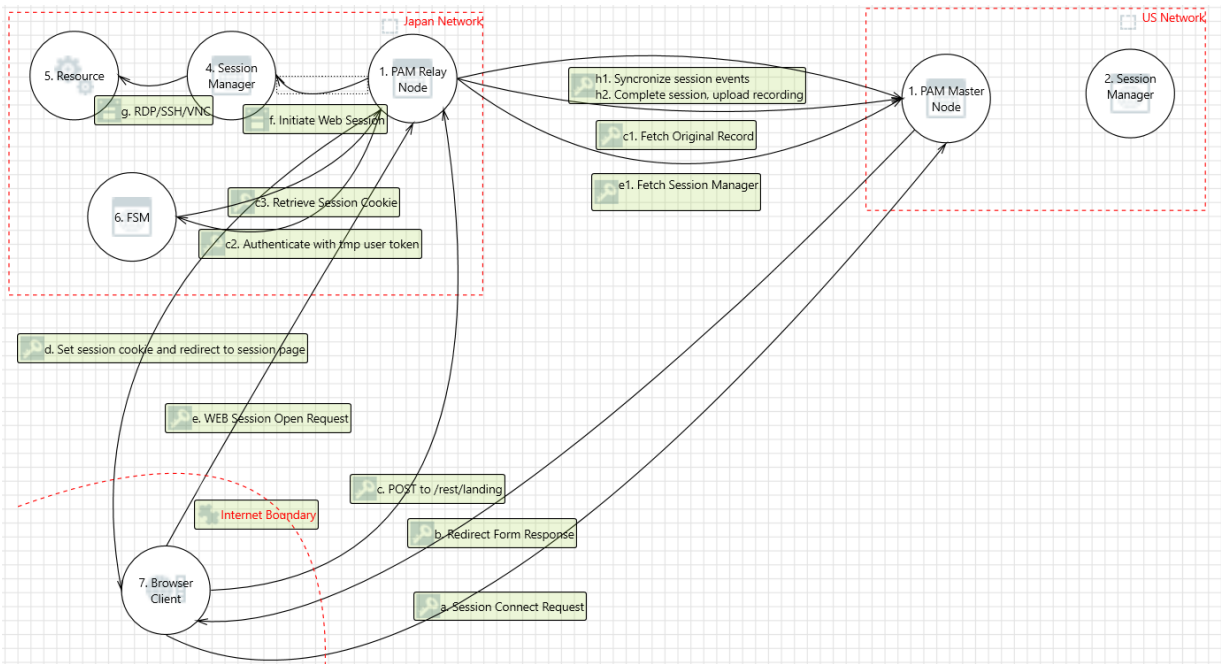
In most deployments, this traffic routing works well for a consistently quality remote session experience; however, when the user's location is similarly located to the destination endpoint, whereas the Master Node is significantly remotely distant to both, routing to this remote Master Node can degrade this session experience.

It is this second scenario that the Session Relay Node looks to optimize by reducing the amount of heavy traffic that needs to occur between the user, destination endpoint and master node(s).



With an optimally deployed Session Relay Node, the heavier network communication like web session traffic is routed locally between the user's device and the Session Relay Node, while only low volume traffic like authentication and permission information) is required to route through the Master Node.

This redirects high traffic communication and can improve a user's session experience by keeping it more local to their and the destination endpoints geography.



To further illustrate this deployment, let us take the example of a PAM deployment residing physically in the US East region and some users and destination endpoints located in Japan.

For a user sitting in Japan and accessing endpoints also located in Japan, heavy traffic routed through US East located Master Node may experience performance degradation.

With a Session Relay Node deployed in the same Japan location, this heavy session traffic now remains in Japan thus reducing the amount of “around the globe” communication necessary to establish and maintain this remote session.

If your PAM deployment, destination endpoints or user base spans across multiple geographies and the session experience involving these regions exhibits latency, then adding an appropriately located Session Relay Node to your deployment may help.

The remainder of this article will describe the Session Relay Node Considerations and Deployment procedures.

## Considerations

When deliberating if a Session Relay Node may improve a session experience in your deployment, please consider the following:

- Is your PAM deployment, including users, components, and destination endpoints, located in vastly remote geographies and remote session experience is noticeably and consistently “laggy” for users?
- Have you already deployed a remote Session Manager component geographically closer to the destination endpoint?
- Have you reviewed your network topography considering any blockers like VPNs, network scanners or analyzers, that may be introducing traffic degradation? If present, can these be removed, optimized or excluded from PAM traffic and communication?
- Are the resources on the PAM server(s) running low? High CPU utilization, high memory usage or low disk space could be contributors to observed PAM performance reports. Increasing server resources and deploying additional PAM nodes like Session Managers or Master Nodes could alleviate high resource consumption.
- Will your existing license key support the additional node requirement? A Session Relay Node consumes one additional node from your registered license key regardless of whether it is deployed to an existing node or as a new node.
- The Federated Sign-in Module (FSM) is a required PAM component on all Master and Session Relay Nodes. Instructions to install or update the federated sign in module can be found <https://help.xtontech.com/content/installation/federated-sign-in-module/federated-sign-in.htm>

## Configuration

Relay Node can be installed to a new PAM node, or an existing Remote Node can be configured to also support the Relay Node function.

Either deployment will consume one Node from the registered license key.

### *New Relay Node Deployment*

This section will include the procedure required to install a PAM Session Relay Node to a new server.

This server's location should be carefully chosen to maximize the benefits of the Relay Node.

The server can be either virtual or physical and should have at least 2 CPUs, 8 GB of memory available and 100 GB of disk space for the PAM services to consume. Valid SSL certificates will also be required to secure traffic between the various components.

## PAM Web Configuration

1. Login to PAM web console with a System Administrator account.
2. Create a new local user that will be used exclusively for the authenticating between the Master and Relay Nodes. If you are deploying multiple Relay Nodes, you may use the same local user for each relay node or choose to create a unique local user for each relay node, either is supported.
3. Grant this local user account the Global Role Service
4. Create an API token for this Relay Node local user account.
5. On the Administration > Settings > Parameters page, locate the parameter *Support Relayed Sessions*, set it to **Enabled** and click the **Save** button.

## Relay Node Configuration

1. On the server, run the PAM installer and select the following options:
  - Internal Database.
  - Directory Service.
  - Application GUI.
  - Job Engine (only select this option if the node will also support remote Job Engine executions).
  - Session Manager.
  - Federated Sign-In.
2. Active Directory integration is not required nor recommended. Leave empty and continue.
3. When the installation is complete, save the deployment's configuration and passwords to a safe and secure location.
4. Open a browser and login to the PAM web console using the default System Administrator account created during installation. Click the **Initialize** button to initialize the database and wait until this operation completes. After it finishes, you may log out of PAM and close your browser.
5. Generate a self-signed or obtain valid SSL certificates whose CN field matches the master and relay nodes host names.
6. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor and locate the parameter named **cas.tgc.crypto.signing.key**. Copy this *signing.key* value from your Master Node and paste it to this parameter on the relay node.
7. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor and add the following new parameters whose values match your Master Node deployment. If you have multiple Master Nodes, you will need to add parameters for each master node using an indexed configuration [0], [1], [2], etc.

Example placeholders in these parameters, noted by the value surrounded by {}, should be replaced with the values specific to your deployment.

```
1 | xtam.remote.enabled=false
2 | xtam.remote.url={https://pam:6443/xtam}
3 | xtam.remote.user=relay
```

```
4 | xtam.remote.id={masterNodeServerName}
5 | xtam.remote.token={RelayNodeAccountToken}
```

*In the case of multiple Master Nodes, indexed configuration may look like this:*

```
1 | xtam.remote.enabled[1]=false
2 | xtam.remote.url[1]={https://pam:6443/xtam}
3 | xtam.remote.user[1]=relay
4 | xtam.remote.id[1]={masterNodeServerName}
5 | xtam.remote.token[1]={RelayNodeAccountToken}
```

8. In the same file, add these new parameters based on your deployment requirements:

```
1 | xtam.relay.node=enabled
```

a.

```
1 | xtam.relay.name={RelayNodeName}
```

b.

- i. Choose a short and descriptive name of this Relay Node that will be used to identify it in the *Application Node list* and the *Connect menu* that the user will select.

We recommend choosing a name that represents the Relay Node's location like *US East Relay* or *Japan Relay*.

9. If the Relay Node is also being used for Job Engine execution, then also add this new line:

```
1 | xtam.remote.enabled=true
```

10. In order for relay node to broker sessions with session managers based on proximity group configuration, add/update the below property:

```
1 | xtam.relay.session.manager.lookup=enabled/disabled (default=enabled)
```

11. Next, SSL certificates will be imported to secure the component communications.

- a. Import the SSL certificate from the Master Node(s) using the SSLImport command.

Example shown below:

- i. Windows: from \$PAM\_HOME, execute `bin\PamDirectory.cmd SSLImport pam.company.com 443`
- ii. Linux: from \$PAM\_HOME, execute `bin/PamDirectory.sh SSLImport pam.company.com 443`

- b. Import the SSL certificate from the Relay Node itself.

Example shown below:

- i. Windows: from \$PAM\_HOME, execute `bin\PamDirectory.cmd SSLImport pam.company.com 443`
- ii. Linux: from \$PAM\_HOME, execute `bin/PamDirectory.sh SSLImport pam.company.com 443`
- c. Import the SSL certificate from each Session Manager configured with the Master Nodes.

Example shown below:

- i. Windows: from \$PAM\_HOME, execute `bin\PamDirectory.cmd SSLImport pam.company.com 443`
- ii. Linux: from \$PAM\_HOME, execute `bin/PamDirectory.sh SSLImport pam.company.com 443`

You may **disable** Session Manager resolution from the Master Node by adding `xtam.relay.session.manager.lookup=disabled` to the `catalina.properties` configuration file on the Master Nodes.

12. **Restart** the PamManagement (Windows) or pammanager (Linux) service on the Relay Node to complete the configuration.

## Testing

After the deployment is complete, it is now time to test the functionality of the Session Relay Node.

This testing will be performed by a System Administrator.

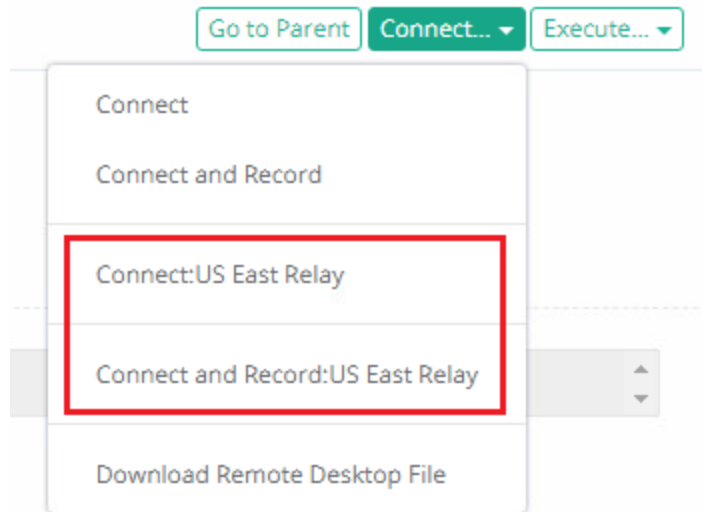
First, let us confirm that the Relay Node is online and communicating with your PAM Master Node(s).

1. Navigate to Administration > Settings > Application Nodes and locate the presence of your Relay Node. It will be shown with the name that was added to the configuration in our previous sections followed by the label *Relay*. For example, **US East Relay:Relay**
2. If the node is online, it will be shown in green font accompanied with an up arrow; conversely if the node is offline, **it will be shown in red font** accompanied with a down arrow. The node must be online before testing continues.

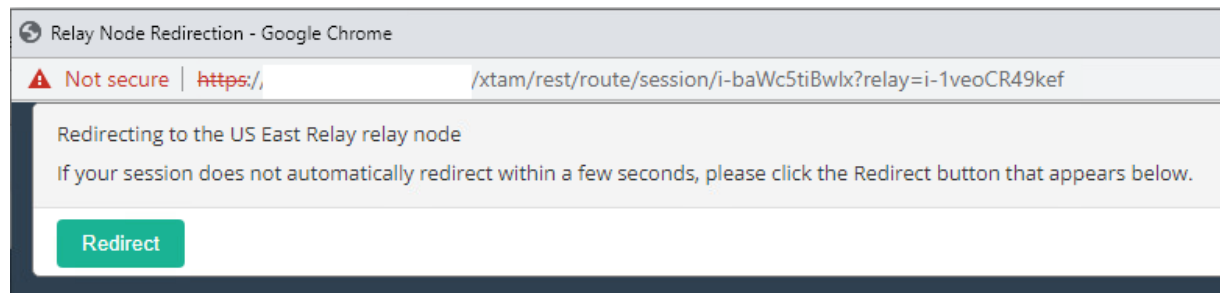
Application Nodes										
Proximity Groups Database Registration Parameters Mail Server AD Syslog										
Found 6 nodes.										<a href="#">Refresh</a> <a href="#">Restart</a>
Node	Message Queue	Discovery	Notification	Job Queue	Render Queue	Scheduling	Aggregation	Session	Actions	
<b>pamwin1-01:GUI</b> 2.3.202212111009 / 12/15/2022 12:15 <span style="color: green;">↑</span>	Idle: 0.5						Idle: 30	Idle: 5	<a href="#">Edit</a>	
<b>pamwin1-01:Worker</b> 2.3.202212111009 / 12/15/2022 12:14 <span style="color: green;">↑</span>	Idle: 0.5	Pool: 5 Idle: 2	Pool: 5 Idle: 5	Pool: 5 Idle: 0.5	Pool: 5 Idle: 0.5	Idle: 5			<a href="#">Edit</a>	
<b>pamwin2-01:GUI</b> 2.3.202212111009 / 12/15/2022 12:14 <span style="color: green;">↑</span>	Idle: 0.5						Idle: 30	Idle: 5	<a href="#">Edit</a>	
<b>pamwin2-01:Worker</b> 2.3.202212111009 / 12/15/2022 12:14 <span style="color: green;">↑</span>	Idle: 0.5	Pool: 5 Idle: 2	Pool: 5 Idle: 5	Pool: 5 Idle: 0.5	Pool: 5 Idle: 0.5	Idle: 5			<a href="#">Edit</a>	
<b>pamwinjob-01:Worker</b> 2.3.202210021124 / 12/15/2022 12:15 <span style="color: green;">↑</span>	Idle: 0.5	Pool: 5 Idle: 2	Pool: 5 Idle: 5	Pool: 5 Idle: 0.5	Pool: 5 Idle: 0.5	Idle: 5			<a href="#">Edit</a>	
<b>US East Relay:Relay</b> / 12/15/2022 12:14 <span style="color: green;">↑</span>	Idle: 0								<a href="#">Edit</a>	

Next, it is time to check session connectivity.

1. Navigate to an existing record or create a test record.
2. From the *Record View* page, open the *Connect* dropdown menu and select the **Connect** option that is shown with the Relay Node name appended to the end.



3. After the Relay Node Connect option is selected, a new Relay Node Redirection browser window or tab will open. An automatic redirect attempt to the Relay Node page will begin and if successful, the user's remote session will then connect to the destination endpoint from the indicated *Relay Node*. If the automatic redirect attempt fails after five seconds, a **Redirect** button will appear that the user must click to continue.



4. Test the remote session functionality to confirm the session connected to the destination endpoint successfully and then complete the session.

Finally, we will confirm that this remote test session was routed through the Relay Node.

1. From the record's Session report or the Report Center's Session report, locate the previous test session that is now complete.
2. In the *Session Manager* column of this session, the Relay Node server's name will be displayed,

confirming that the Relay Node connected this session.

Found 26 sessions.

Time: Last Month State: Any Columns

Show 50 entries Search:

CSV PDF XLSX PDF Protected CSV Protected XLSX Protected

Showing 1 to 26 of 26 entries

Record	User	Start Time	Completion Time	Type	Status	Session Manager	Recording
Prod-East	John Williams (jwilliams) /AD	12/14/2022 10:57:01	12/14/2022 10:57:51	RDP	Completed	s://useast-relay-4822	Recorded

## SSH Proxy with Relay Node

### Requirements

Ensure Relay node setup is complete following instructions from the above [article](#).

### Relay Node Configuration

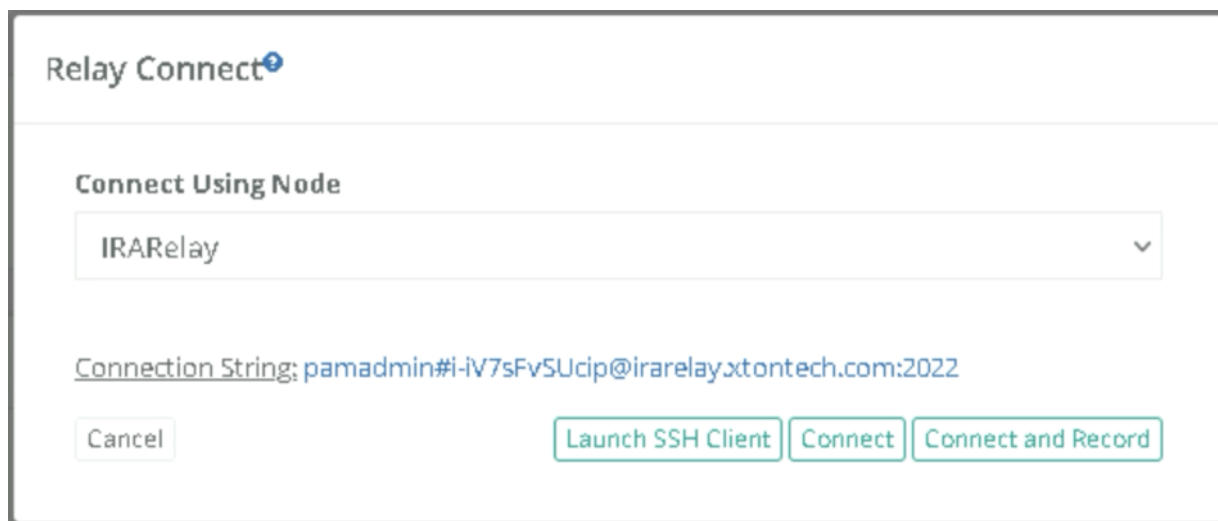
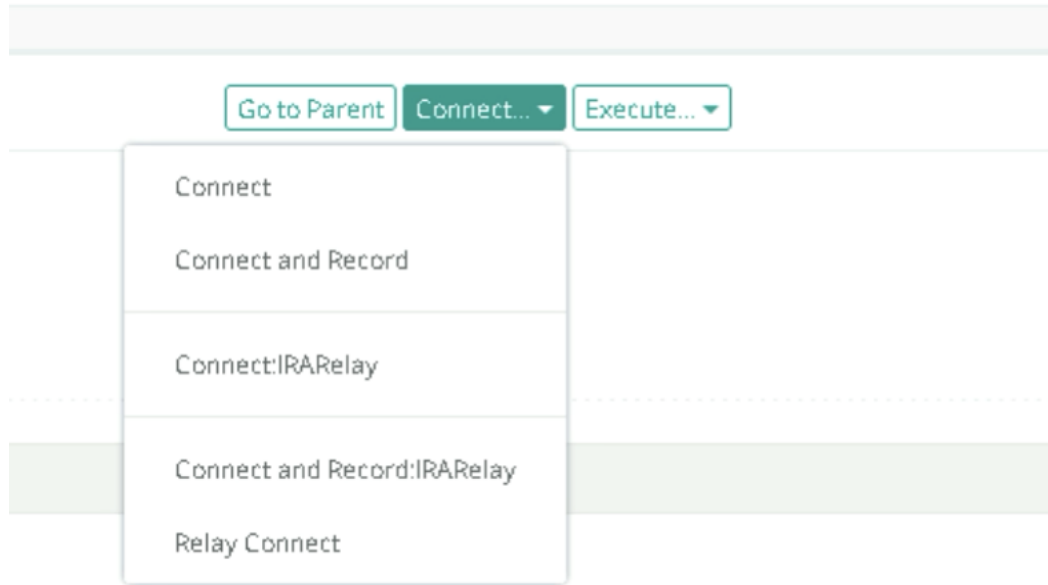
1. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor and add the following new parameters:

```
1 | xtam.ssh.proxy=enabled
2 | xtam.ssh.proxy.port=2022
```

2. Restart Pammanager (Linux) or pammanagement service on Windows.

## Testing SSH Proxy connection with Relay node

1. In case of Relay node, users can get the connection string by navigating to the record to be connected and clicking on Connect > Relay Connect and clicking the connection string value to the clipboard:



2. The instructions to connect and test using native tools such as Putty are available [here](#).
3. Replace the **Hostname** with the hostname from the connection string captured in #1.

## RDP Proxy with Relay Node

### Requirements

- Ensure Relay node setup is complete ([PAM Web Configuration](#)).

### Relay Node Configuration

1. Open the file `$PAM_HOME/web/conf/catalina.properties` on the relay node in a text editor and add the following new parameters:



```
1 | xtam.rdp.proxy=enabled
2 | xtam.rdp.proxy.port=3388
```

2. Restart **Pammanager** (Linux) or **pammanagement** service on Windows.

### Testing RDP Proxy connection with Relay node

1. Follow steps as given in <https://help.xtontech.com/content/administrators-and-power-users/secure-remote-sessions-connect/rdp-client-proxy-sessions.htm>.
2. In the *Relay Connect* popup, select the correct *Relay node* and press **Download Remote Desktop File**:

#### Relay Connect<sup>?</sup>

##### Connect Using Node

Relay Node-1

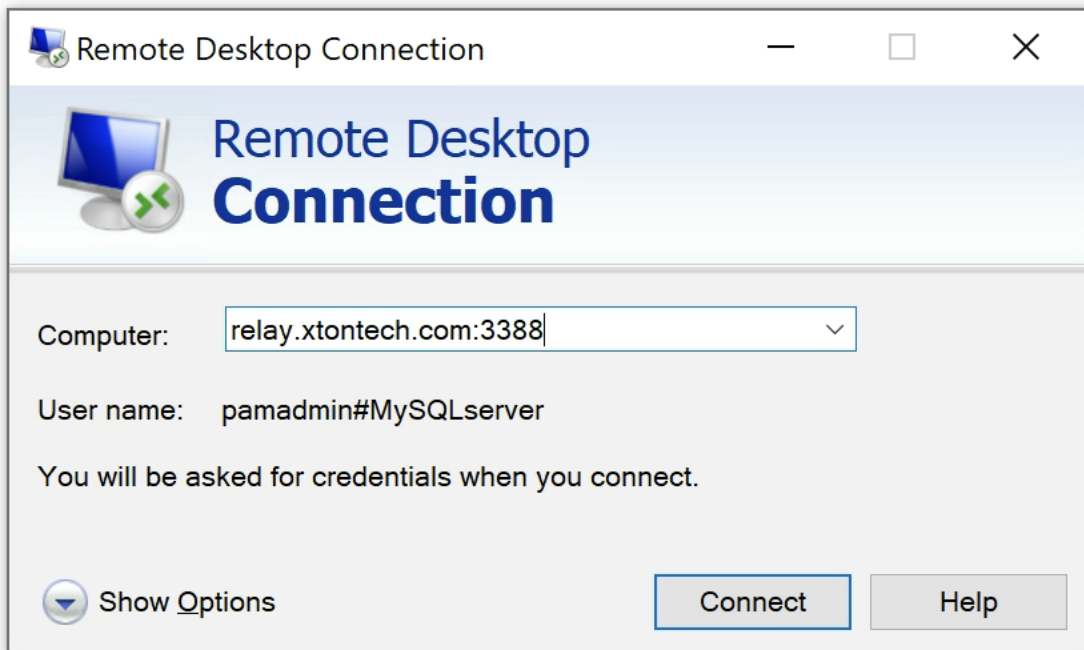
Cancel

Download Remote Desktop File

Connect

Connect and Record

3. The instructions to connect and test using native tools such as Windows RDP Client are available here: <https://help.xtontech.com/content/administrators-and-power-users/secure-remote-sessions-connect/rdp-client-proxy-sessions.htm>.
4. Replace the **Hostname** with the hostname from the connection string captured in #1.



# Command Line Secure Shell Interface (SSH) with Relay Node

## Requirements

- Ensure Relay node setup is complete ([PAM Web Configuration](#)).
- Ensure SSH proxy on relay node is complete ([SSH Proxy with Relay Node Configuration](#)).

## Testing SSH connection with relay node

1. [The instructions to connect and test using native tools such as Putty.](#)
2. Replace the **Hostname** with the hostname of the relay node.

## Limit Relay Node option to specific containers or records

In some cases, it may be required to associate relay nodes to specific containers (folders or vaults) or records.

## Requirements

- Ensure Relay node setup is complete ([PAM Web Configuration](#)).

## Additional Configuration

- Set the Settings > Use Proximity Groups to Resolve Relays property to **Enabled**.
- From Settings > Proximity Groups, Select the **Add Relay** button and choose the Relay node to be associated.

Application Settings

Root Folder / System Settings

---

Application Nodes

Proximity Groups

Database

Registration

Parameters

Mail Server

AD

Syslog

---

Proximity Groups ⓘ

---

Group: Relay Group (Folder)

---

Group Name

Relay Group (Folder)

Selector

Folder Based ▾

Folder Name

Relays Folder

---

Servers

Add Server

Add Relay

Relay: iratest-01 ▾

localhost :4822 ▾

Relay: EF-serv2016-01 ▾

Enabled

☒

## Storing Master Password on Separate Server

For additional security, PAM provides a simple method for storing your Master Password ([what is the Master Password?](#)) key on a separate host.

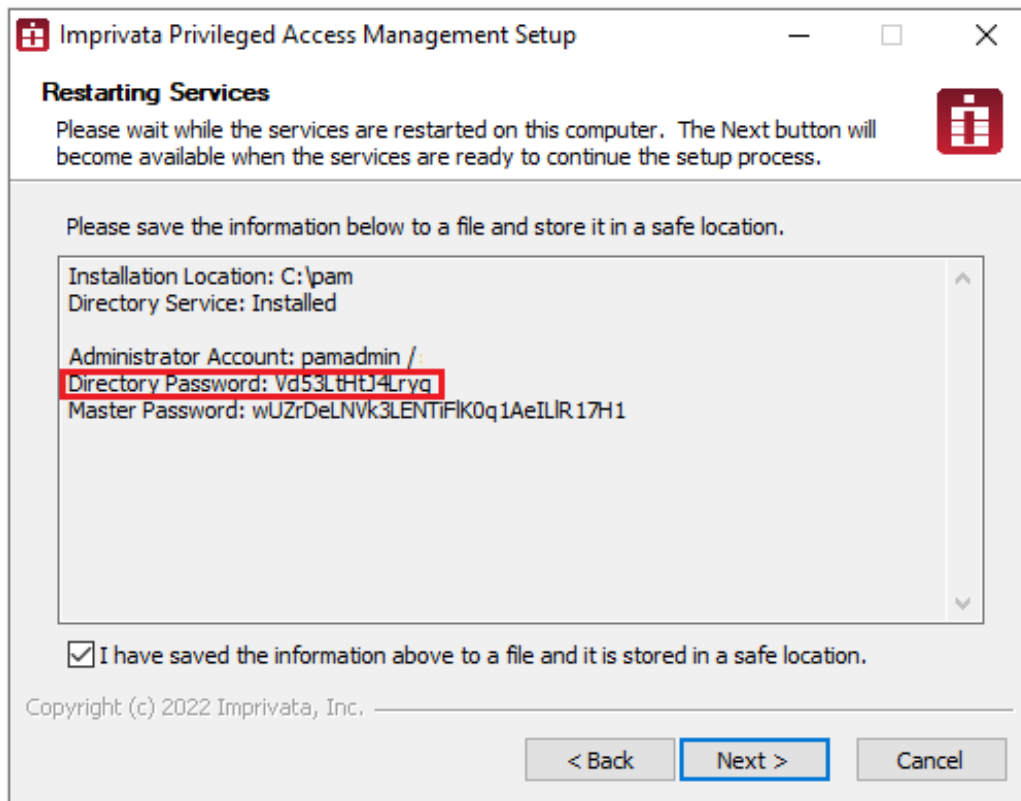
If you are considering this approach, then the following describes the method to configure this setup during installation.

## Pre-requisites

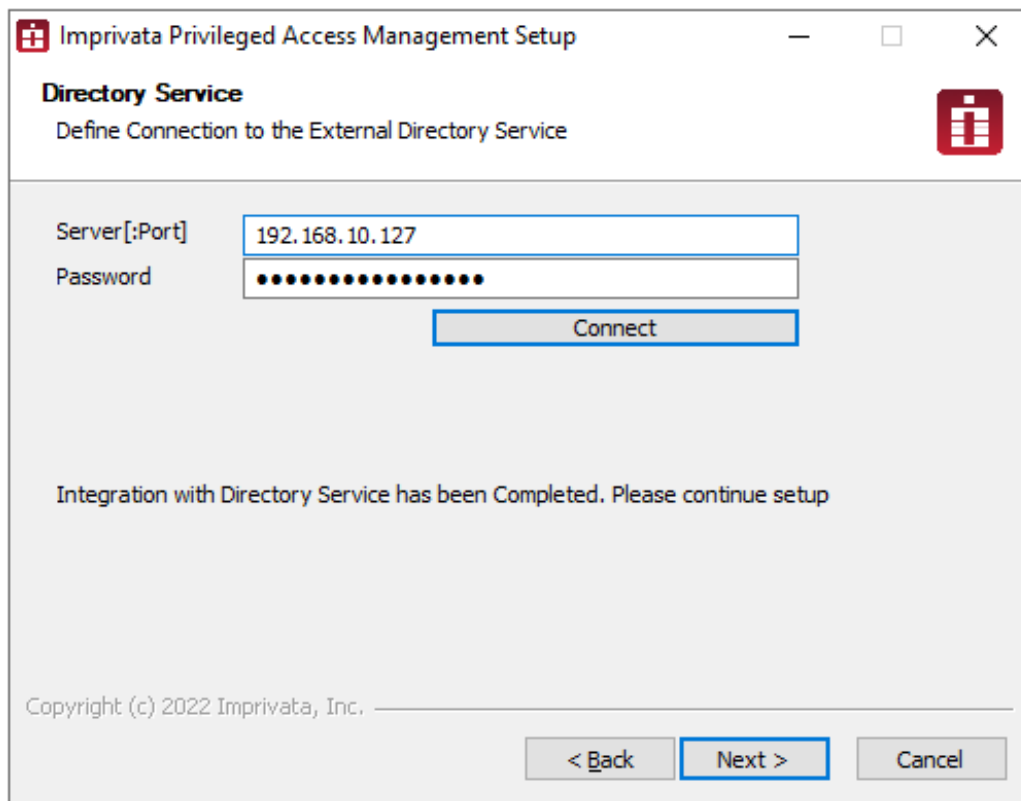
- At least two servers, one to store the master password and the other for the PAM installation.
- Encrypted traffic between these servers is over port 10636. Ensure this port is open.

## Configuration

1. Login to the server that will be used to store the Master Password and run the PAM setup file.
2. During installation, on the *Choose Components* screen, check the option **Directory Service** only.
3. Complete the installation and save the Passwords supplied at the end to a safe location. You will need the Directory Password later in this guide.



4. **Login** to the server that will be used to for the PAM installation and run the PAM setup file.
5. During installation, on the *Choose Components* screen, check all the options required for your deployment, leaving the Directory Service option unchecked.
6. **Continue** through the installation as required.
7. When you reach the *Directory Service* screen:
  - a. For the **Server**, enter the name or IP address of your Master Password server and optionally the port 10636.  
For example, *serverName* or *serverName:10636*.
  - b. For the **Password**, enter the Directory Password that was generated at the end of the PAM Master Password installation (example shown in the screenshot above).
8. Click the **Connect** button to test.



9. When the test connection is successful, continue as required by clicking **Next** to complete the PAM installation.

## External Database Connection Strings

PAM supports a wide range of the most popularly used databases system in the market.

When configuring PAM to use your own database, you will need to supply the database connection string.

In general, the connection string will comply with the following example:

*db-host or db-host:port*

NOTE: The installation process does not create its own database or tablespace but rather makes use of an existing one. With that in mind, please ensure one with the name “PamDB” already exists as this will be used by the application.

### Apache Derby

*db-host or db-host:port*

### Microsoft SQL Server

*db-host or db-host:port*

### MySQL

*db-host or db-host:port*

# Oracle

Service: `//db-host/db-service`

Instance: `//db-host:port:SID`

# PostgreSQL

`db-host` or `db-host:port`

## PostgreSQL database account management

PAM users get manage accounts in PostgreSQL database including *Check Status* and *Password Reset* tasks including direct and shadow account access as well as permission and workflow based *password unlock* and *custom script execution*.

Initially hidden record type for PostgreSQL database including *check status* and *password reset tasks* based on the PostgreSQL Connection string given by:

`host:port/database`, `host/database`, `host[:port]/database`

or full JDBC connection string:

`jdbc:postgresql://host[:port]/database`

To enable account management:

- **Connection** (Type: String, Display Name: Connection String) to define `host:port/database` connection string
- **CommandUser** (Type: String, Display Name: Command User) to define account login
- **CommandPassword** (Type: String, Display Name: Command Password) to define account password

If you want to change the database after deployment, please see the following article for more information: [Changing PAM's back-end Database.](#)

## Configure HTTP to HTTPS Redirect

### To Configure HTTP (8080) to HTTPS (443/6443) Redirection

If you want to redirect HTTP 8080 to HTTP 443/6443 then follow the steps provided below.

1. Login to PAM host server and open the file `$PAM_HOME/web/conf/server.xml` in a text editor.
2. Near the end of this file, locate the line:

```
1 | <Host name="localhost" appBase="webapps"
2 |     unpackWARs="true" autoDeploy="true">
```

3. Immediately after that line, add this new line:

```
1 | <Valve className="org.apache.catalina.valves.rewrite.RewriteValve" />
```

As a result, it should look like this:

```

1 | <Host name="localhost" appBase="webapps"
2 |     unpackWARs="true" autoDeploy="true">
3 |
4 |     <Valve className="org.apache.catalina.valves.rewrite.RewriteValve" />

```

4. Next, in this same `server.xml` file, locate the connector section for port 8080. In this section, make these two changes:

- from: `secure="true"` to: `secure="false"`
- from: `scheme="https"` to: `scheme="http"`

Before the two changes, shown in proxyPort `secure="true" scheme="https"`:

```

1 | <Connector port="8080" protocol="HTTP/1.1"
2 |
3 |     connectionTimeout
4 |     = "20000" proxyPort="443" secure="true" scheme="https" SSLEnabled="false"
5 |
6 |     redirectPort="443" />

```

After the two changes, shown in proxyPort `secure="false" scheme="http"`:

```

1 | <Connector port="8080" protocol="HTTP/1.1"
2 |
3 |     connectionTimeout
4 |     = "20000" proxyPort="443" secure="false" scheme="http" SSLEnabled="false"
5 |
6 |     redirectPort="443" />

```

5. Save and close the file.
6. Next, download this new `rewrite.config` file (<https://help.xtontech.com/ref/rewrite.config>) and place it in the directory `$PAM_HOME/web/conf/catalina/localhost/`.
7. If you are using HTTPS 443, then you do not need to make any changes to this new `rewrite.config` file. If you are using an HTTPS port other than 443, like 6443, then open this file in a text editor and change 443 to your HTTPS port number. **Save and close** the file when done.
8. Finally, restart the **PamManagement** (Windows) or **pammanager** (Linux) service to complete the process. When the service comes back online, any connection made to 8080 will be redirected to 443 or another port defined earlier.

## Changing the PAM Database

Switching PAM's back-end database from one to another is a relatively straight forward process. For example, you originally deployed your PAM instance using the Internal Database option and now wish to use MS SQL. The following article describes this process.

1. Navigate to `$PAM_HOME/web/conf` and make a copy of the file **catalina.properties**. Save this to a location outside of `$PAM_HOME` and if something goes wrong, you can simply replace this file, restart the

service and you will be back to the original database (assuming it still exists).

2. Create an on-demand Export of PAM (Administration > Settings > Database > **Export Encrypted**).
3. Manually create the new database in your chosen database. The database name should be **PamDB** (case sensitive) and the database account should have full control, owner or ALL privileges.
4. Next we will run an PAM command to switch it from your current database to this new one. Execute the command from `$PAM_HOME`, replacing the value in **green** to your new **database** vendor and the values in **red** with your new database parameters: **database****db.server db.user db.password**. The supported database vendors are:

#### Database Vendors

- MSSQL
- MySql
- Oracle
- PostgreSQL
- Derby

For Windows:

```
1 | bin\PamDirectory.cmd DBConnect web database db.server db.user db.password
```

For Unix or Linux:

```
1 | bin/PamDirectory.sh DBConnect web database db.server db.user db.password
```

For example, if your PAM instance is deployed to a Windows server and you are switching the back-end database to MS SQL, your command would look similar to this:

```
1 | bin\PamDirectory.cmd DBConnect web MSSQL 10.0.0.152 sa 6QP8psY93PWVe3Dr
```

Or if you do not want to include the password in the command, you can simply replace it with a dash character and after it is executed, you will be prompted to enter the required password.

Note if your password includes special characters, we would recommend this approach to minimize potential errors.

```
1 | bin\PamDirectory.cmd DBConnect web MSSQL 10.0.0.152 sa -
```

5. After the command is run successfully, restart the **PamManagement** (Windows) or **pammanager** (Linux) service.
6. When the service restarts, open your browser and login to PAM. You should see the Database Initialization screen, click the **Initialize** button to setup PAM's new database.
7. After it initializes your new database, navigate to Administration > Settings > Database and click the **Import** button for the export you created in [step 2](#).
8. Once the import is complete (may take several minutes), test the import by clicking around the Vault to make sure everything is running as expected (folders, permissions, unlock, etc.)

If anything goes wrong during the procedure, you can revert the process by replacing the **catalina.properties** file that was saved in step 1, restarting the service again and PAM will return to your original database. **Do not delete** this original PAM database until you are absolutely sure the entire process has completed successfully.

## Enabling JMX Monitoring

### JMX Support for PAM Instances

The PAM Framework component (Java JRE) now includes support for Java Management Extensions (JMX). JMX is a broad topic.

There are many ways to configure JMX, and the correct configuration depends on the network environment and use case.

Comprehensive JMX documentation is provided in the JMX User Guide:

<https://docs.oracle.com/en/java/javase/21/jmx/java-management-extensions-jmx-user-guide.html>.

There is also detailed JMX documentation for Apache Tomcat:

<https://tomcat.apache.org/tomcat-9.0-doc/monitoring.html>

The most common reason for enabling JMX in Apache Tomcat is to integrate with Zabbix, LogicMonitor, or other similar tools.

Monitoring software usually includes JMX integration documentation, for example:

<https://www.zabbix.com/integrations/tomcat>

<https://www.logicmonitor.com/support/logicmodules/datasources/data-collection-methods/jmx-data-collection>

### JMX Security Considerations

JMX is often configured to expose management endpoints to external monitoring tools.

This must be done carefully with due consideration to security.

Recommended practice is to configure secure transport, authentication, and roles for remote connections.

The Tomcat JMX documentation linked above is a good source for guidance on this topic.

Network firewall policies can be (and probably should be) configured to control which network hosts are able to connect to the JMX endpoints.



Please note that the examples provided in this article assume PAM is installed into a specific folder `$PAM_HOME` which are expected to be `/opt/pam` for Linux or `C:\PAM` for Windows. Replace the `$PAM_HOME` with your correct PAM installation folder.

## Checking JMX Support for PAM Framework Component (Java JRE)

You can check your current PAM Framework (Java JRE) to see if it has JMX enabled.

Run the following command.

For Windows:

```
1 | $PAM_HOME\jre\bin\java.exe --list-modules | findstr java.management.rmi
```

For Linux:

```
1 | $PAM_HOME/jre/bin/java --list-modules | grep java.management.rmi
```

If JMX is enabled, the current JMX RMI module version should be displayed, for example:

*java.management.rmi@21.0.4*

The version shown here (21.0.4) may update over time but if no output is produced, then JMX is not enabled and you may need to [upgrade your PAM Framework component](#).

Please note that it is possible the version shown here (21.0.4) may update over time, but if no output is produced, then JMX is not enabled and you may need to [upgrade your PAM Framework component](#).

## Enabling and Configuring

### *JMX for Apache Tomcat on Linux*

For PAM on Linux, Java options for Apache Tomcat are defined in this script file:

`$PAM_HOME/bin/pammanager`

This script file may be modified to extend Java options with JMX configuration properties. Please make a backup copy of the file before making any changes.

Open the `$PAM_HOME/bin/pammanager` file, locate the line with **JAVA\_OPTS**, it should look similar to this:  
*export JAVA\_OPTS="\$DERBY\_OPTS ..."*

Note: This is usually a very long line of options. Only the first part is shown here to save space.

The idea is to extend JAVA\_OPTS with JMX properties after this line, like this:

```

1 | export JAVA_OPTS="$DERBY_OPTS ..."
2 | # Enable JMX for Apache Tomcat
3 | export JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote"
4 | export JAVA_OPTS="$JAVA_OPTS -Djava.rmi.server.hostname=localhost"
5 | export JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=8686"
6 | export JAVA_OPTS="$JAVA_OPTS -Djava.net.preferIPv4Stack=true"
7 | export JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.authenticate=false"
8 | export JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.ssl=false"

```

The first line is unchanged, but then additional lines are added to set the JMX properties.

This is a very simple example with authentication and secure transport disabled. In a production environment, authentication and secure transport should be enabled. Consult JMX documentation for guidance.

After updating this script file, the PAM Manager service must be reloaded and restarted to pick up the changes:

```
1 | sudo systemctl daemon-reload
```

```
1 | sudo systemctl restart pammanager.service
```

## JMX for Apache Tomcat on Windows

For PAM on Windows, Java options for Apache Tomcat are defined in this script file:

`$PAM_HOME\bin\ServiceManagement.cmd`

This script file may be modified to extend Java options with JMX configuration properties. Please make a backup copy of the file before making any changes.

Open the `$PAM_HOME\bin\ServiceManagement.cmd` file, locate the line with **JAVA\_OPTS**, it should look similar to this:

`@set JAVA_OPTS=%DERBY_OPTS% ...`

Note: This is usually a very long line of options. Only the first part is shown here to save space.

The idea is to extend JAVA\_OPTS with JMX properties after this line, like this:

```

1 | @set JAVA_OPTS=%DERBY_OPTS% ...
2 | :: Enable JMX for Apache Tomcat
3 | @set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote
4 | @set JAVA_OPTS=%JAVA_OPTS% -Djava.rmi.server.hostname=localhost
5 | @set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.port=8686
6 | @set JAVA_OPTS=%JAVA_OPTS% -Djava.net.preferIPv4Stack=true
7 | @set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.authenticate=false

```

```
8 | @set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.ssl=false
```

The first line is unchanged, but then additional lines are added to set the JMX properties.

This is a very simple example with authentication and secure transport disabled. In a production environment, authentication and secure transport should be enabled. Consult JMX documentation for guidance.

For Windows deployments, start the **PamManagement** service to update the Windows registry:

```
1 | $PAM_HOME\bin\ServiceManagement.cmd remove
```

```
1 | $PAM_HOME\bin\ServiceManagement.cmd install
```

Note: The **PamManagement** service resets to the default *Local System account* Log on property once this service for PAM is reinstalled. If you are using a Log account other than an *Local System account* for this service, then you must restore it prior to restarting the **PamManagement** service. Navigate to Services > PamManagement > Properties > Log, then select **This account:** and restore the required service account.

## How to increase the amount of memory a PAM server can use

You can increase the dynamic (heap) memory that a PAM system will use for Windows or Linux Operating Systems, please see instructions below.

### Information

PAM in the default configuration uses maximum 25% of all computer RAM for dynamic (heap) memory assuming that there might be other applications competing for the same memory. For example, if computer has 16 Gb of RAM, PAM will only use 4 Gb by default. If you think, you can give PAM more RAM there is a way to configure the max memory.

In the steps below, we make 8 Gb (8192 Mb) as the maximum amount of memory PAM can consume. You can set the max memory to whatever you desire using the below examples. Keep in mind that this max memory should allow other processes on the OS to work too that also includes other PAM components such as session manager or directory services.

If the system cannot allocate sufficient memory for the processes during startup, it will fail to start the service **pammanager/PamManagement** service.

The max memory setting to use requires some experimentation to ensure that the PAM Server has sufficient memory yet still allowing other processes to run on the same computer.

There are different steps that need to be taken to increase the maximum Java RAM for Linux and Windows.

There are a few settings that can be set, such as:

- -Xms, which specifies the initial memory allocation pool
- -Xmx, which specifies the maximum memory allocation pool for a Java virtual machine (JVM)

Note: We do not set an -Xms setting here, leaving the initial memory allocation pool as default and memory usage to grow.

The syntax options for the memory setting are shown in the examples below:

4GB	-Xmx4096m
	-Xmx4g
8GB	-Xmx8192m
	-Xmx8g
10GB	-Xmx10g
24GB	-Xmx24g

## Linux

For example, to make max memory 8GB.

1. Create a file named `setenv.sh` in the `$PAM_HOME/web/bin` folder with the following content.
  - `export CATALINA_OPTS="$CATALINA_OPTS -Xmx8192m"`
2. Save the file.
3. Make its owner:group permissions the same as all other files in the folder, and make it executable
  - `chmod +x setenv.sh`
4. Restart the pammanager service.
5. Check in the log file that it used this parameter by observing the line like this one in the beginning after startup:
  - 21-Dec-2020 14:55:32.657 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log  
Command line argument: -Xmx8192m

## Windows

On Windows, the PamManagement service needs to be modified to contain the new max memory setting. This is done by updating the *ServiceManagement* configuration file, then removing and again installing the *PamManagement* service. For example, to make max memory 8GB.

1. Stop the PamManagement service.
2. Make a copy of the `$PAM_HOME\bin\ServiceManagement.cmd` file and save this to a location outside of the PAM directory structure.
3. Edit the `$PAM_HOME\bin\ServiceManagement.cmd` file.
4. Locate the line that starts with `@set JAVA_OPTS=%DERBY_OPTS%`
5. Before the text `-Dlog4j.configuration=`, add the following:
  - `-Xmx8192m`
6. This should now read something like:

- a. `@set JAVA_OPTS=%DERBY_OPTS% -Xmx8192m -Dlog4j.configuration=file:/.....etc.`
7. Save the `ServiceManagement.cmd` file.
8. Run the following two commands from a command prompt (running as Administrator)
  - a. `cd C:\$PAM_HOME`, where `$PAM_HOME` is your Pam Directory folder} (e.g. `cd C:\PAM`)

```
1 | bin\ServiceManagement.cmd remove
```

b.

```
1 | bin\ServiceManagement.cmd install
```

c.

9. Start the *PamManagement* service.

## To verify the max memory has changed

1. Log into PAM and navigate to Management > About.
2. At the bottom of the page (Performance), view the Memory middle value.
3. Memory (total/max/free): 775,946,240 / 4,294,967,296 / 317,691,720.

## Generate and Replace the SSL Certificate for PAM WEB Session Manager

Use this guide to generate a new SSL certificate to replace the current certificate for your WEB Session Manager.

1. Generate a new SSL certificate using this openssl command:

```
1 | openssl req -x509 -newkey rsa:4096 -keyout session.key -out session.crt -  
sha512 -days 3650 -nodes -subj '/CN=Session Manager'
```

The command will produce two files: `session.key` and `session.crt`

2. Backup your existing certificate files on the WEB Session Manager host by copying the following files to a location outside of `$PAM_HOME`

- On a Linux host:

```
$PAM_HOME/guac/etc/ssl/server.key
```

```
$PAM_HOME/guac/etc/ssl/server.crt
```

- On a Windows host:

```
$PAM_HOME\guacd\etc\ssl\server.key
```

```
$PAM_HOME\guacd\etc\ssl\server.crt
```

3. Replace your existing files with the new ones generated in [step #1](#):

On a Linux host:

```
$PAM_HOME/guac/etc/ssl/server.key
```

```
$PAM_HOME/guac/etc/ssl/server.crt
```

On a Windows host:

```
$PAM_HOME\guacd\etc\ssl\server.key
```

```
$PAM_HOME\guacd\etc\ssl\server.crt
```

- Restart **pamsession** (Linux) / **PamSession** (Windows) services on the WEB Session Manager host.
- Import newly generated certificates into the keystores on all master nodes by running the following command from the `$PAM_HOME` home folder and importing the missing certificate into the keystore by following the interactive prompts. Replace the red highlighted value in the command with that of your WEB Session Manager host FQDN.

- On a Linux host:

```
1 | bin/PamDirectory.sh SSLImport web-session-manager-host-fqdn 4822
```

- On a Windows host:

```
1 | bin\PamDirectory.cmd SSLImport web-session-manager-host-fqdn 4822
```

- Restart **pammanager** (Linux) / **PamManagement** (Windows) service on the master nodes after importing the certificate.
- Next, check the connectivity of the master nodes to the WEB Session Manager with the updated certificate by checking for the green status of the session manager in the Administration > Settings > Proximity Groups tab of the WEB GUI.
- To roll-back the change, if needed, restore the following files on the WEB Session Manager host and restart **pamsession** (Linux) / **PamSession** (Windows) service:

- Linux

```
$PAM_HOME/guac/etc/ssl/server.key
```

```
$PAM_HOME/guac/etc/ssl/server.crt
```

- Windows

```
$PAM_HOME\guacd\etc\ssl\server.key
```

```
$PAM_HOME\guacd\etc\ssl\server.crt
```

## Generate and Replace the SSL Certificate for PAM Local Directory Service

Use this guide to generate a new SSL certificate for use by PAM's Local Directory Service and to replace the existing certificate.

- Generate a new certificate by executing the following command from the command line in the PAM home folder `$PAM_HOME`:

On a Linux host:

```
1 | bin/PamKeytool.sh -genkey -keyalg "RSA" -alias ads.local -keystore web/conf/dskeystore.jks -validity 730 -deststoretype jks
```

On a Windows host:

- 1 | `bin\PamKeytool.cmd -genkey -keyalg "RSA" -alias ads.local -keystore web\conf\dskeystore.jks -validity 730 -deststoretype jks`

```
PS C:\pam> .\bin\PamKeytool.cmd -genkey -keyalg "RSA" -alias c365srvwap03.connect365.net -keystore web\conf\dskeystore.jks -validity 730 -deststoretype jks
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: c365srvwap03.connect365.net
What is the name of your organizational unit?
[Unknown]:
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=c365srvwap03.connect365.net, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
[No]: yes
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 730 days
for: CN=c365srvwap03.connect365.net, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
Enter key password for <c365srvwap03.connect365.net>
(RETURN if same as keystore password):
Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore web\conf\dskeystore.jks -destkeystore w
eb\conf\dskeystore.jks -deststoretype pkcs12".
PS C:\pam>
```

Please note that the only field you have to fill is "What is your first and last name?" For this field, enter the FQDN which you'll use to connect from other nodes, or the host name of this node itself.

2. Edit the Apache DS LDAP settings file `ads-serverid=ldapserver.ldif` located in the following folder using a text editor:

On a Linux host:

- 1 | `$PAM_HOME/ds/instances/default/conf/ou=config/ads-directoryserviceid=default/ou=servers`

On a Windows host:

- 1 | `$PAM_HOME\ds\instances\default\conf\ou=config\ads-directoryserviceid=default\ou=servers`

Add 2 new parameters to the end of this file with the path to the keystore file and its password:

*ads-keystoreFile:*

*ads-certificatePassword:*

Password can be stored as plain text or base64 encoded string. If you are using the *base64* variant you'll need to add a second colon after the parameter name as shown in the second example below.

The plain text version will look similar to this:

```
ads-keystoreFile: c:/pam/web/conf/dskeystore.jks
ads-certificatePassword: SecretPass01
```

And *base64* encoded:

```
ads-keystoreFile: c:/pam/web/conf/dskeystore.jks
ads-certificatePassword: U2VjcmV0UGFzczAx
```

You can convert a plain text to base64 using an online service or OS command-line utility:

<https://www.base64encode.org>

- Restart the **PamDirectory** or **pamdirectory** service.
- On all master nodes run the following command from the \$PAM\_HOME location to import the new certificate:

On a Linux host:

```
1 | bin/PamDirectory.sh SSLImport localhost 10636
```

On a Windows host:

```
1 | bin\PamDirectory.cmd SSLImport localhost 10636
```

- Add the certificate to the java cert store by choosing 1 in the dialog

```
PS C:\pam> .\bin\PamDirectory.cmd SSLImport c:\365srvwap03.connect365.net 10636
Loading KeyStore C:\pam\jre\lib\security\cacerts...
Opening connection to c:\365srvwap03.connect365.net:10636...
Starting SSL handshake...
javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
at java.base/sun.security.ssl.Alert.createSSLException(Alert.java:131)
at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:370)
at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:313)
at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:300)
at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.checkServerCerts(CertificateMessage.java:654)
at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.onCertificate(CertificateMessage.java:473)
at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.consume(CertificateMessage.java:369)
at java.base/sun.security.ssl.SSLHandshake.consume(SSLHandshake.java:396)
at java.base/sun.security.ssl.HandshakeContext.dispatch(HandshakeContext.java:480)
at java.base/sun.security.ssl.HandshakeContext.dispatch(HandshakeContext.java:458)
at java.base/sun.security.ssl.TransportContext.dispatch(TransportContext.java:200)
at java.base/sun.security.ssl.SSLTransport.decode(SSLTransport.java:172)
at java.base/sun.security.ssl.SSLSocketImpl.decode(SSLSocketImpl.java:1500)
at java.base/sun.security.ssl.SSLSocketImpl.readHandshakeRecord(SSLSocketImpl.java:1415)
at java.base/sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:450)
at java.base/sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:421)
at com.pam.dir.Directory.sslImport(Directory.java:4466)
at com.pam.dir.Directory.main(Directory.java:272)
Caused by: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
at java.base/sun.security.validator.Validator.validate(Validator.java:439)
at java.base/sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:306)
at java.base/sun.security.validator.PKIXValidator.engineValidate(PKIXValidator.java:306)
at java.base/sun.security.validator.Validator.validate(Validator.java:264)
at java.base/sun.security.ssl.X509TrustManagerImpl.checkTrusted(X509TrustManagerImpl.java:242)
at java.base/sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:113)
at com.pam.dir.Directory$SavingTrustManager.checkServerTrusted(Directory.java:4652)
at java.base/sun.security.ssl.AbstractTrustManagerWrapper.checkServerTrusted(SSLContextImpl.java:1441)
at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.checkServerCerts(CertificateMessage.java:638)
... 13 more
Caused by: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
at java.base/sun.security.provider.certpath.SunCertPathBuilder.build(SunCertPathBuilder.java:141)
at java.base/sun.security.provider.certpath.SunCertPathBuilder.engineBuild(SunCertPathBuilder.java:126)
at java.base/java.security.cert.CertPathBuilder.build(CertPathBuilder.java:297)
at java.base/sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:434)
... 20 more
Server sent 1 certificate(s):
1 Subject: CN=c365srvwap03.connect365.net, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
Issuer: CN=c365srvwap03.connect365.net, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
Expires: Thu Apr 25 07:24:31 PDT 2024
sha1 ce 11 82 6f 93 ab 3f 2a dd f3 6a a5 40 f9 c1 80 1e 4f fa 50
md5 6c a1 e4 6c ec c2 86 8f 08 ee 50 be 17 f7 1d 26
Enter certificate to add to trusted keystore or 'q' to quit: [1]
1
```

- Restart **pammanager** (Linux) / **PamManagement** (Windows) service on master nodes.

## Integration with HSM device

PAM relies on the database integration with HSM device to increase security of the encrypted data. PAM provides a wide selection of back-end databases chosen to satisfy maintenance, compliance or regulatory requirements.

For HSM integration choose the database that supports database encryption with the master key managed by your HSM device.

Use the following steps to introduce HSM into data encryption strategy:



1. Configure your database server with your encryption provider integrated with your HSM device.
2. Create PamDB database.
3. Enable database encryption using the crypto provider configured above.

Example for MS SQL Server.

- Run following query against PamDB database:

```
1 | USE PamDB;  
2 | CREATE DATABASE ENCRYPTION KEY  
3 | WITH ALGORITHM = AES_256  
4 | ENCRYPTION BY SERVER ASYMMETRIC KEY <ASYNCKeyName>;
```

where ASYNCKeyName is the name of key prepared with your crypto provider.

- Enable encryption for database with the following query:

```
1 | ALTER DATABASE PamDB  
2 | SET ENCRYPTION ON;
```

4. Install PAM using configured PamDB.

## Integration with Smart Cards

The PAM WEB Server provides a mechanism to authenticate users who present client certificates (X.509) during the login process.

The client certificate might come from a Smart Card or be deployed into a user's browser.

The document below describes the PAM configuration to enable client certificate authentication.

Note: this document describes configuration on **Linux**. For Windows, all is almost the same except paths to files and executable names.

1. Create new trust store with root CA certificate in it:
  - Go to PAM folder and run followed command:

```
1 | bin/PamKeytool.sh -import -file /path/to/ad2_root.cer -alias trustedCA -  
   | keystore /opt/xtam/web/conf/truststore.jks
```

- Enter a new password for the newly created cert store.
- Answer yes, once it asks for trust cert or not.
- Example output is in the following screenshot:

```

root@xtam-local:/opt/xtam$ bin/PamKeytool.sh -import -file /home/xtam/ad2_root.cer -alias trustedCA -keystore /opt/xtam/web/conf/truststore.jks
Enter keystore password:
Re-enter new password:
Owner: CN=ad2-DC-CA, DC=ad2, DC=net
Issuer: CN=ad2-DC-CA, DC=ad2, DC=net
Serial number: 5
Valid from: Wed Apr 20 15:46:51 UTC 2016 until: Tue Apr 20 15:56:49 UTC 2021
Certificate fingerprint:
    SHA1: B0:AC:
    SHA256: F5:C4:
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

Extensions:
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00
...
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:
    CA:true
    PathLen:2147483647
]
#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
    DigitalSignature
    Key_CertSign
    Crl_Sign
]
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
    KeyIdentifier [
0000: B9 E:
0010: 76
    ]
]
Trust this certificate? [no]: yes
Certificate was added to keystore

```

2. Stop **pammanager / PamManagement** service (depends on host OS).

3. Edit `$PAM_HOME/web/conf/server.xml`.

- Add the following properties to connector configuration below

**"BEGIN: SELF SIGNED SSL" comment: truststoreFile="/opt/xtam/web/conf/truststore.jks"**  
**truststorePass="pass@word1",**

where **truststoreFile** is the path to trust certificate store from **step 1** and **truststorePass** is password for this store.

- Change **clientAuth** property value from **"false"** to **"want"** - if you want to have a fall back to **certificate/smartcard** authentication with forms based **auth**, or to **"true"** - if you want to force PAM to use **certificate/smartcard** authentication only.
- You can see the configuration example in the screenshot below:

```

<!-- BEGIN: SELF SIGNED SSL -->
<Connector
    keystoreFile="${xtam.cert.path}"
    keystorePass="${xtam.cert.password}"
    protocol="com.pam.config.Http11NioEncryptedProtocol"
    port="6443" maxThreads="200" proxyPort="443"
    scheme="https" secure="true" SSLEnabled="true"
    sslProtocol="TLSv1.2"
    truststoreFile="/opt/xtam/web/conf/truststore.jks"
    truststorePass="pass@word1"
    sslEnabledProtocols="TLSv1.2+TLSv1.3"
    ciphers="TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256"
    clientAuth="want" keystoreType="JKS"/>
<!-- END: SELF SIGNED SSL -->

```

4. Edit `$PAM_HOME/web/conf/catalina.properties`.

Add this property like on screenshot below:

```
cas.authn.x509.principalType=SUBJECT_ALT_NAME
cas.view.defaultRedirectUrl=https://xtamubuntu.
# CAS x509 auth
cas.authn.x509.principalType=SUBJECT_ALT_NAME
# to override-remove default users
cas.authn.accept.users=
# CAS master password
cas.standalone.config.security.psw=J09n5vJF2d2t
cas.standalone.config.security.alg=PBEWithMD5And
#cas.authn.ldap[N].type=AUTHENTICATED|AD
cas.authn.ldap[0].type=DIRECT
```

By default, this parameter is sufficient to work with certificates, but only in the case of one internal certificate authority, if there are subordinate CAs, and the user certificate is issued, you need to add the second parameter:

**cas.authn.x509.max-path-length-allow-unspecified=true**

5. Move `cas.war` and `cas` folder from `$PAM_HOME/web/webapps/` to some location outside `$PAM_HOME` folder for being able to revert those changes.
6. Download [x509-enabled CAS module](#).
7. Put downloaded `cas.war` file to `$PAM_HOME/web/webapps/` folder. Changing the ownership of this file may be necessary.

For example, if PAM services are running under `xtam` user account and PAM is deployed to `/opt/xtam/`, followed command will change ownership for all files inside this directory: `chown -R xtam:xtam /opt/xtam`.

Start **pammanager / PamManagement** service (depends on host OS).

8. After services start **certificate/smartcard** authentication should work.

Additional configuration on client PC might be needed, for example installing smartcard drivers or put certificate to OS/browser trusted certificate store.

## PAM Internal Database Tables

Please find the list of PAM internal database tables in the spreadsheet below with a breakdown by the following categories:

- \* **Configuration** – tables used for system configuration (record types, workflows setup, password reset policies, session routing, etc)
- \* **Operations** – tables used to record historical data: audit log, job history, event subscriptions, sessions
- \* **Content** – tables used to store assets (records, folders, permissions)

\* **Cache** – tables used for temporary data local for the nodes using this database (authentication service tickets, locks, messages from the queue, etc).

<https://help.xtontech.com/ref/XTAM%20Tables.xlsx>

The categorized list of tables might be used to design replication procedures when deciding priorities of data copied from different tables.

In databases that support sequences, special attention should be paid to the sequence called **HIBERNATE\_SEQUENCE** that should be maintained between databases.

This sequence is used to generate primary keys for the system tables.

Its values should be greater than the largest primary key in the system.

For databases that do not support sequences (MySQL, Maria DB, etc) the role of the sequence is played by the correspondingly named table.

# Linux Installation Guide

## Introduction

This guide is designed to show system administrators how to install, initialize and run Privileged Access Management (PAM) on a Unix computer.

## Technical Support

If at any time you encounter an issue, have questions or need guidance, please contact us using the information provided in our documentation site.

If questions remain or issues arise while using PAM, please contact our Support team:

<https://support.imprivata.com/communitylogin>.

## Privileged Access Management

Privileged Access Management (PAM) is an agentless solution that provides a secured database to manage privileged accounts and secrets, establishes secure sessions for users through a standard web browser and automates the execution of jobs or tasks without disclosing or sharing access.

The purpose of this guide is to perform a new installation and first time system initialization.

At the conclusion of this guide, PAM will be ready for system configuration and use.

The target audience is system administrators with knowledge of computer administration, Active Directory and (optionally) database connectivity.

is installed to a Windows or Unix computer (physical or virtual), with optional connection to Active Directory or LDAP.

The system consists of several modules; a database that contains secrets, configuration, passwords and audit events, a service to establish, monitor and record privileged sessions, a user directory to maintain local users and groups and a job engine to execute scripts and tasks.

## Privileged Account Management

A secure AES 256-bit encrypted database that contains records which can be stored, shared and used without disclosing the actual privileged account or its secrets (passwords, certificates or keys).

## Privileged Session Management

The ability to establish a privileged session to an underlying system (Windows, Unix, Linux, Mac) through a standard web browser while providing the means to *monitor, join, record* or *terminate* this session.

## Privileged Job Management

Schedule, automate or execute on demand jobs to privileged systems without embedding the secrets in scripts or sharing them with untrusted users.

## Software Components

To accomplish the requirements above, PAM needs to install, configure and run the following software and services.

These components are deployed during the installation process (single server deployment) or they can be distributed to multiple servers (farm deployment) to scale performance.

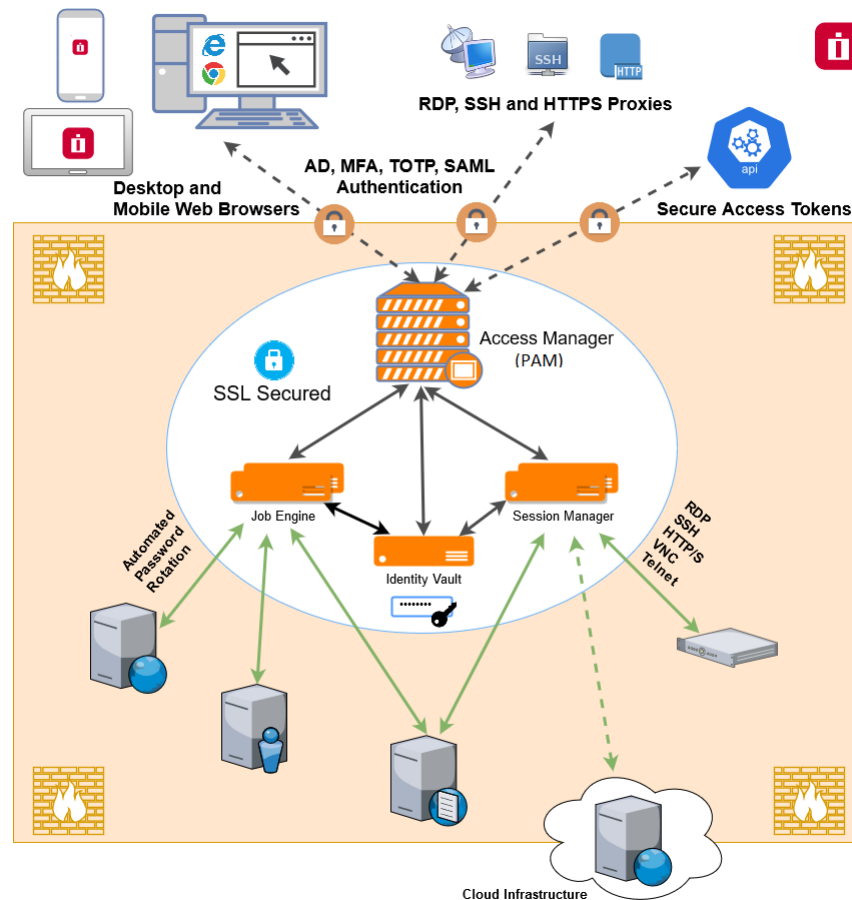
Single server deployments can be scaled to farm deployments when additional resources become needed.

## Architectural Diagram

PAM sits within the firewall in its own SSL secured network.

Client computers make requests, establish sessions and run jobs from inside or outside the firewall to computers also located inside or outside the firewall using only their native web browser of choice.

The Database of Secrets secures all records using an **AES 256-bit encrypted protocol** and only delivers these secrets to authorized remote requests.



Privileged Access Management Architectural Diagram

## Services

Depending on your installation, the following services may be deployed to Automatically startup on your computer.

Service	Function
PamDirectory	Provides the directory service to manage local users and groups in PAM.
PamManagement	Provides the service to manage the PAM system.
PamSession	Provides the service to establish, maintain, control and record privileged sessions via a user's web browser.

Table: PAM Services

## Active Directory or LDAP Integration

Integration with Active Directory or LDAP provides the ability to add Active Directory Users or Groups to PAM to manage or use the system.

PAM will use this Active Directory integration to:

- Authenticate user logins;
- Read Active Directory group membership;
- Reset Active Directory passwords.

## Planning your Installation and Deployment

The key to a successful deployment is proper planning.

Before you begin the installation process, please understand the following.

- The full scope of your user base. How many individual users will be working with PAM and of those how many will be accessing the system at the same time. This will help in planning the amount of resources and servers that are required to run the system efficiently.
- Setup a test environment. This could be a basic single server VM or a dedicated workstation, but ensure PAM is configured and running in your test environment before deploying to production. This can also act as a test bed for future software releases.
- Decide if you want to integrate with Active Directory or LDAP for users, groups and authentication or to maintain a local directory for users and groups.
- If you want to use a SSL certificate to ensure a secure connection between the client computers and PAM, then it is highly recommended to obtain and deploy the certificate prior to installation.
- Create a new user (non-root) with su or sudo privileges and a new directory (not `/tmp`) for the PAM software. Neither the root account nor the `/tmp` location should be used for installation.

## Getting Started Guidelines

Before you begin your installation of PAM, please be sure to have the following readily available.

- Your operating system (OS) of choice. Use [our recommendations](#) to determine which is best for your needs.

- Your external database connection parameters. If you are using an [external database](#) for PAM, make sure you have the database, connection string and proper credentials to provide the required connectivity.
- Your Active Directory connection parameters. If you are [integrating PAM with your Active Directory](#), make sure you have the required connection string and credentials to provide the required connectivity.
- Your enterprise's SSL certificate. If you plan on replacing our temporary self-signed certificate with your own trusted SSL certificate, make sure you have access to the certificate so that it can be imported into PAM.

## Installing Privileged Access Management

This section will work through the process of installing Privileged Access Management (PAM) to a Unix computer.

### System Requirements

The following are minimum requirements to use PAM for Single Server and medium use Production farms. Please contact us <https://support.imprivata.com/communitylogin> to discuss architecture and system recommendations for large scale farm deployments.

**NOTE: Do not install PAM using a *root* account.** This is not recommended nor best practices for installing or configuring any software in a Unix environment. The recommendation is to create a new user and give it *su* or *sudo*(or add to the sudo group) privileges to perform the installation.

	Single Server, Test or Quick Trial	Medium Use Production Farm
<b>Windows O/S (64-bit only)</b>	Windows Server 2019+ / Windows 10	Windows Server 2019+
<b>Other O/S (64-bit only)</b>	Red Hat, Ubuntu, Debian, CentOS	Red Hat, Ubuntu, Debian, CentOS
<b>Database</b>	Included*	MS SQL, MySQL, Oracle, PostgreSQL
<b>Memory (reserved for PAM use)</b>	4GB+	8GB+
<b>Disk Space (reserved for PAM use)</b>	20GB+	50GB+

Table: System Requirements

\*For Single Server, Test or Quick Trial deployments the recommendation is to use the included, internal database however you can use any of the other supported databases that are available to you.



# Software Requirements

- Web Browsers (*latest version is recommended if not specified*)
  - Windows Edge, Google Chrome, Mozilla Firefox or Apple Safari

## External Database

The default installation includes an internal database that can be deployed. If you would prefer to use an existing database in your environment, the following are supported.

Please be prepared to supply a valid connection string to your database as well as an appropriate user and password to successfully establish this connection. *Please contact your Database Administrator if you need assistance.*

NOTE: The installation process does **not create** its own database or tablespace but rather makes use of an existing one. Also, for Oracle DB you just need to create a user (you do not need to create a new data base). With that in mind, please ensure one with the name “PamDB” already exists as this will be used by the application.

- Apache Derby version 10.12.1.1+
- Microsoft SQL version 2016+ (SQL Authentication only)
- MySQL Community or Enterprise Edition version 5.7+
- Oracle version 11.2+
- PostgreSQL version 9.5+

# Installation

The following section will describe each option that is available when executing the Unix installation shell script.

Software binaries can be downloaded from <https://help.xtontech.com/content/more-information/binary-distribution-and-signatures.htm>.

To begin, run the shell script from the location where you want to install the software.

Depending on the options selected, the following configuration parameters may be available.

TIP: Rather than using the Unix /tmp folder to perform the installation, create a new folder because background processes on the host may attempt to “clean” this directory during this process. Suggested locations would be either /opt/pam or /usr/local/pam.

```
pam@demo-ipam01-01:/opt/pam$ sh XtamSetup.sh_
```

Execute Installation Shell Script

## License Agreement

Press <ENTER> to read the license agreement and enter <Q> when complete.

When prompted, accept the license agreement by entering <Y> to continue.

The license agreement must be accepted to install the software.

```
pam@demo-ipam01-01:/opt/pam$ sh XtamSetup.sh
Please confirm the application installation in the following directory (do not install into
temp directories) "/opt/pam" (Y/N) [Y]: Y
System information
Linux demo-ipam01-01 5.3.0-42-generic #34~18.04.1-Ubuntu SMP Fri Feb 28 13:42:26 UTC 2020 x
86_64 x86_64 x86_64 GNU/Linux
No LSB modules are available.
Distributor ID: Ubuntu
Description:   Ubuntu 18.04.5 LTS
Release:      18.04
Codename:     bionic
Free space detected: /dev/sda1 29G

Setup requires root user privileges, please provide your password for sudo access
Copyright (c) 2021 Imprivata, Inc.

Welcome to Imprivata Privileged Access Management Setup
Please press <ENTER> to read the software license agreement. Press Q when finished.
Downloading: EULA.txt to /opt/pam/EULA.txt
Press Y to accept the license agreement and continue or N to quit this setup (Y/N) [Y]: Pre
ss Y to accept the license agreement and continue or N to quit this setup (Y/N) [Y]: Y_
```

Read and Accept the License Agreement

## Components

Choose from the available list of components to install on this computer.

If you are looking to deploy a quick test environment, the recommendation is to accept the default options by pressing the **<Enter>** for each component.

If you would like to customize the installation, then please review the following sections to understand the purpose of each component and enter the **<N>** key to exclude a component.

Please note that while you can choose to not install some components on this computer, they may still be required for proper software operations.

For example, you may wish to install the Session Manager service on another system for performance optimization.

In this situation, you would choose to not deploy this service on your primary host and then after this initial installation is complete, you would then run this same script on your other host and only choose the Session Manager option.

Later on in the configuration of the software, you will have the ability to define which workstation is running each service.

```
Choose which components of Imprivata Privileged Access Management you want to install on this computer.

The following components are available
- Internal Database
- Directory Service for local user and groups directory and master password storage
- Application GUI to support the application's graphical user interface (GUI) and manage the system
- Job Engine for to process job execution commands and discovery operations
- Session Manager for proxying user sessions to end point computers
- Federated Sign-In for federated authentication using SSL or SSO providers

Include the Internal Database component (Y/N) [Y]: Y
Include the Directory Service component (Y/N) [Y]: Y
Include the Application GUI component (Y/N) [Y]: Y
Include the Job Engine component (Y/N) [Y]: Y
Include the Session Manager component (Y/N) [Y]: Y
Include the Federated Sign-In component (Y/N) [N]: N_
```

### Choose Components

#### Internal Database

This option will define which database to use.

When included (**<Y>**) the installation will deploy, configure and use its internal database.

If excluded (**<N>**), you will be prompted to supply an existing database in your environment to use (connection string, user and password).

Please review the requirements section for more information about [External Database](#) support.

*For single server or test environments, the recommendation is to include (**<Y>**) this option to use the included database.*

#### Directory Service

**This option will define which user store to use.**

When included (<Y>) the installation will include a local user store that can be used to create users and groups and a database to secure the master password.

When excluded (<N>) the installation will not deploy this component to the computer; however, this is a required component so it must be deployed to only one other computer and configured post installation in PAM.

To install this component on another host, simply run the script on that system and include (<Y>) this option.

*The recommendation is to include (<Y>) this option during installation.*

## Application GUI

This option will define the deployment of the PAM interface (GUI). When included (<Y>) the installation will include the manager interface (GUI) to this host computer.

When excluded (<N>) the installation will not deploy the GUI requirements to this host computer.

To install this component on another host, simply run the script on that system and include (<Y>) this option.

*The recommendation is to include (<Y>) this option during installation.*

## Job Engine

The Job Engine is required to execute background operations like discovery queries and password resets.

This option defines the deployment of a worker role to this host computer.

When included (<Y>) a Job Engine role will be deployed.

When excluded (<N>) a Job Engine role will not be deployed to this computer.

To install this component on another host, simply run the script on that system and include (<Y>) this option.

Please note that at least one job engine should be present in the farm to execute password reset, remove script execution or discovery queries.

*The recommendation is to include (<Y>) this option during installation.*

## Session Manager

The Session Manager component is required to establish, control and record privileged sessions.

This option defines the deployment of a session manager service to this host computer.

When included (<Y>) a session manager service will be deployed, configured and run from this host.

When excluded (<N>) a session manager service will not be deployed.

To install this component on another host, simply run the script on that system and include (<Y>) this option.

Review the following section if you intend to install Session Manager on a remote computer(s): [Remote Session Manager Configuration](#)

Please note that if a session manager service is not defined during installation, you will need to add one during system configuration before sessions can be established.

*The recommendation is to include (<Y>) this option during installation.*

## Federated Sign-In

This option defines the deployment of a federated sign-in component that can be used to establish user authentication.

When included (<Y>) you will need to supply your federated sign-in server connection parameters.

When excluded (<N>) a SSO server will not be configured and the default login authentication will be used.

To install this component on another host, simply run the script on that system and include (<Y>) this option.

*This is an advanced option and should only be included if necessary. For single server or test environments, the recommendation is to not include (<N>) this option.*

NOTE: The Federated Sign-In component requires the use of a properly trusted (not self-signed) SSL certificate which is used to communicate over a secure HTTPS connection. This ensures that both the client browsers and server side components trust the certificate. If you do not want to deploy and configure a trusted certificate, then do not include this component during installation.

## Component v.6.5 or 5.2

This option defines the deployment of which version of federated sign-in component should be used to establish user authentication to this host computer.

When printed (<1>) a CAS v5.2 (legacy version recommended for extending PAM deployments which are currently use v.5.2) will be deployed.

When printed (<2>) a CAS v6.5 (recommended for all new deployments) will be deployed.

```
If new deployment choose latest CAS 6.5, choose 5.2 if extending a pam deployment which is currently using CAS 5.2
Please select one of the following CAS version:
1 - CAS version 5.2 (Legacy version)
2 - CAS version 6.5 (Recommended version)
Please Enter CAS version Option [2]: 2
```

## CAS Components

## System Administrator

Enter the required parameters to create your default System Administrator login to PAM.

The account specified here may be used as the first System Administrator, so be sure to choose a memorable login (default login is “**pamadmin**”) with a strong password (maximum of 30 characters).

Both the user login and password will be displayed later when they can be saved to a file for safe keeping.

Press the **<Enter>** key after each field to continue.

```
Create system administrator by specifying login, first name, last name and password

Please enter the Administrator Login [pamadmin]: pamadmin
Please enter the Administrator First Name [System]: System
Please enter the Administrator Last Name [Administrator]: Administrator
Please enter a Password:
Please repeat Password: _
```

Create PAM System Admin Account

## SSO Connect

To define a managed path to be used with federated sign in, select (**<Y>**) the SSO option and then enter that valid path in the **Managed Path** field.

If PAM is to be used with an SSL certificate, then this option should be enabled and the managed path needs to be defined with a secure path (for example, <https://host.example.com>).

Press the **<Enter>** key to continue.

```
Do you want to access this server using SSO Service (Y/N) [N]: Y
Please Enter Managed Path []: https://host.example.com
```

Enable and Define Federation Connection (optional)

## External Database

If the Internal Database option was excluded (**<N>**) earlier, then you will now need to define your connection to your external database.

Choose your database type by entering the number to the left of its name and then press **<Enter>**.

You will then be required to enter the database host, connection and a user and password to establish a successful connection.

If further assistance is required, please contact your Database Administrator.

NOTE: The installation process does **not** create its own database or tablespace but rather makes use of an existing one. With that in mind, please ensure one with the name “PamDB” already exists as this will be used by the application.

**Example strings are listed below.**

- Remote Embedded Database [1]
  - Example connection string: db-host or db-host:port

- Microsoft SQL Server [2]
  - Example connection string: db-host or db-host:port
    - A database with the name “PamDB” must already exist and will be used for the application. Ensure the supplied account is the “owner” of this database and it is a SQL account for authentication. Active Directory accounts are not supported.
- Oracle [3]
  - Example service: db-host/db-service
  - Example instance: db-host:port:SID
    - Grant (*at a minimum*) “CONNECT, RESOURCE, UNLIMITED TABLESPACE” to the supplied user account.
- MySQL [4]
  - Example connection string: db-host or db-host:port
    - A schema with the name “pamdb” must already exist and will be used for the application. Ensure the supplied account has ALL schema privileges assigned.
- PostgreSQL [5]
  - Example connection string: db-host or db-host:port
    - A database with the name “PamDB” must already exist and will be used for the application. Ensure the supplied account is the “owner” of this database or has been provided with “ALL” privileges to it (CTC).

```
Please configure Database Connection

Please select one of the following database options:
1 - Remote Embedded Database
2 - Microsoft SQL Server
3 - Oracle
4 - MySQL
5 - PostgreSQL
Please Enter Directory Service Host [1]: 2
Please Enter DB Server []: 
```

Connect to an External Database (optional)

## Active Directory Integration

Optionally, you may choose to [integrate PAM](#) with your existing [Active Directory](#) or [LDAP server](#).

Enter your **LDAP Server FQDN**, your Active Directory or LDAP **User** (user@domain.com or domain\user), its **Password**, **Repeat the Password** and then the <Enter> key.

If the connection is successful, this user may become a System Administrator in PAM and you may continue.

If you cannot or do not want to integrate with Active Directory or LDAP, simply enter <N> at the prompt and <Enter> to continue with the setup.

```
Do you want to configure access to Microsoft Active Directory or LDAP (Y/N) [N]: Y
Please enter LDAP Server []: ad.example.com
Please enter User []: user@domain.com
Please enter a Password:
Please repeat Password:
Connecting to AD... Ok
Successfully configured connection to your Microsoft Active Directory or LDAP Server: ad.example.com
```

### Active Directory or LDAP Server Integration

## Installation Complete

When the installation is complete and all services are started, the following summary will appear.

The summary will display the services, accounts and passwords that were created during installation.

It is **extremely** important that the example information highlighted in the yellow box below be saved to a file and kept in a safe location.

The [Master Password](#) displayed will be required in a “[break glass](#)” or [database transfer scenario](#) and no one will be able to identify nor update this password if it is ever lost.

```
Generating Session Manager certificate... Ok
Archive: /opt/pam/certbundle.zip
  inflating: session.crt
  inflating: session.key
Creating environment file
Fontconfig warning: "/etc/fonts/conf.avail/53-monospace-lcd-filter.conf", line 10: Having multiple values in <test> isn't supported and may not work as expected
Import session manager certificate from ADS... Ok
Successfully imported session manager certificate from ADS
Ok
Installing service: pamsession
Created symlink /etc/systemd/system/multi-user.target.wants/pamsession.service → /etc/systemd/system/pamsession.service.
Starting service: pamsession
Installing service: pammanager
Created symlink /etc/systemd/system/multi-user.target.wants/pammanager.service → /etc/systemd/system/pammanager.service.
Starting service: pammanager
Waiting for Web services to start.....done
Imprivata Privileged Access Management installation had been successfully completed.
Below is the information about the system to remember. It is important to save this information to a file and store it in a safe location.

System Admin: pamadmin/root-mouse-home
Master Password: Ok: yCJNbPwvFcyDni5QOE9MqzpmuU90imwQ
DB Password: Ok: I99JunukpaCkSa
Directory Admin Password: Ok: kQDLaVNBciI06t
Copy certificate bundle file /opt/pam/certbundle.zip to the Session Manager components.
pam@demo-ipam01-01:/opt/pam$
```

Summary Screen with Passwords (save this information to a file for safe keeping)

If you do not see these passwords or receive any errors in this Summary screen the installation was not successful.

Complete the installation and then uninstall to try again.



Do not initialize PAM without a successful deployment and a safe and secure copy of the logins and passwords shown in the example Summary screen.

Privileged Access Management is now installed and ready for initialization. You can now exit the installation session and login to PAM at <https://localhost:6443/xtam/>.

NOTE: It is extremely important that all the passwords displayed in this section are saved to a file and this file is stored in a safe location. These passwords cannot be retrieved by development team or anyone else once the installation is complete.

## Linux deployment of HA and DR nodes

The option to Linux installation script to deploy the new system with the provided master password instead of generated one to simplify deployment of High Availability or recovery nodes.

This simplifies deployment of additional or disaster recovery nodes based on the main node master key to decrypt system data.

Previously the option was available in a post-installation script replacing system master password with a new one.

To activate the feature use **-mp MASTER-PASSWORD** option in Linux installation script replacing **MASTER-PASSWORD** place-holder with the master password of the main node.

## PAM Centralized Deployment Manager

The PAM Centralized Deployment Manager (CDM) is an Ansible-based toolset to help automate PAM deployment and configuration tasks.

## Supported Scope of Operations

Tasks that the PAM Centralized Deployment Manager can perform:

<b>Deploy PAM Master Nodes</b>	A PAM master node is a PAM node with the Management Console service installed. The PAM CDM supports both <i>single-master</i> and <i>multi-master</i> PAM farms. All PAM master nodes deployed with the PAM CDM will also have the Session Manager and Job Engine services installed.
<b>Deploy PAM Remote Nodes</b>	A PAM remote node is a PAM node with the Session Manager and/or Job Engine services installed, but <u>not the Management Console service</u> . The PAM CDM <b>supports any number of remote nodes</b> in a PAM farm.
<b>Deploy PostgreSQL Database</b>	Can install PostgreSQL database and configure it for use with the PAM farm being deployed. PAM CDM also supports external database integration which is the recommended configuration for production PAM farms.

<b>Deploy Apache Load Balancer</b>	Can install Apache web server and configure it as a load balancer for the PAM farm being deployed. PAM CDM also supports integration with an external load balancer which is the recommended configuration for production PAM farms.
<b>Add Nodes to an Existing PAM Farm</b>	With some restrictions, PAM CDM can deploy new PAM master and/or remote nodes and integrate them into a PAM farm that was previously deployed with the PAM CDM.
<b>Update PAM Components</b>	Includes tools to help update the PAM framework, web, or session components on existing PAM installations. This is currently considered an experimental feature.

## System Requirements

The PAM CDM operates on a set of hosts, which are typically VMs but could be physical servers. The required VM count depends on the complexity of the PAM farm.

The basic requirement is that PAM CDM must be able to connect to the VM over SSH with a user that has sudo privileges.

**NOTE: Do not install PAM using a `root` account.** This is not recommended nor best practices for installing or configuring any software in a Unix environment. The recommendation is to create a new user and give it `su` or `sudo` (or add to the sudo group) privileges to perform the installation of PAM Centralized Deployment Manager (CDM).

## Operating System Requirements

	<b>Single Ansible controller VM, Test or Quick Trial *minimum</b>	<b>Medium Use Deployment Production Farm *recommended</b>
<b>Unix O/S (64-bit only)</b>	Ubuntu 22.04, Alma 9	Ubuntu 22.04, Alma 9
<b>Database</b>	CDM-Managed PostgreSQL or External PostgreSQL, MSSQL, MySQL, or Oracle	CDM-Managed PostgreSQL or External PostgreSQL, MSSQL, MySQL, or Oracle
<b>VM size</b>	2 VCPUs	4 VCPUs
<b>Memory (reserved for use)</b>	8 GB+	16 GB+
<b>Disk Space (reserved for use)</b>	40 GB+	80 GB+
<b>Ports in use</b>	Ports 6443, 5432 are allowed. Follow <a href="#">PAM Ports</a> for details.	Ports 6443, 5432 are allowed. Follow <a href="#">PAM Ports</a> for details.

*Windows installation for PAM using the CDM tool is not supported.*

Detailed Host VM requirements are available in the PAM CDM documentation [package](#).

Please contact us <https://support.imprivata.com/communitylogin> to discuss the architecture and system recommendations for large scale farm deployments.

## Getting Started

Follow the documentation to get started with your PAM Centralized Deployment Manager deployment:

PAM CDM documentation: <https://bin.xtontech.com/cdm/README.html>

PAM CDM package: <https://bin.xtontech.com/cdm/pam-cdm.tgz>

PAM CDM checksum: <https://bin.xtontech.com/cdm/pam-cdm.tgz.sha256>

Please contact us <https://support.imprivata.com/communitylogin> if you have any question about the PAM Centralized Deployment Manager (CDM).

## Logging into Privileged Access Management

Open your web browser and navigate to the login screen of PAM or double click the shortcut on your desktop.

- Non-secured login: <http://localhost:8080/xtam>
- Secured login: <https://localhost:6443/xtam>

At the login prompt, you can sign in with one of the following system administrator logins:

- The [System Administrator](#) account that was created during the installation process.
- The [Active Directory or LDAP account](#) that was (optionally) used to establish integration during the installation process.

Enter the System Admin user and password and click the **Login** button.

Upon successful login, you will be directed to the initialization page of PAM.

The account used as the first login will become a System Administrator.

## Browser SSL Certificate

A default installation of PAM comes with a pre-created PAM Self-signed SSL certificate to encrypt traffic.

Because this SSL certificate is self-signed and therefore not trusted by your browser or certificate authority, a security warning will appear when the login page opens.

1. You may use the non-secured login at this location: <http://localhost:8080/xtam> to avoid the browser warning and continue using the software without encrypting your traffic.
2. You may accept the warning, install the certificate and use it as supplied. Although it is self-signed, it will still encrypt the traffic.
3. You may substitute our non-trusted, self-signed certificate with your own trusted, signed certificate by following the procedure described in this [article](#).

It is safe to accept the security warning for this self-signed certificate only; however, you may consider these options:

While our self-signed SSL certificate is acceptable for trial or PoC deployments, they should not be used for any production deployments. We **strongly** recommend the use of a well-known trusted SSL certificate or one generated by your own Certificate Authority.

## Initialize

The first login (and only the first) after a new installation will require a system initialization.

When logged in for the first time, click the Initialize button to begin this process.

During this time, the system will create all its needed configuration in the database and services.

Depending on the complexity of your configuration, this process may take anywhere from a few seconds to 1-2 minutes to finish.

### This is the application initialization page

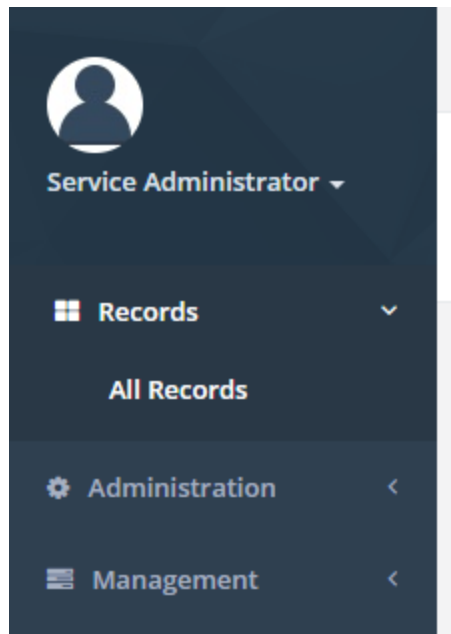
Clicking the button below will initialize the application database with the initial data. Currently logged in user Service Administrator will become the application administrator.

Initialize

#### PAM “first-time” Initialization

When the initialization is complete, the system will redirect you to the landing page.

You should see a few menu headings on the left side including Records, Administration and Management indicating that the process is complete.



PAM Initialization Complete

# License Registration

If you have a license key, then you should activate it now.

1. Navigate to Administration > Settings > Registration.
2. On the registration screen, copy and paste your key into the “Activation Code” field and then click **Automatic Registration**.
3. When the license is retrieved successfully (status should display “License is Valid”), click the **Save License** button to finalize.
4. The software is now activated and ready for use.

The screenshot shows the 'PAM License Activation' interface. At the top right, there are three buttons: 'Save License', 'Automatic Registration', and 'Manual Registration'. Below these, the 'Status' is displayed as 'License is Valid'. The 'Activation code' field contains 'c810'. The 'License' field contains a multi-line text block: '-----LICENSE BEGIN-----', 'Activation:c810', 'Product:PAM', 'HUB:XtonTech', and 'Client:ckd'. A vertical scrollbar is visible on the right side of the license text area.

PAM License Activation

## Manual Registration

If the computer is not connected to the internet or cannot establish a connection to the license server for registration, then the following procedure will register the software manually.

1. Click the **Manual Registration** button. A new browser window will appear.
2. Copy or transfer this URL to a computer with an internet connection and load the page.
3. Select the copy the license information between and including the LICENSE BEGIN header and LICENSE END footer.
4. Save this information to a file or paste it directly into the “License” field in PAM.
5. Click the **Save License** button.
6. The license status will read “**License is Valid**” and the software is now registered.

# Uninstalling Privileged Access Management

You can uninstall PAM by simply running the uninstall shell script located in its installation directory.

## Uninstaller

First, logout and close any open Sessions in PAM as well as any open sessions in your Web Browser.

Execute the uninstall script and follow the prompts.

When the script completes, the software and its services will be removed from your computer.

NOTE: The uninstall script is `./uninstall.sh` and should be executed from the `$PAM_HOME` directory.

If you deployed additional services to other servers, then you will need to run the uninstall script on each of these computers to remove the components.

## Database Cleanup

If you have configured PAM with the use of an external database, then you will need to manually remove these database objects.

Please contact your database administrator for assistance.

## Appendix

### Remote Session Manager Configuration

When installing the Session Manager component on a remote Unix or Linux computer(s), then the following steps should be taken.

1. Ensure that PAM is Installed and configured on your master computer.
2. Run the install script on the remote computer where Session Manager is to be deployed.
3. Read and accept the License Agreement by pressing **<ENTER>** to display the agreement, **<Q>** when finished and finally **<Y>** to accept it and continue.
4. Enter **<N>** to exclude each component except for the "Session Manager component" which you will include **<Y>**.

```
Include the Internal Database component (Y/N) [Y]: Y
Include the Directory Service component (Y/N) [Y]: Y
Include the Application GUI component (Y/N) [Y]: Y
Include the Job Engine component (Y/N) [Y]: Y
Include the Session Manager component (Y/N) [Y]: Y
Include the Federated Sign-In component (Y/N) [N]: N
Downloading components...
```

Select the "Session Manager" component

5. Next, enter the location of the certificate bundle that was deployed to your master computer where PAM was installed earlier and press **<ENTER>** to continue.

```
Configuring components...
Provide certificate bundle location: /opt/pam/certbundle.zip
```

Enter the Certificate Bundle file location

1. The certificate bundle is in the root PAM installation directory on your master computer. The default file location is `/certbundle.zip`
2. You may select the zip file from this default location (if possible), copy it to a shared network location or simply copy the zip file to this remote computer and select it locally.

NOTE: This step is optional, so if you wish to not supply the certificate you may simply click **Next** to continue. By skipping this option, you are acknowledging that the communication between PAM on the master computer and this remote Session Manager computer will not be secured. Because of this, it is recommended that you supply the certificate when prompted and do not skip this step.

6. The Session Manager service will now startup on this computer and the installation script will finalize the operation.

```
Configuring components...
Provide certificate bundle location: /opt/pam/certbundle.zip
Archive: /opt/pam/certbundle.zip
  inflating: session.crt
  inflating: session.key
Creating environment file
Below is the information about the system to remember. It is important to save
this information to a file and store it in a safe location.

pam@demo-ipam01-01:/opt/pam$
```

Session Manager Component Deployed

## Web Server

If you are configuring PAM using a trusted SSL certificate or exposing it to external traffic, then a web server will need to be deployed and configured.

The PAM installation process does not include web server deployment and configuration and therefore should be performed by a knowledgeable Unix administration.

Popular web servers include Apache HTTP or NGINX.

The purpose of the web server is to act as a reverse proxy.

Its forwarding rules should process the certificate secured HTTPS 443 inbound port and route it to the PAM port (default 8080) inside the server.

Since the trusted SSL certificate is applied to a specific domain (i.e. <https://host.example.com>) this URL becomes the managed path for PAM's Federated Sign-In server.

## Windows Installation Guide

### Introduction

This guide is designed to show system administrators how to install, initialize and run Privileged Access Management (PAM) on a Windows host.

### Technical Support

If at any time you encounter an issue, have questions or need guidance, please contact us using the information provided in our documentation site.

If questions remain or issues arise while using PAM, please contact our Support team:

<https://support.imprivata.com/communitylogin>.



# Privileged Access Management

Privileged Access Management (PAM) is an agentless solution that provides a secured database to manage privileged accounts and secrets, establishes secure sessions for users through a standard web browser and automates the execution of jobs or tasks without disclosing or sharing access.

The purpose of this guide is to perform a new installation and first time system initialization.

At the conclusion of this guide, PAM will be ready for system configuration and use.

The target audience is system administrators with knowledge of computer administration, [Active Directory](#) and (optionally) database connectivity.

PAM is installed to a Windows or Unix computer (physical or virtual), with optional connection to Active Directory or LDAP.

The system consists of several modules; a database that contains secrets, configuration, passwords and audit events, a service to establish, monitor and record privileged sessions, a user directory to maintain local users and groups and a job engine to execute scripts and tasks.

## Privileged Account Management

A secure AES 256-bit encrypted database that contains records which can be stored, shared and used without disclosing the actual privileged account or its secrets (passwords, certificates or keys).

## Privileged Session Management

The ability to establish a privileged session to an underlying system (Windows, Unix, Linux, Mac) through a standard web browser while providing the means to monitor, join, record or terminate this session.

## Privileged Job Management

Schedule, automate or execute on demand jobs to privileged systems without embedding the secrets in scripts or sharing them with untrusted users.

## Software Components

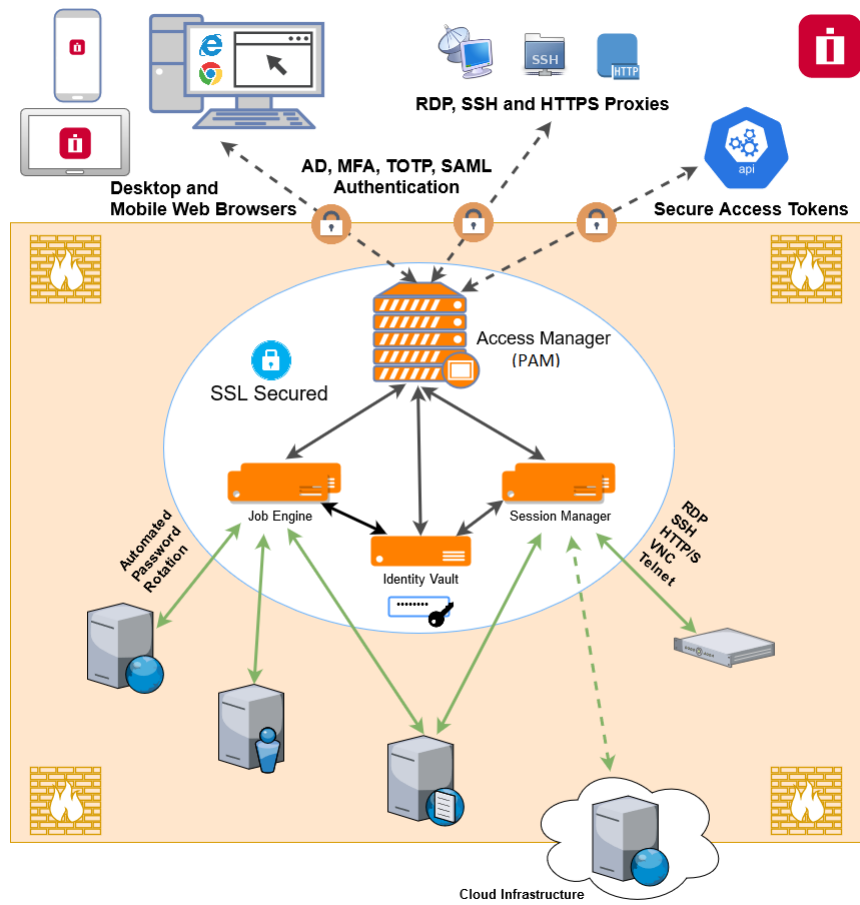
To accomplish the requirements above, PAM needs to install, configure and run the following software and services. These components are deployed during the installation process (single server deployment) or they can be distributed to multiple servers (farm deployment) to scale performance. Single server deployments can be scaled to farm deployments when additional resources become needed.

### *Architectural Diagram*

PAM sits within the firewall in its own SSL secured network.

Client computers make requests, establish sessions and run jobs from inside or outside the firewall to computers also located inside or outside the firewall using only their native web browser of choice.

The Database of Secrets secures all records using an AES 256-bit encrypted protocol and only delivers these secrets to authorized remote requests.



Privileged Access Management Architectural Diagram

## Services

Depending on your installation, the following services may be deployed to Automatically startup on your computer.

Service	Function
PamDirectory	Provides the directory service to manage local users and groups in PAM.
PamManagement	Provides the service to manage the PAM system.
PamSession	Provides the service to establish, maintain, control and record privileged sessions via a user's web browser.

Table: PAM Services

## Active Directory or LDAP Integration

Integration with Active Directory or LDAP provides the ability to add Active Directory Users or Groups to PAM to manage or use the system.

PAM will use this Active Directory integration to:

- Authenticate user logins;
- Read Active Directory group membership;
- Reset Active Directory passwords.

## Planning your Installation and Deployment

The key to a successful deployment is proper planning. Before you begin the installation process, please understand the following.

- The full scope of your user base. How many individual users will be working with PAM and of those how many will be accessing the system at the same time. This will help in planning the amount of resources and servers that are required to run the system efficiently.
- Setup a test environment. This could be a basic single server VM or a dedicated workstation, but ensure PAM is configured and running in your test environment before deploying to production. This can also act as a test bed for future software releases.
- Decide if you want to integrate with Active Directory or LDAP for users, groups and authentication or to maintain a local directory for users and groups.
- If you want to use a SSL certificate to ensure a secure connection between the client computers and PAM, then it is highly recommended to obtain and deploy the certificate prior to installation.

## Getting Started Guidelines

Before you begin your installation of PAM, please be sure to have the following readily available.

- Your operating system (OS) of choice. Use [our recommendations](#) to determine which is best for your needs.
- Your external database connection parameters. If you are using an [external database](#) for PAM, make sure you have the database, connection string and proper credentials to provide the required connectivity.

- Your Active Directory connection parameters. If you are [integrating PAM with your Active Directory](#), make sure you have the required connection string and credentials to provide the required connectivity.
- Your enterprise's SSL certificate. If you plan on replacing our temporary self-signed certificate with your own trusted SSL certificate, make sure you have access to the certificate so that it can be imported into PAM.

## Installing Privileged Access Management

This section will work through the process of installing Privileged Access Management (PAM) to a Windows computer.

### System Requirements

The following are minimum requirements to use PAM for Single Server and medium use Production farms.

Please contact us <https://support.imprivata.com/communitylogin> to discuss architecture and system recommendations for large scale farm deployments.

	Single Server, Test or Quick Trial	Medium Use Production Farm
<b>Windows O/S (64-bit only)</b>	Windows Server 2019+ / Windows 10	Windows Server 2019+
<b>Other O/S (64-bit only)</b>	Red Hat, Ubuntu, Debian, CentOS	Red Hat, Ubuntu, Debian, CentOS
<b>Database</b>	Included*	MS SQL, MySQL, Oracle, PostgreSQL
<b>Memory (reserved for PAM use)</b>	4GB+	8GB+
<b>Disk Space (reserved for PAM use)</b>	20GB+	50GB+

Table: System Requirements

\*For Single Server, Test or Quick Trial deployments the recommendation is to use the included, internal database however you can use any of the other supported databases that are available to you.

### Software Requirements

- Web Browsers (*latest version is recommended if not specified*)
  - Windows Edge, Google Chrome, Mozilla Firefox or Apple Safari

### External Database

*The default installation includes an internal database that can be deployed. If you would prefer to use an existing database in your environment, the following are supported. Please be prepared to supply a valid connection string to your database as well as an appropriate user and password to successfully establish this connection. Please contact your Database Administrator if you need assistance.*

NOTE: The installation process does **not** create its own database or tablespace but rather makes use of an existing one. Also, for Oracle DB you just need to create a user (you do not need to create a new data base). With that in mind, please ensure one with the name “PamDB” already exists as this will be used by the application.

- Apache Derby version 10.12.1.1+
- Microsoft SQL version 2016+ (SQL Authentication only)
- MySQL Community or Enterprise Edition version 5.7+
- Oracle version 11.2+
- PostgreSQL version 9.5+

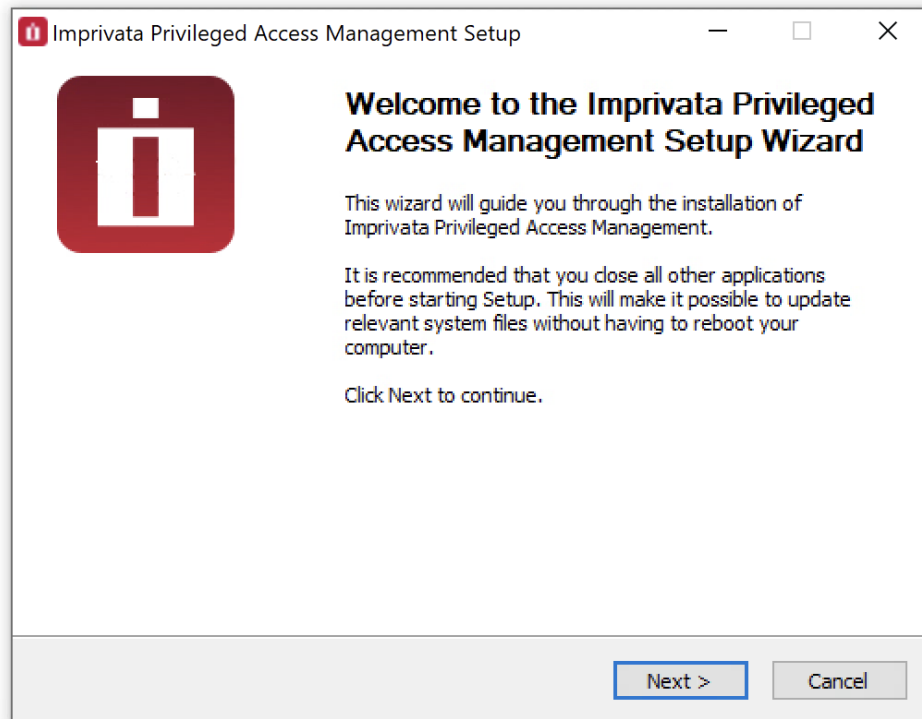
# Installation

The following section will describe each option that is available in the installation wizard.

Software binaries can be downloaded from <https://help.xtontech.com/content/more-information/binary-distribution-and-signatures.htm>.

To begin, run the setup file from your computer and follow through the wizard.

Depending on the options selected, the following configuration parameters may be available.

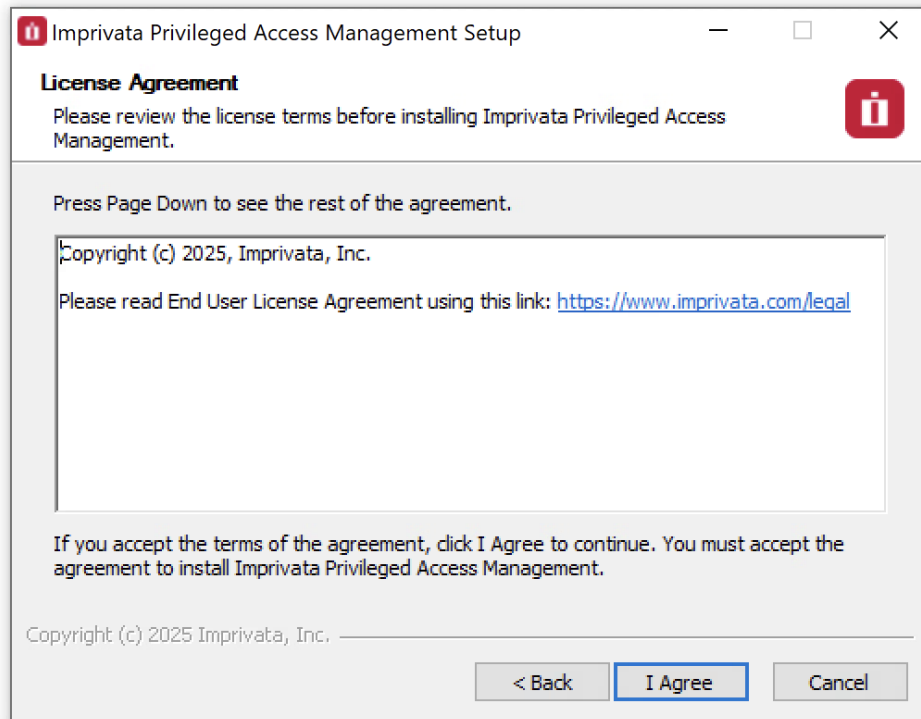


Setup Welcome Page

## License Agreement

Read and accept the license agreement by clicking the **I Agree** button to proceed.

The license agreement must be accepted to install the software.



### Read and Accept the License Agreement

## Components

Choose from the available list of components to install on this computer. If you are looking to deploy a quick test environment, the recommendation is to leave the default options and simply click **Next** to continue.

If you would like to customize the installation, then please review the following sections to understand the purpose of each component.

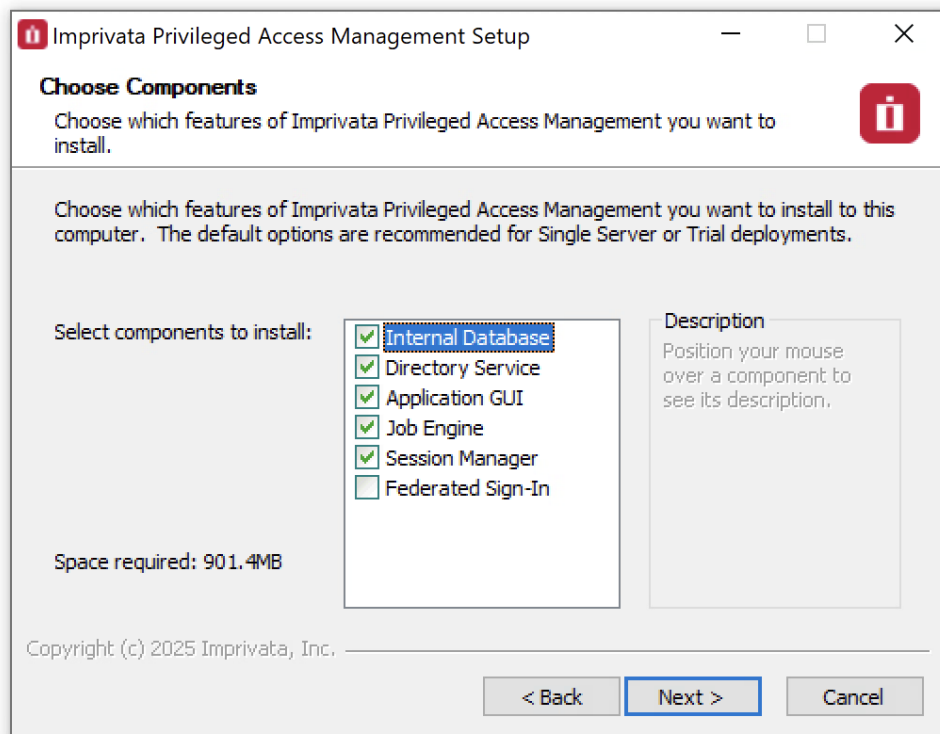
When you are finishing customizing your component selection, click **Next** to continue.

Please note that while you can choose to not install some components on this system, they may still be required for proper software operations.

For example, you may wish to install the Session Manager service on another system for performance optimization.

In this situation, you would choose to not deploy this service on your primary host and then after this initial installation is complete, you would then run this same installer on your other host and only choose the **Session Manager** option.

Later on in the configuration of the software, you will have the ability to define which workstation is running each service.



Choose Components

### Internal Database

This option will define which database to use.

When enabled (checked) the installation will deploy, configure and use its internal database.



If disabled (unchecked), you will be prompted to supply an existing database in your environment to use (connection string, user and password).

Please review the requirements section for more information about [External Database](#) support.

*For single server or test environments, the recommendation is to enable (check) this option to use the included database.*

## Directory Service

This option will define which user store to use.

When enabled (checked) the installation will include a local user store that can be used to create users and groups and a database to secure the master password.

When disabled (unchecked) the installation will not deploy this component to the computer; however, this is a required component so it must be deployed to only one other computer and configured post installation in PAM.

To install this component on another host, simply run the installer on that system and enable (check) this option.

*The recommendation is to include this option during installation.*

## Application GUI

This option will define the deployment of the PAM interface (GUI).

When enabled (checked) the installation will include the manager interface (GUI) to this host computer.

When disabled (unchecked) the installation will not deploy the GUI requirements to this host computer.

To install this component on another host, simply run the installer on that system and enable (check) this option.

*The recommendation is to include this option during installation.*

## Job Engine

The Job Engine is required to execute background operations like discovery queries and password resets.

This option defines the deployment of a worker role to this host computer.

When enabled (checked) a Job Engine role will be deployed. When disabled (unchecked) a Job Engine role will not be deployed to this computer.

To install this component on another host, simply run the installer on that system and enable (check) this option.

Please note that at least one job engine should be present in the farm to execute password reset, remove script execution or discovery queries.

*The recommendation is to include this option during installation.*

## Session Manager

The Session Manager component is required to establish, control and record privileged sessions.

This option defines the deployment of a session manager service to this host computer.

When enabled (checked) a session manager service will be deployed, configured and run from this host. When disabled (unchecked) a session manager service will not be deployed.

To install this component on another host, simply run the installer on that system and enable (check) this option.

Review the following section if you intend to install Session Manager on a remote computer(s): [Remote Session Manager Configuration](#)

Please note that if a session manager service is not defined during installation, you will need to add one during system configuration before sessions can be established.

*The recommendation is to include this option during installation.*

## Federated Sign-In

This option defines the deployment of a federated sign-in component that can be used to establish user authentication.

When enabled (checked) you will need to supply your federated sign-in server connection parameters.

When disabled (unchecked) a SSO server will not be configured and the default login authentication will be used.

To install this component on another host, simply run the installer on that system and enable (check) this option.

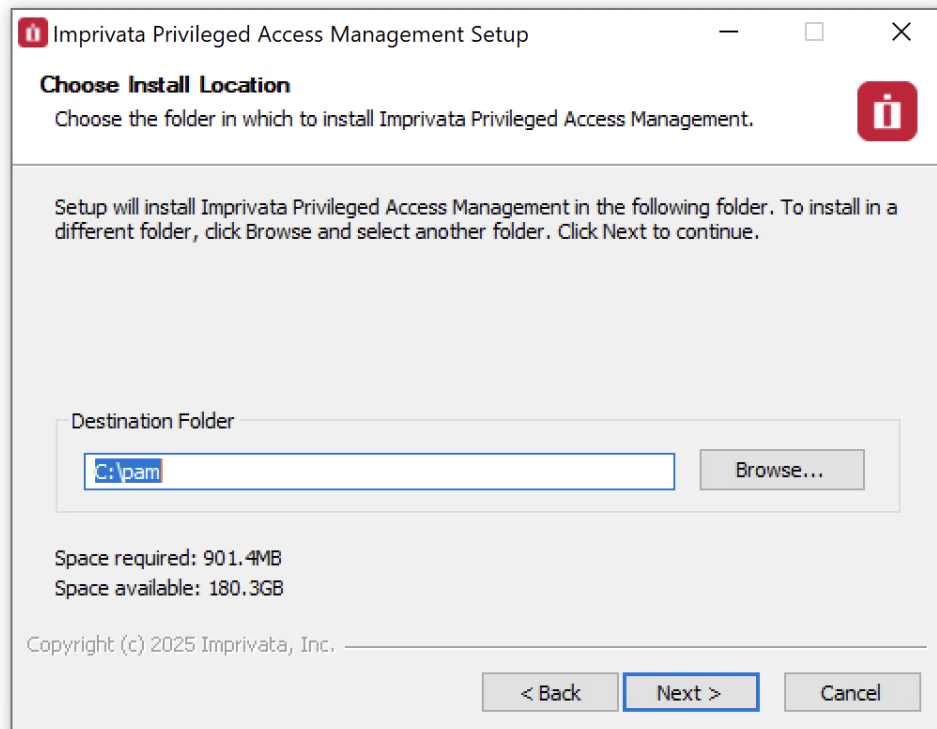
*This is an advanced option and should only be included if necessary. For single server or test environments, the recommendation is to not include this option.*

NOTE: The Federated Sign-In component requires the use of a properly trusted (not self-signed) SSL certificate which is used to communicate over a secure HTTPS connection. This ensures that both the client browsers and server side components trust the certificate. If you do not want to deploy and configure a trusted certificate, then do not include this component during installation.

## Installation Location

Enter or select the location where the PAM software will be downloaded and installed.

Click **Next** to continue.



Choose Installation Location

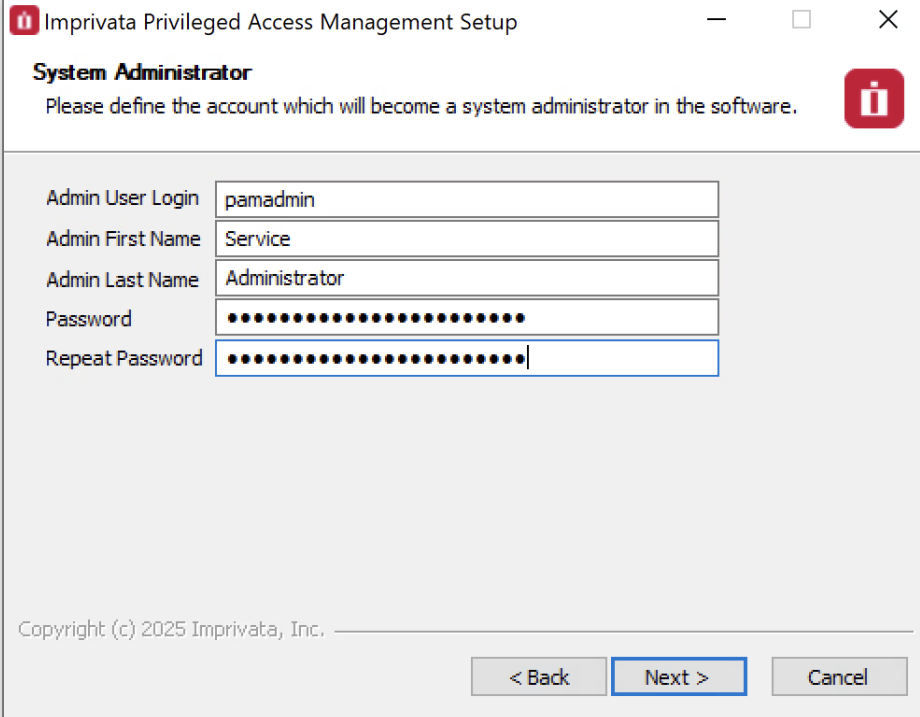
## System Administrator

Enter the required parameters to create your default System Administrator login to PAM.

The account specified here may be used as the first System Administrator, so be sure to choose a memorable login (default login is “**pamadmin**”) with a strong password (maximum of 30 characters).

Both the user login and password will be displayed later when they can be saved to a file for safe keeping.

Click **Next** to continue.



Imprivata Privileged Access Management Setup

**System Administrator**  
Please define the account which will become a system administrator in the software.

Admin User Login: pamadmin

Admin First Name: Service

Admin Last Name: Administrator

Password: .....

Repeat Password: .....

Copyright (c) 2025 Imprivata, Inc.

< Back   Next >   Cancel

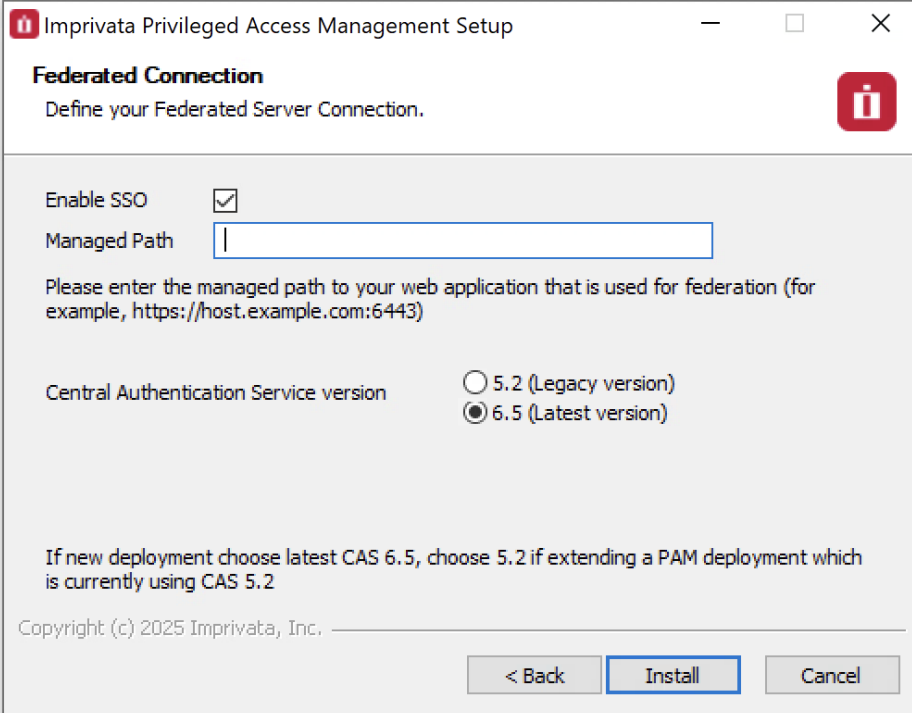
Create PAM System Admin Account

## SSO Connect

To define a managed path to be used with federated sign in, enable (check) the **Enable SSO** box and then enter that valid path in the **Managed Path** field.

If PAM is to be used with an SSL certificate, then this option should be enabled and the managed path needs to be defined with a secure path (for example, <https://host.example.com>).

Click **Next** to continue.



The image shows a Windows-style dialog box titled "Imprivata Privileged Access Management Setup". The main heading is "Federated Connection" with a subtitle "Define your Federated Server Connection." Below this, there is a section for "Enable SSO" with a checked checkbox. Next to it is a text input field for "Managed Path". A note below the input field says: "Please enter the managed path to your web application that is used for federation (for example, <https://host.example.com:6443>)". Below this, there are two radio buttons for "Central Authentication Service version": "5.2 (Legacy version)" and "6.5 (Latest version)", with the latter being selected. At the bottom, there is a copyright notice "Copyright (c) 2025 Imprivata, Inc." and three buttons: "< Back", "Install" (highlighted with a blue border), and "Cancel".

Imprivata Privileged Access Management Setup

**Federated Connection**  
Define your Federated Server Connection.

Enable SSO ☒

Managed Path

Please enter the managed path to your web application that is used for federation (for example, <https://host.example.com:6443>)

Central Authentication Service version

☐ 5.2 (Legacy version)  
☒ 6.5 (Latest version)

If new deployment choose latest CAS 6.5, choose 5.2 if extending a PAM deployment which is currently using CAS 5.2

Copyright (c) 2025 Imprivata, Inc.

< Back Install Cancel

Enable and Define Federated Connection (optional)

## External Database

If the Database option was left disabled (unchecked) earlier, then you will now need to define your connection to your external database.

Select your **Database** type and then enter the required parameters to establish a successful connection.

If further assistance is required, please contact your Database Administrator.

Click **Next** to continue.

NOTE: The installation process does **not** create its own database or tablespace but rather makes use of an existing one. With that in mind, please ensure one with the name "PamDB" already exists as this will be used by the application.

Example strings are listed below.

### • Apache Derby

- Example connection string: db-host or db-host:port

### • Microsoft SQL Server

- Example connection string: db-host or db-host:port
  - A database with the name "PamDB" must already exist and will be used for the application. Ensure the supplied account is the "owner" of this database and it is a SQL account for authentication. Active Directory accounts are not supported.

### • MySQL


- Example connection string: db-host or db-host:port
  - A schema with the name "pamdb" must already exist and will be used for the application. Ensure the supplied account has ALL schema privileges assigned.

### • Oracle

- Example service: db-host/db-service
- Example instance: db-host:port:SID
  - Grant (*at a minimum*) "CONNECT, RESOURCE, UNLIMITED TABLESPACE" to the supplied user account.


### • PostgreSQL

- Example connection string: db-host or db-host:port
  - A database with the name "PamDB" must already exist and will be used for the application. Ensure the supplied account is the "owner" of this database or has been provided with "ALL" privileges to it (CTC).

 **Imprivata Privileged Access Management Setup** — □ ×

**External Database**

Define your connection parameters to the external database.



Database	Derby
DB Server[:Port]	Derby
User	MS SQL Server
Password	MySQL
	Oracle
	PostgreSQL

Connect

Copyright (c) 2024 Imprivata, Inc.

< Back   Next >   Cancel

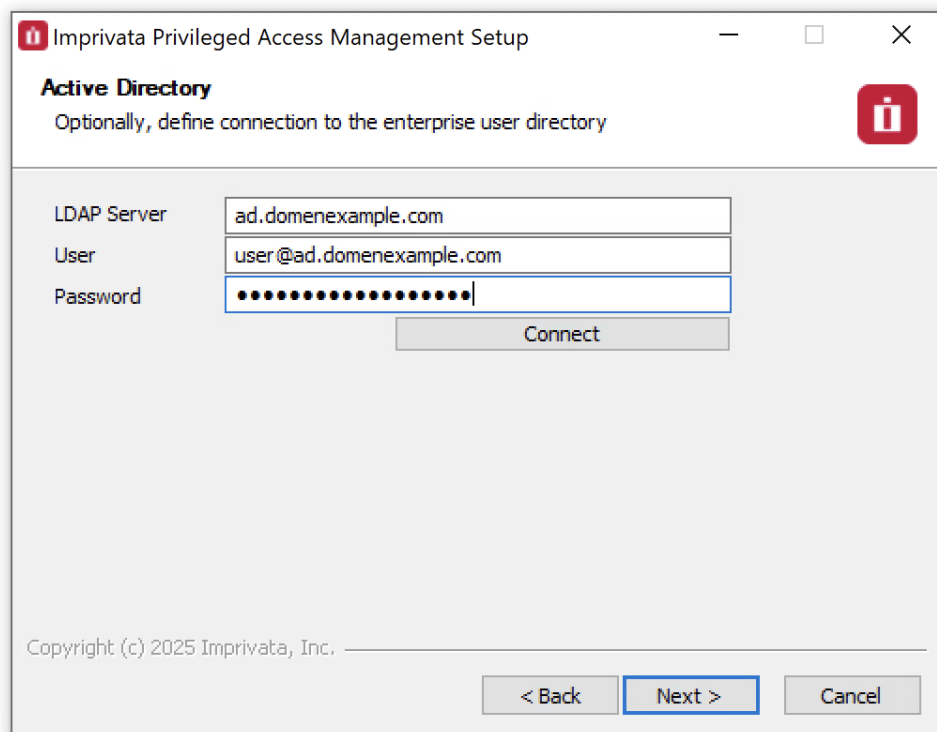
Connect to an External Database (optional)

## Active Directory Integration

Optionally, you may choose to integrate PAM with your existing Active Directory or LDAP server. Enter your **LDAP Server** FQDN, your Active Directory or LDAP **User** (*user@domain.com* or *domain\user*), its **Password** and then click **Connect**.

If the connection is successful, this user may become a System Administrator in PAM and you may continue. If you cannot or do not want to integrate with Active Directory or LDAP, you may leave these parameters empty.

Click **Next** to continue.



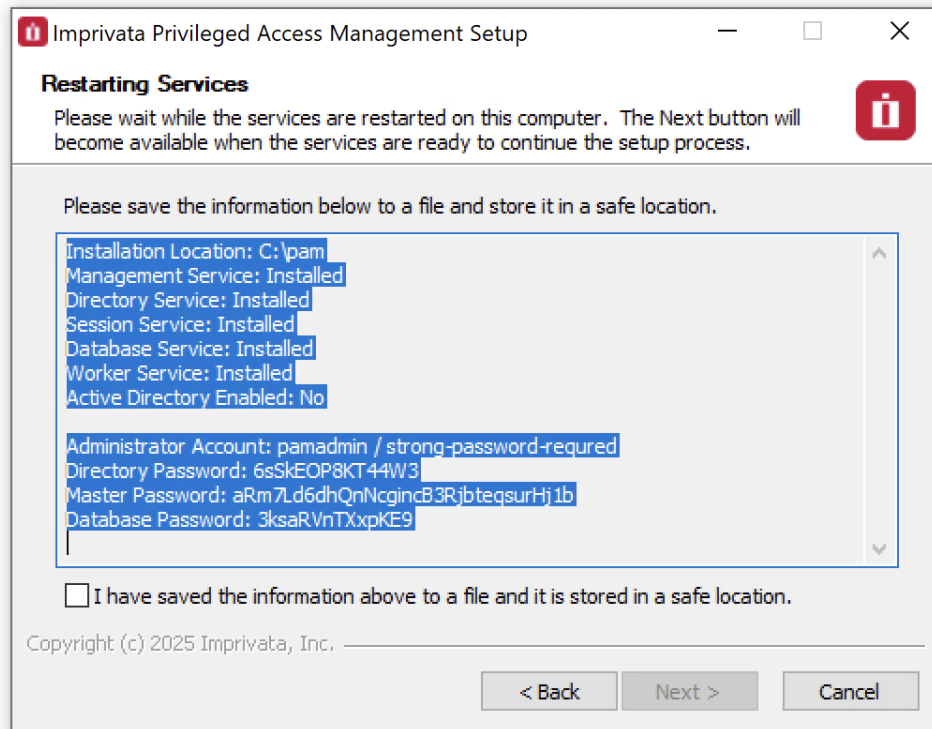
The screenshot shows a Windows-style window titled "Imprivata Privileged Access Management Setup". The window has a red icon in the top-left corner and standard window controls (minimize, maximize, close) in the top-right. The main content area is titled "Active Directory" in bold, with a subtitle "Optionally, define connection to the enterprise user directory". Below this, there are three input fields: "LDAP Server" with the value "ad.domenexample.com", "User" with the value "user@ad.domenexample.com", and "Password" with a masked password represented by dots. A "Connect" button is positioned below the password field. At the bottom of the window, there is a copyright notice "Copyright (c) 2025 Imprivata, Inc." and three navigation buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

Active Directory or LDAP Server Integration



## Summary

The summary screen will display all the services, accounts and password that were created during installation. It is **extremely** important that all this information be saved to a file and kept in a safe location. The [Master Password](#) displayed will be required in a [“break glass”](#) or database transfer scenario and no one will be able to identify nor update this password if it is ever lost.



Summary Screen with Passwords (save this information to a file for safe keeping)

If you do not see these passwords or receive any errors in this Summary screen the installation was not successful.

Complete the installation and then uninstall to try again.

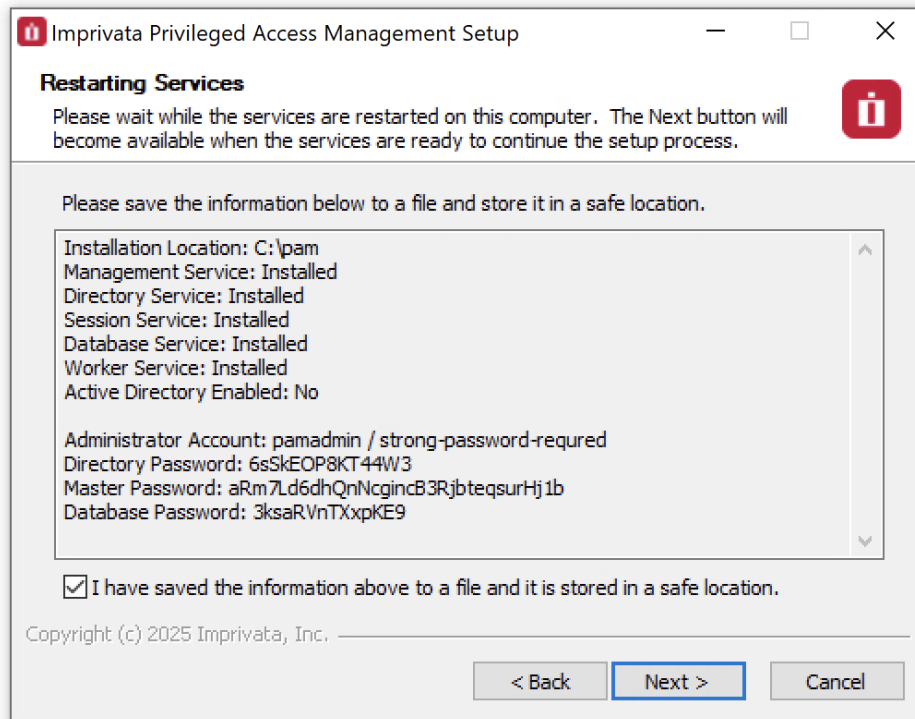
Do not initialize Privileged Access Management without a successful deployment and a safe and secure copy of the logins and passwords shown in the example Summary screen.

The **Next** button will be disabled until all the services have been started and are available on this computer.

This process may take a few minutes to complete.

When the services are ready, check the box to confirm that your passwords have been saved to a file in a safe location and then the **Next** button will become available.

Click **Next** to continue.



### Summary Screen with Confirmation

**NOTE:** It is extremely important that all the passwords displayed in this section are saved to a file and this file is stored in a safe location. These passwords cannot be retrieved by software developers or anyone else once the installation is complete.

## Completing the Installation

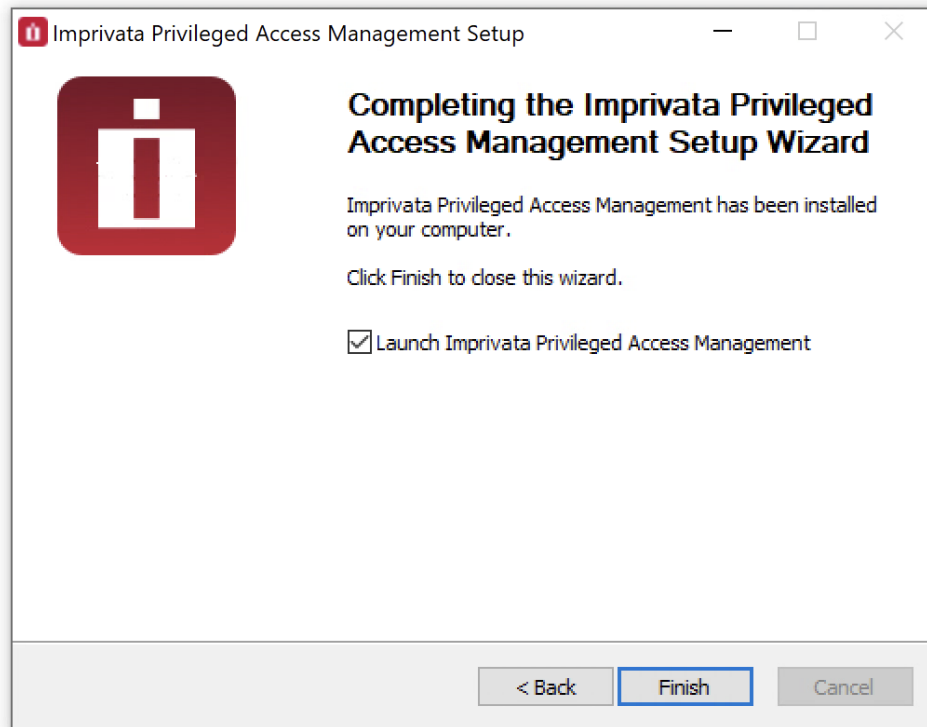
On the final page, confirmation that the installation has been completed will appear.

Enable (check) the box to launch the sign-in page or disable (uncheck) the option to not open the page.

Click **Finish** to close the installation wizard.

The software is now installed.

The default location for PAM is <https://localhost:6443/xtam/>.



Installation Complete

## Logging into Privileged Access Management

Open your web browser and navigate to the login screen of PAM or double click the shortcut on your desktop.

- Non-secured login: <http://localhost:8080/xtam>
- Secured login: <https://localhost:6443/xtam>

At the login prompt, you can sign in with one of the following system administrator logins:

- The [System Administrator](#) account that was created during the installation process.
- The [Active Directory or LDAP account](#) that was (optionally) used to establish integration during the installation process.

Enter the System Admin user and password and click the **Login** button.

Upon successful login, you will be directed to the initialization page of PAM.

The account used as the first login will become a System Administrator.

# Browser SSL Certificate

A default installation of PAM comes with a pre-created PAM Self-signed SSL certificate to encrypt traffic.

Because this SSL certificate is self-signed and therefore not trusted by your browser or certificate authority, a security warning will appear when the login page opens.

It is safe to accept the security warning for this self-signed certificate only; however, you may consider these options:

1. You may use the non-secured login at this location: <http://localhost:8080/xtam> to avoid the browser warning and continue using the software without encrypting your traffic.
2. You may accept the warning, install the certificate and use it as supplied. Although it is self-signed, it will still encrypt the traffic.
3. You may substitute our non-trusted, self-signed certificate with your own trusted, signed certificate by following the procedure described in this [article](#).

While our self-signed SSL certificate is acceptable for trial or PoC deployments, they should not be used for any production deployments.

We **strongly** recommend the use of a well-known trusted SSL certificate or one generated by your own Certificate Authority.

## Initialize

The first login (and only the first) after a new installation will require a system initialization.

When logged in for the first time, click the Initialize button to begin this process.

During this time, the system will create all its needed configuration in the database and services.

Depending on the complexity of your configuration, this process may take anywhere from a few seconds to 1-2 minutes to finish.

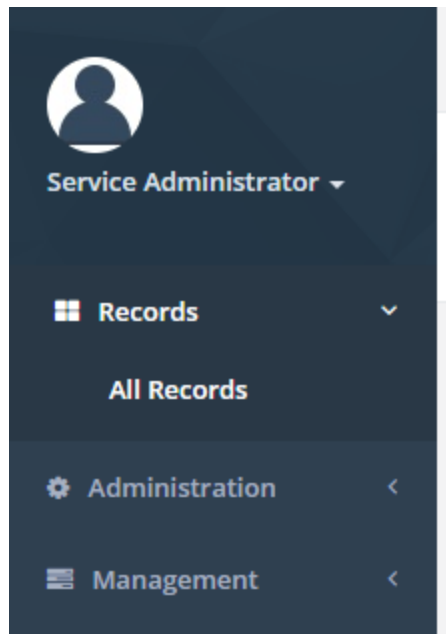
**This is the application initialization page**  
Clicking the button below will initialize the application database  
with the initial data. Currently logged in user Service  
Administrator will become the application administrator.

Initialize

PAM “first-time” Initialization

When the initialization is complete, the system will redirect you to the landing page.

You should see a few menu headings on the left side including Records, Administration and Management indicating that the process is complete.



Initialization Complete

## License Registration

If you have a license key, then you should activate it now.

1. Navigate to Administration > Settings > Registration.
2. On the registration screen, copy and paste your key into the “Activation Code” field and then click **Automatic Registration**.
3. When the license is retrieved successfully (status should display “License is Valid”), click the **Save License** button to finalize.
4. The software is now activated and ready for use.

[Save License](#) [Automatic Registration](#) [Manual Registration](#)

Status

License is Valid

Activation code

c810

License

-----LICENSE BEGIN-----  
Activation:c810  
Product:PAM  
HUB:XtonTech  
Client:ckd

License Activation

## Manual Registration

If the computer is not connected to the internet or cannot establish a connection to the license server for registration, then the following procedure will register the software manually.

1. Click the **Manual Registration** button. A new browser window will appear.
2. Copy or transfer this URL to a computer with an internet connection and load the page.

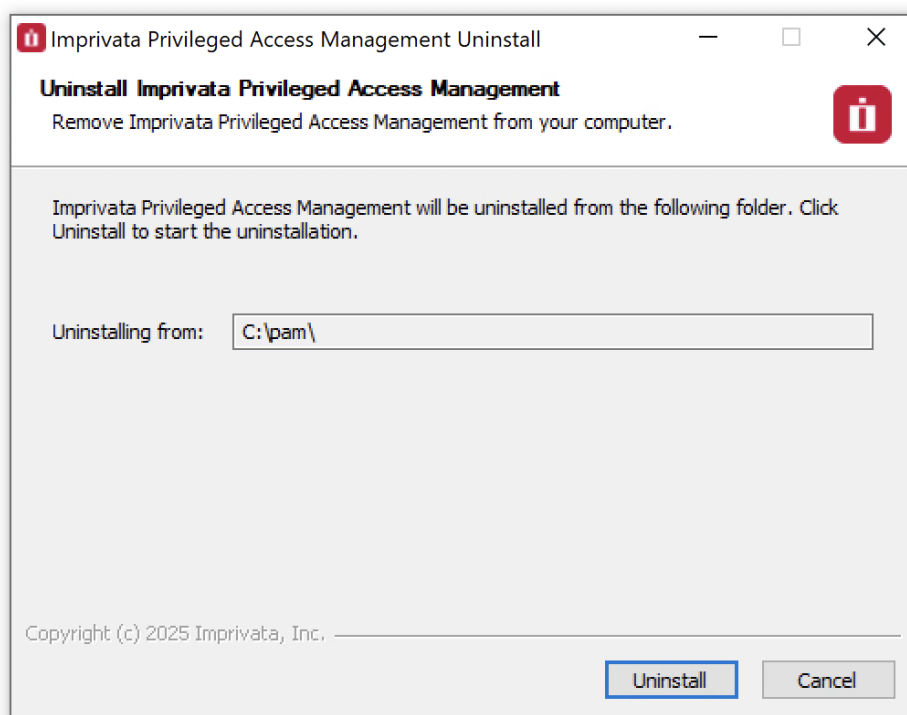
3. Select the copy the license information between and including the LICENSE BEGIN header and LICENSE END footer.
4. Save this information to a file or paste it directly into the “**License**” field in PAM.
5. Click the **Save** License button.
6. The license status will read “**License is Valid**” and the software is now registered.

## Uninstalling Privileged Access Management

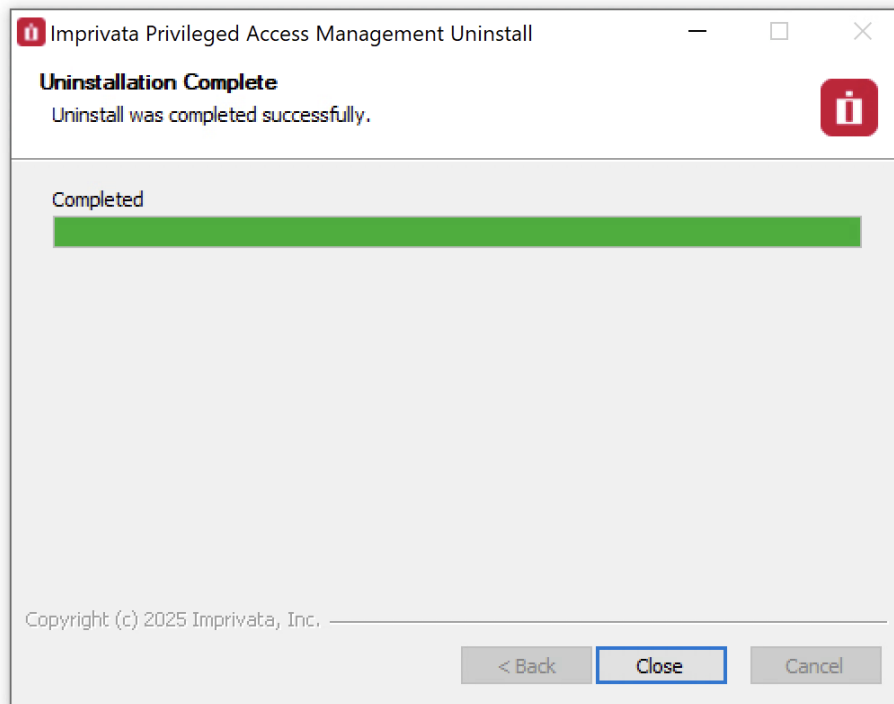
You can uninstall PAM by simply running the uninstall executable located in its installation directory.

### Uninstaller

1. First, logout and close any open Sessions in PAM as well as any open sessions in your Web Browser.
2. Double click the uninstall executable and follow the wizard.



3. When the wizard completes, the software and its services will be removed from your computer.



4. If you deployed additional services to other servers, then you will need to run the uninstall executable on each of these computers to remove the components.

## Database Cleanup

If you have configured PAM with the use of an external database, then you will need to manually remove these database objects.

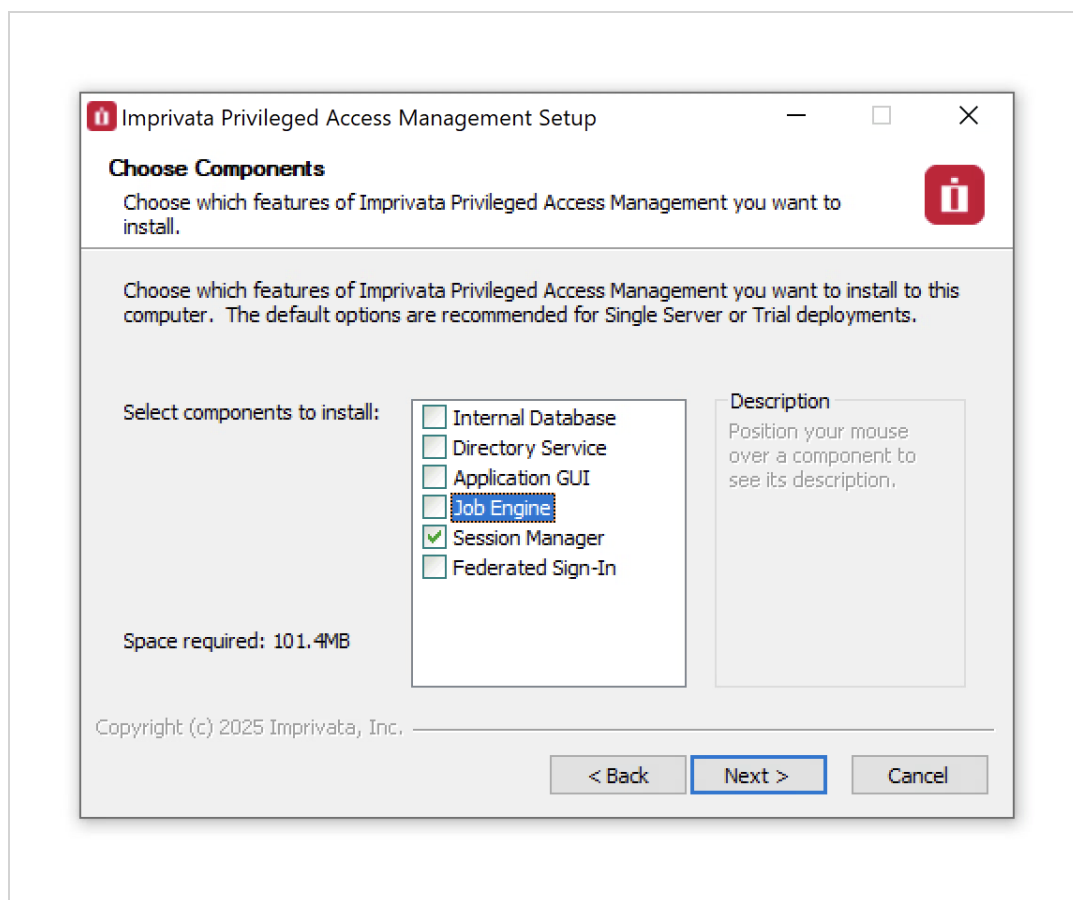
Please contact your database administrator for assistance.

## Appendix

### Remote Session Manager Configuration

When installing the Session Manager component on a remote Windows computer(s), then the following steps should be taken.

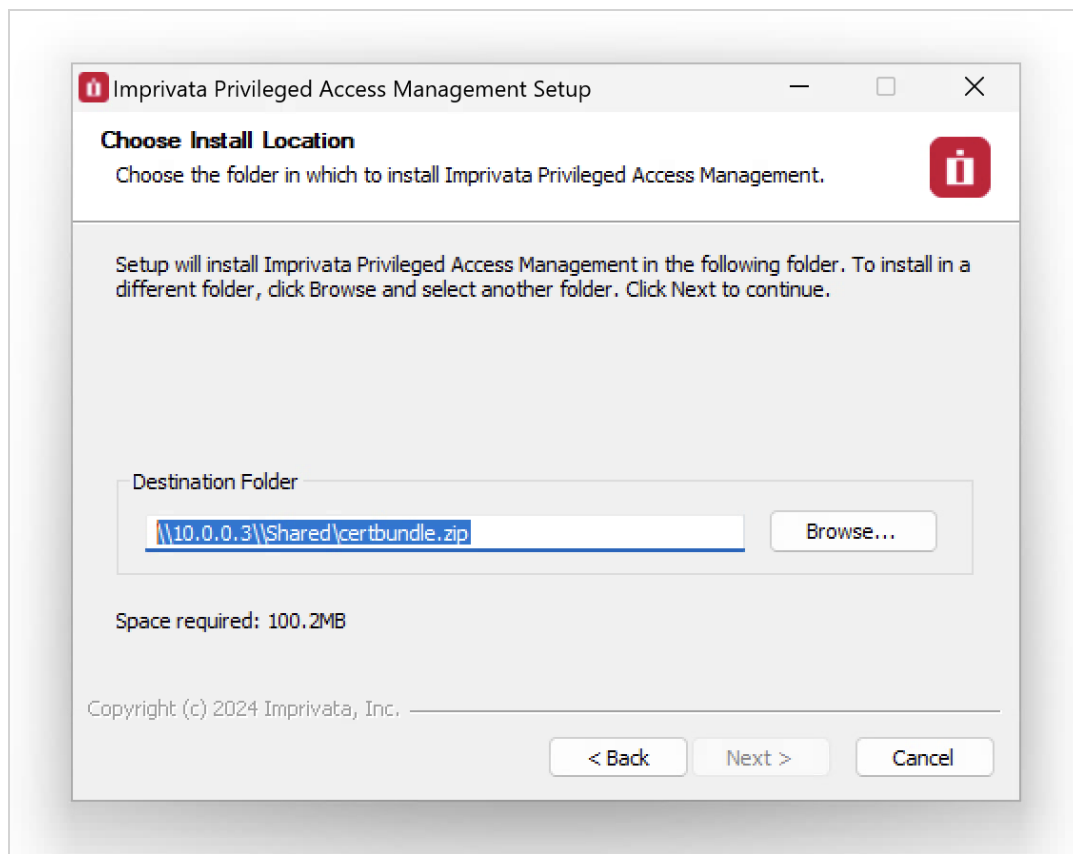
1. Ensure that PAM is Installed and configured on your master computer.
2. Run the setup file on the remote computer where Session Manager is to be deployed.
3. On the Welcome screen, click **Next** to begin the installation on this computer.
4. Read and accept the License Agreement by clicking the **I Agree** button to continue.
5. Uncheck all Component options except Session Manager. Click **Next** to continue.



Select the Session Manager Component

6. Choose your installation location and click **Next** to continue.
7. When prompted, locate and select the certificate bundle that was deployed to your master computer where PAM was installed earlier. Click **Next** to continue.





Locate and Select `certbundle.zip`

- The certificate bundle is in the root PAM installation directory on your master computer. The default file location is `C:\pam\certbundle.zip`
- You may select the `zip` file from this default location (if possible), copy it to a shared network location or simply copy the `zip` file to this remote computer and select it locally.

NOTE: This step is optional, so if you wish to not supply the certificate you may simply click **Next** to continue. By skipping this option, you are acknowledging that the communication between PAM on the master computer and this remote Session Manager computer will not be secured. Because of this, it is recommended that you supply the certificate when prompted and do not skip this step.

8. The Session Manager service will now startup on this computer. Click **Next** to continue.
9. Click **Finish** to complete the installation.

## Offline Installation

Offline Installation Procedure.

If external internet access is disabled or firewall rules are blocking connectivity to our servers preventing the traditional online installation to your desired host server, then PAM can be downloaded and installed using the following offline installation procedure.

1. Download the PAM Offline Installation package from here: <https://bin.xtontech.com/product/XTAMOfflineInstallation.zip>
2. Copy the downloaded `.zip` file to your desired PAM host server. (PAM [System Requirements](#)).
3. Extract the `.zip` file to a temporary location on this host server.

We recommend disabling or adding exceptions to any Anti-Virus or Malware scanners that may be running on this host server. These applications may modify or remove core components of PAM that can lead to failed installations.

4. Run the **XtamSetup** file (`.exe` for Windows, `.sh` for Unix/Linux).

At this point, the offline and online installation procedures are the same, the only exception being with this offline procedure, all the software components have already been downloaded.

5. Complete the installation using the wizard as needed.

For additional information about the actual installation process, please review the appropriate Installation Guide ([Windows](#) or [Unix/Linux](#)) available on our [Documentation page](#).

If questions remain or issues arise while using PAM, please contact the Support team:

<https://support.imprivata.com/communitylogin>.

## Downgrade PAM to an earlier version

1. Download the previous version needed:
  - Browse to <https://bin.xtontech.com/>.
  - Perform a find (Ctrl+F) on the page for the version you need (e.g. 20211219).
  - Copy the text from the tag (e.g. `legacy/pkg/pam-pkg.20211219.zip`).

Note: You can ignore the `.asc`, `.nd5` and `.sha512` files.

- Paste this to the end of the URL in the browser address bar and press enter(e.g. <https://bin.xtontech.com/legacy/pkg/pam-pkg.20211219.zip>).
  - This will prompt you to save this package version.
  - From the `pkg\pam` folder in the `.zip` file, copy the `xtam.war` and `xtamWorker.war` files from the `.zip` file and save them locally.
2. Login to the PAM host server (You will need admin permissions).
  3. Stop the **PamManagement/pammanager** and **PamSession** services.

Note that this PAM node will now be offline until the downgrade is complete.

4. Navigate to `$PAM_HOME/web/webapps` and delete both files `xtam.war` and `xtamWorker.war`. Also delete the `xtam` and `xtamWorker` directories.
  - Optionally, rather than deleting these files and directories, you can move them to a temp or backup location outside of `$PAM_HOME`. If the downgrade process fails, you can move these back and restart the service.
5. Paste the extracted `xtam.war` and `xtamWorker.war` files into `$PAM_HOME/web/webapps` directory.
6. Start the **PamManagement/pammanager** service. This will begin the downgrade process which should complete in a few minutes.
7. Start the **PamSession** Service.

If you are not using the Federated Sign-in Module, then the update process should be complete for this node.

## For the Federated Sign-in Module users

If you are using the Federated Sign-in Module, then you will also need to complete these steps:

1. Stop the **PamManagement/pammanager** service again. This is a second operation which can not be combined with the first procedure.
2. Download the Federated Sign-in Module configuration file (<https://www.xtontech.com/wp-content/uploads/2017/12/web.zip>) and extract to a temporary location.
3. In this extracted archive, there will be a single `web.xml` file.
4. Copy `web.xml` and paste to `$PAM_HOME/web/webapps/xtam/WEB-INF`, overwriting the current file of the same name that already exists in this directory.
5. Start the **PamManagement/pammanager** service.
6. Once the downgrade process is complete for this node, you can repeat these steps for other needed PAM nodes.

## Connection to your own external database

Access Manager supports a wide range of the most popularly used database systems on the market.

When configuring PAM to use your own database, you will need to supply the database connection string.

In general, the connection string will comply with the following example:

*db-host or db-host:port*

To view specific examples for each supported database, please [review this page](#).

## Security Hardening Guide

### Introduction

This section outlines some of the best practices for securing your PAM instance, whether it be installed on a single server or in a multi-clustered environment.

# Technical Support

If questions remain or issues arise while using PAM, please contact the Support team:

<https://support.imprivata.com/communitylogin>.

## Implementation

It is critical to build a secure process around your PAM implementation.

This needs to include a layered approach to security (defense in depth) starting at the operating system, software updates, access to physical systems, protocols, system settings, backups, and personnel procedures.

### General

- **Keep Host Operating System up-to-date.** Operating System (OS) vendors, whether commercial or open source, regularly released security patches that resolve vulnerabilities and improve system security. We recommend keeping your server up-to-date.
- **Backup At Least Daily.** Consider your Disaster Recovery plan.
- **Review System Log for Errors.** It is important to periodically check the OS System Logs for any recurring errors especially after system updates.

### Database

- **Limit access to your PAM database.** When you create your PAM database or scheme, you must limit access to as few users as possible. PPAM encrypts sensitive data in the database using its Master password which is stored outside of this database (in the PAM User Directory). However, the database contains hierarchical structure and the permissions scheme that could be modified by a malicious user. Consider enabling monitoring of the PAM database scheme for unauthorized access.
- **Limit access to your database backups.** Database backups are critical for disaster recovery, but they also carry a risk if someone gains access. The PAM database is encrypted but you must still limit access to ensure that you are following “defense in depth.” Make sure to limit access to database backups to as few individuals as possible.
- **Don't store the database on a server that contains less sensitive databases.** Putting the database on a server with other less secure database instances can open up vulnerabilities. For example, an attacker might potentially use SQL injection on another application to access your private PAM database.
- **Review Database vendor recommendations for SQL security.** Follow your database vendor's recommendations for general security best practices.

### Application Server

- **Use SSL / HTTPS.** Secure Sockets Layer (SSL) is required to ensure that all communication between the web browser and PAM is encrypted and secure (and not cleartext travelling across your network). It is suggested that you install a third-party certificate trusted by a major Internet authority, domain certificate, or self-signed certificate on your Web server.
- **Force SSL / HTTPS.** Even after you install an SSL certificate, users might still be able to access PAM through HTTP. To prevent access through HTTP, disable non-SSL traffic to the PAM server by disabling the open HTTP port 8080 in the `server.xml` file.

- **Limit access to your PAM directory.** It is important to limit access to your PAM home directory. This contains the PAM database and user directory connection information. These values are encrypted but remember “defense in depth.” Try to grant access to as few users as possible.
- **Limit access to shared Content and Export directory.** It is important to limit access to your Content and Export directories. These directories contain session recordings, important certificates for integration with 3<sup>rd</sup> party systems as well as periodic system exports. Content and Export directories are shared between system nodes in the case of multi-node deployments.
- **Limit log on rights to the Application Server.** Administrators accessing the Application Server directly might attempt to monitor memory in use on the server. They also have better chances to access PAM home directory. PAM does several things to protect application memory but the best safeguard is to limit access to the Application Server to as few users as possible.
- **Secure traffic with Active Directory or other external user directories.** It is a good practice to setup integration with Active Directory through its SSL communication channel using the LDAPS protocol.
- **Limit access to PAM user directory.** The PAM user directory stores the master key and local PAM users with their passwords. In case of High-Availability deployments, the PAM User Directory is installed on each PAM node in replication mode. PAM user directory services can be accessed using the LDAPS protocol over port 10636. Make sure that this port is blocked by a firewall to access by anyone but the PAM server.
- **Limit access to PAM session manager.** The PAM Session Manager routes the session traffic and by default it listens on port 4822. The traffic handled by the Session Manager module is encrypted by SSL certificates. Make sure that the port is blocked by firewall by anyone but PAM server. Make sure that the traffic to all system Session Managers is secured with SSL certificate (watch for green session manager entry in the Administration / Settings / Proximity Groups configuration).
- **Protect your Master key.** The Master key for PAM is stored in the PAM user directory service. The Master key is obfuscated and encrypted, but “defense in depth” would require limiting access to the directory. Make sure you back up the original master key and store it in a very safe and secure location.

## Application Settings

- **Secure the Local Admin Account.** When you create the first user in PAM, it is a privileged admin account that you can use when your domain is down. We recommend protecting this account with a very strong password. This password should be stored in a physical safe with limited access (there is no need to use this account except in emergencies where other accounts are not working, if AD is down or for some other reason).
- **Review Activity Reports.** It is a good practice to regularly review the activity and permissions reports. This can help find anomalies in system access.
- **Use Event Subscriptions or SIEM to notify of any security anomalies.** Event subscriptions can be used to send email alerts on various events in the system, and syslog can send PAM events to a SIEM tool for correlation. This might be used to notify administrators if there are failed login attempts or if certain Secrets are viewed, and so on.

## Maintenance

### Web Browser

#### AutoComplete

Browser AutoComplete allows web browsers to save the account credentials for the PAM login screen. These credentials are often kept by the web browser in an insecure manner on the user's workstation. Allowing AutoComplete also interferes with the security policy of your PAM deployment by not requiring the user to re-enter their login credentials on your desired timeout schedule.

### **Force Password Masking**

Password Masking prevents over the shoulder viewing of your passwords by a casual observer (passwords show as \*\*\*\*\*).

The number of asterisks does not relate to the length of the password for added security.

Use the copy password to clipboard option instead of displaying the passwords on the screen to increase security.

## **Permissions and Authentication**

### **Login Password Requirements**

Passwords that are used by local users to log in to PAM can be strengthened by requiring a minimum length and the use of various character sets. Configure the password formula for local users to match policies of your organization.

### **Two-Factor Authentication**

Users must authenticate to PAM at least once by using either local PAM credentials or their Active Directory credentials.

However, when a password gets compromised, you can protect yourself by enabling two factor authentication (MFA) in PAM.

When you use multiple factors of authentication, each factor must be a different type of information – that is, either a piece of information a user **knows**, **possesses**, or **is** (for example, when a fingerprint is used as a biometric identifier).

It is a good practice to protect logins to PAM using two-factor authentication.

### **Roles**

PAM uses role-based access control, which allows administrative and user capabilities to be partitioned by these roles.

This can allow for granular control over which areas of the application a user has access to – for example, allowing someone the rights to view reports in PAM, but no other administrative permissions otherwise.

### **Separation of Duties**

PAM administration workflows allow for the delegation of administrative function to different users.

The workflows can also create a dual-control environment where important administrative functions could only be performed with peer approval of other administrators.

## Privileged Access Management

Privileged Access Management (PAM) is an agentless solution that provides a secured database to manage privileged accounts and secrets, establishes secure sessions for users through a standard web browser and automates the execution of jobs or tasks without disclosing or sharing access.

The purpose of this guide is to perform a new installation and first time system initialization.

At the conclusion of this guide, PAM will be ready for system configuration and use.

PAM is installed to a Windows or Unix computer (physical or virtual), with optional connection to Active Directory or LDAP.

PAM consists of several modules; a database that contains secrets, configuration, passwords and audit events, a service to establish, monitor and record privileged sessions, a user directory to maintain local users and groups and a job engine to execute scripts and tasks.

## Privileged Account Management

A secure AES 256-bit encrypted database that contains records which can be stored, shared and used without disclosing the actual privileged account or its secrets (passwords, certificates or keys).

## Privileged Session Management

The ability to establish a privileged session to an underlying system (Windows, Unix, Linux, Mac) through a standard web browser while providing the means to monitor, join, record or terminate this session.

## Privileged Job Management

Schedule, automate or execute on demand jobs to privileged systems without embedding the secrets in scripts or sharing them with untrusted users.

## Software Components

To accomplish the requirements above, PAM needs to install, configure and run the following software and services.

These components are deployed during the installation process (single server deployment) or they can be distributed to multiple servers (farm deployment) to scale performance.

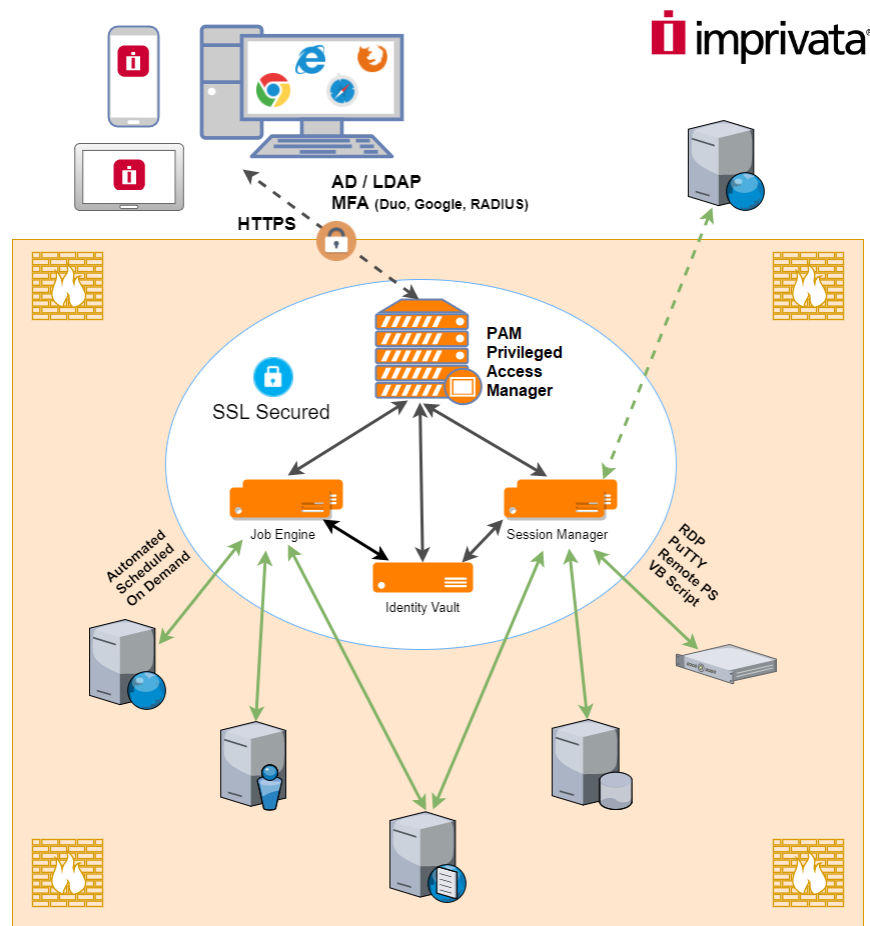
Single server deployments can be scaled to farm deployments when additional resources become needed.

## Architectural Diagram

PAM sits within the firewall in its own SSL secured network.

Client computers make requests, establish sessions and run jobs from inside or outside the firewall to computers also located inside or outside the firewall using only their native web browser of choice.

The Database of Secrets secures all records using **an AES 256-bit encrypted protocol** and only delivers these secrets to authorized remote requests.



Privileged Access Management Architectural Diagram

## Navigating the User Interface

The Record List can be thought of as the homepage of the PAM system.

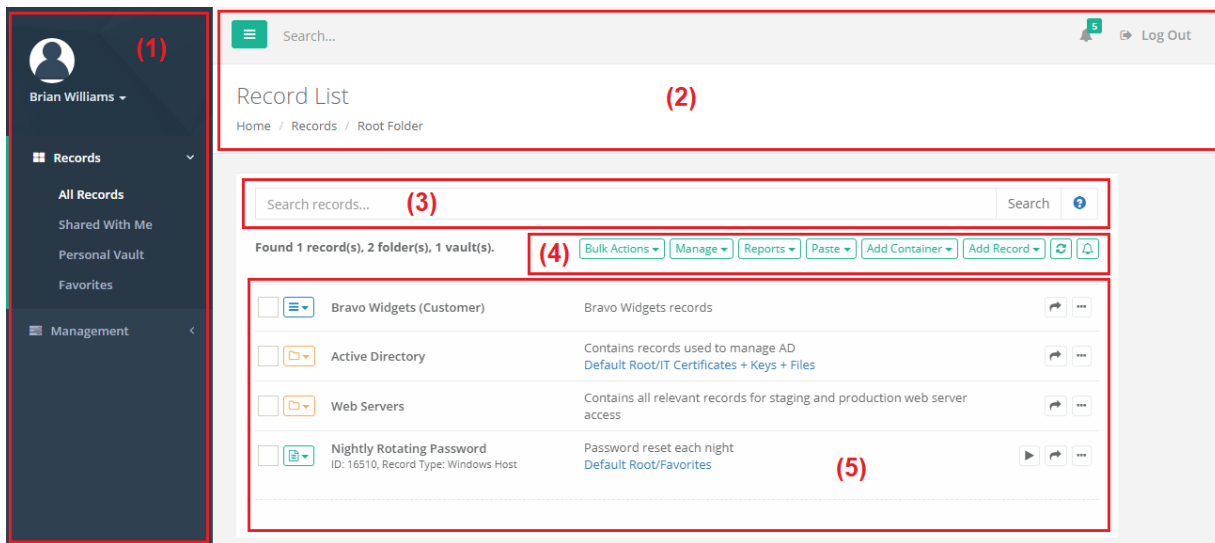
Regardless of your role, upon login to PAM, you will be directed to the Record List, which may also be referred to as the **Root Folder** or **Default Root**.

It is here where all users will be able to locate, search, connect, share or favorite any object in the PAM identity vault for which they have permissions to access.

### The Record List contains the following sections:

- [1. Left Menu Navigation](#)
- [2. Top Menu](#)
- [3. Search Records](#)
- [4. Action Menu](#)
- [5. Object List](#)





## Left Menu Navigation

The Left Menu Navigation section named Records provides convenient links to access various areas of your Record List while the section named Management provides access to options that are specific to your PAM profile.

You can use the **Expand** or **Collapse** button to expand or collapse this, or any, section of this navigation.

**In the Records section, the following menu options are available:**

**All Records:** Displays the All Records view where any objects (Vaults, Folder and Records) that you have permissions to access are available.

Records are displayed using their hierarchical layout, so you can navigate through the vaults or containers to access the necessary records.

**Shared With Me:** Displays all objects that you have permission to access regardless of the object's hierarchical layout.

This view is useful if you have access to a record but not the folder in which it resides.

Users with the System Administrator role will not have a **Shared With Me** view since this role gives them access to all objects.

**Personal Vault:** Use this link to access your Personal Vault view.

If the Personal Vault link does not appear it may have been disabled by the PAM Administrator. Please check with your PAM Administrator for more information.

**Favorites:** Any objects that you favorite, will appear in this view.

Additionally, if a Vault or Folder is favorited, then it will appear as a link itself under this Records section.

The link will appear as **<Folder Name>**.

**In the Management section, the following menu options are available:**

These Management links can also be accessed by using the dropdown menu displayed below your login picture and name at the top of this menu.

**My Sessions:** Displays a list of all *Active* or *Completed* sessions that you created or joined. If you have the applicable permissions, you will be able to access the session recordings and events from this view as well.

**My Profile:** Displays a list of options that can be configured for your account. This includes changing your login password (local user accounts only), subscriptions (alerts) and account preferences.

**My Alerts:** Displays a list of all your alerts.

**My Workflows:** Displays a list of all Active, Current or Expired workflow requests that involve you (Requestor or Approver) and a list of all workflow requests that you have been assigned to *Approve* or *Reject*. Use this view to see the current status of any of your workflow requests or to Approve or Reject any workflow requests of other users.

**About:** Displays information about the current version of PAM.

# Top Menu

The Top Menu appears on all pages and provides the following options:

**Collapse Navigation:** Click this button to collapse the left menu navigation pane. This is helpful for users working on lower resolution displays.

**Search:** This Search box is used to search for objects by name that appear in the Left Menu Navigation only. For example, if you have many Folders or Vaults marked as your favorites, this search box will display only those links to match your search criteria. Use the Search Records box to search for all objects regardless of your Favorite state.

**Alert Notification:** If you receive any alerts, a badge will appear indicating the number of alerts as well as a dropdown displaying the most recent 6 alerts received. Click the **See All Alerts** link at the bottom of the list to navigate to your **My Alerts** view.

**Logout:** Click this button to logout of PAM. For security purposes, it is recommended to close your all browser sessions after logout to complete the logout process.

**Object Header:** Displays the name of the current *Object* you are viewing as well as breadcrumb navigation.

## Search Records

The **Search records...** bar will allow you to search for any objects (Vaults, Folders or Records) that you have permission to access by using various criteria.

Type your search query into this bar, click the **Search** button and the results will be displayed below in the Object List.

For a list of example Search Query options, please read our [Search Query](#) article.

# Action Menu

The Action Menu bar will allow you to perform a number of actions based on your current location in the Record List.

The list of Actions available in this bar depends entirely on your permissions, so you may not see all the options described in this section.

**Bulk Actions:** Allows you to perform an action against multiple selected objects.

**Manage:** Used to manage the configuration of the current container, including the Import function.

**Reports:** Generates the selected report specific to only the current container.

**Paste:** Use to *Paste* the currently copied object(s). Paste will paste the copied object as a new object, while *Link* will paste the copied object as a linked reference to the original.

**Add Container:** Use to create a new [Vault or Folder](#) in this current container.

**Add Record:** Use to create a new Record in this current container.

**Refresh:** Click to Refresh the current view.

**Subscribe to Alert:** Use to Subscribe to Alert based on this current container.

# Object List

The Object List displays all the objects (Vaults, Folder and Records) that you both have permission to access as well as meet the criteria of the current Search Query or View.

**From left to right, the following information is displayed:**

**Check Box:** Select an object(s) by enabling this checkbox next to each selected object. These check boxes allow you to perform Bulk Actions.

**Icon Menu:** The Icon defines what the object is and provides a dropdown menu of actions that can be performed against this object.

Vault containers are defined with the **Blue icon**, Folders, the **Orange icon** and Records, are the **Green icon**.

The Action dropdown menu will only display options that are available based on your permission to this object.

**Object Name:** Displays the name of the object and can be clicked to navigate to or into this object.

**Object Description:** Displays the object's Description, if one was supplied.

**Object Link:** Displays all the *links* to this object that resides within other containers or locations of PAM. These links are visible to all users, however when clicked if the user does not have permission to this linked location, they will receive an access denied message.

**Object Actions:** Displays all the available options to be performed with this object:

- **Connect:** The Connect button will appear for any Records that have a *Session Connect* option.
- **Quick View:** The Quick View button will display the contents of the selected record in the foreground without having to open it. This is useful if you need to quickly retrieve information from a record like the Username or Password. The Quick View option cannot be used to manage the record, it is only for viewing, copying or unlocking fields.
- **Share:** The Share button will appear for any Objects. Assuming you have permission to share the object, this will open the Share menu in order to quickly grant others access to this object.
- **Action Menu:** The Action Menu will display a dropdown menu of options that are available for this object based on your current permissions.

## Personal Vault

Let us remember your secrets so you don't have to!

PAM automatically provisions a **Personal Vault** for each user who logs into PAM. These Personal Vaults provide a secure area where users can store their own secrets, connections, logins, keys or any other records they wish.

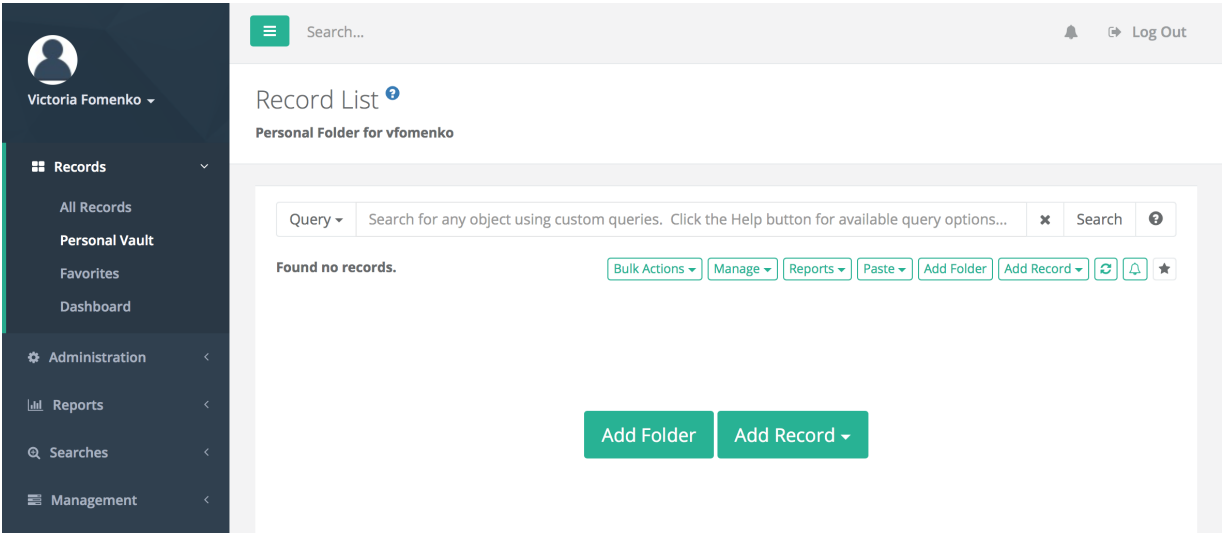
**By default**, these areas give each user full ownership of their own vault and its content, while no other non-Administrative users are granted access.

However, any folders and records created in a Personal Vault can be shared with others users if the Vault owner chooses, creating a shared secret area.

PAM System Administrator may decide to limit the permission users have within their Personal Vault.

The default *Owner* permission allows the user to have full control over the content of their Personal Vault including the option to share; however, they may decide to limit this to the *Manager* role.

The *Manager* role allows the user to create, edit and delete content within their vault but removes their ability to share this content with others, restricts access to reporting and more.



## Benefits

Personal Vaults provide the following benefits:

- Creates better organization as users do not have to store their personal secrets in PAM's default Records List (i.e. root folder).
- Provides a secure area where a user may store and have full control over their own assets like logins, keys and connections.
- Works with the [PAM Browser Extension](#) to provide an automated login experience to websites.
- Allows a user to share records from their vault with others, creating a shared secret space.
- System Administrators, Auditors and users with [Global Permissions](#) still maintain some access to Personal Vaults to ensure corporate compliance and regulations.

## Personal Vault Role

If you wish to change the Role that is granted to the user when their Personal Vault is provisioned (Record Control: Owner is the default), use the following procedure:

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Parameters > Personal Vault Role.
3. Select the desired role: *Owner* or *Manager*.
4. Click the **Save** button.

Please note that this role change will only be applicable to newly provisioned Personal Vaults. All existing Personal Vaults will retain their current permission.

# Personal Vault Recording

Sessions created from within a user's Personal Vault permit the user to decide to record their session or not by providing both **Connect** and **Connect and Record** options.

PAM System Administrators may override this behavior to force all sessions created from within any Personal Vaults to be done so with video and/or event recording enabled.

To enforce event recording for all sessions from any Personal Vaults:

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Parameters > Personal Vault Event Recording.
3. Select the option *Default* or *Enforced*.
  - Default defers recording to the user's permission or selection while Enforced enforces recording.
4. Click the **Save** button.

To enforce video recording for all sessions from any Personal Vaults:

1. Navigate to Administration > Settings > Parameters > Personal Vault Session Recording.
2. Select the option *Default* or *Enforced*.
  - Default defers recording to the user's permission or selection while Enforced enforces recording.
3. Click the **Save** button.

## Disabling

If you wish to not enable the use of Personal Vaults for users, then they can be disabled using the following procedure:

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Parameters > Personal Vault.
3. Select the *Disabled* option for the dropdown menu and then click the **Save** button.



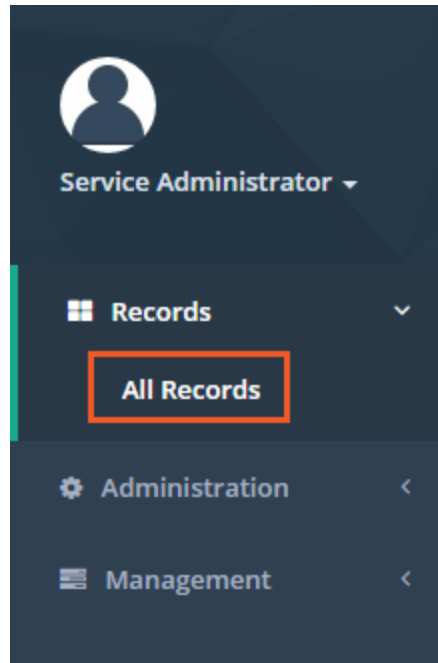
# Working with Folders

Folders provide a straightforward way to organize and more easily share records. We will begin this guide's feature walkthrough with folders.

## Creating Folders

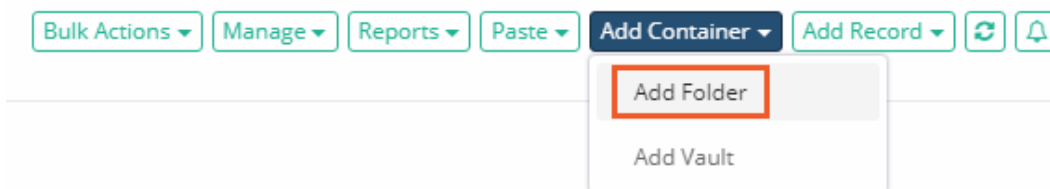
To create our first folder:

1. On the left navigation menu, expand the Records section and click **All Records**.



All Records Menu Option

2. From the Records List page, click the *Add Container* > **Add Folder** button.



Add Folder

3. For the new folder, enter:
  - a. *Name*: IT Records;
  - b. *Description*: Use this folder to organize and share records within the IT department.
4. Click **Create**.

## Create Folder

### Name

IT Records

### Description

Use this folder to organize and share records within the IT department

Cancel

Create

### Creating a New Folder

5. Your new folder will now appear in the root Records List page view. The folder Name and Description will display in this view as well as Action menus located to the left and right side of this folder.

## Folder Options

Folders can contain or be associated to several custom objects which we will cover throughout this guide.

For now, let's begin with two basic options: *Alerts* and *Favorites*.

Alerts configured on a folder will notify the user to specific events that take place on and within this container.

### To setup your alert:

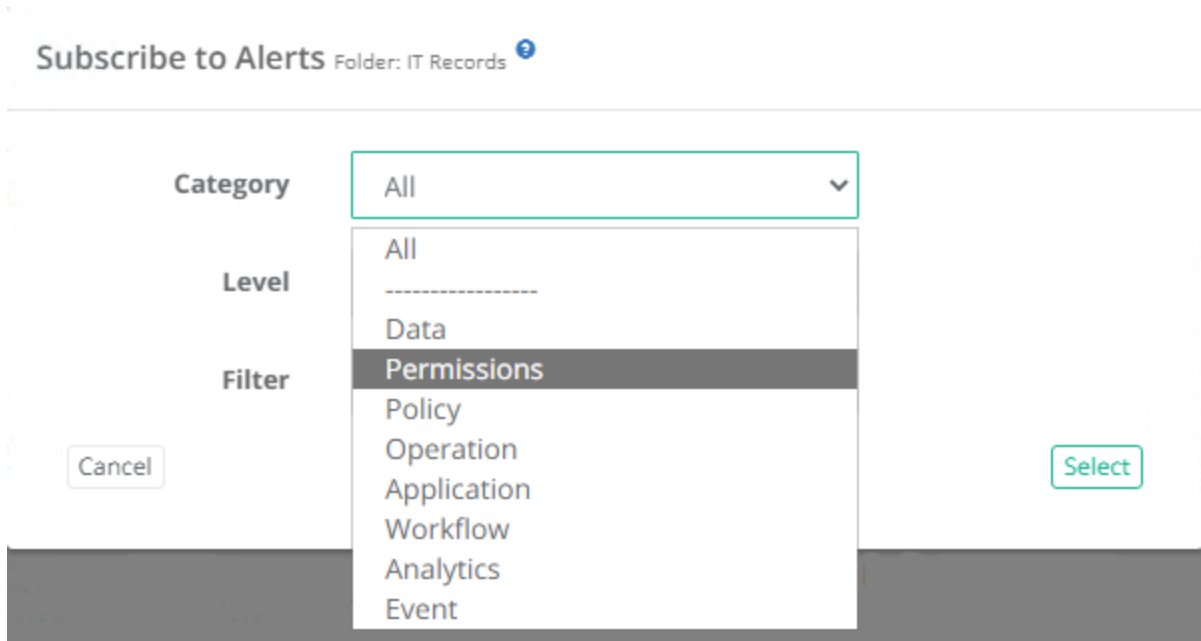
1. Open the "IT Records" folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
2. When in the **IT Records** folder, click the **Alerts** icon along the top row.



### Subscribe to Alerts

3. On the **Subscribe to Alerts** dialog, select:
  - a. *Category*: **Permissions**
  - b. *Level*: **All**

- c. *Event Filter*: can be left empty.



4. Click **Select**. The alert is now saved to your profile and will trigger when any permission events are generated for this folder.

Favorites can be assigned to folders to make them more easily accessible when navigating throughout the software.

Favorited folders will appear in the Records section of the left navigation menu.

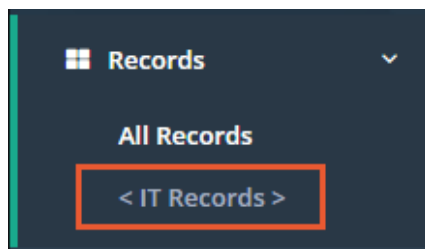
#### To favorite your folder:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
2. Click the **Favorites** button along the top row.



Add to Favorites

3. The GUI will refresh and in a few moments your favorited folder **<IT Records>** will appear in the left navigation menu.



Favorites Menu

NOTE: To *unfavorite* a folder, simply click this same button a second time.

Folders are configurable containers within PAM to organize records. We will revisit these options later in the guide.

For now, we have this basic building block configured, so we can move on to [Records](#).

## Creating Records

Records are the objects that store session host connection parameters, secured passwords, certificate and key files as well as several other secrets.

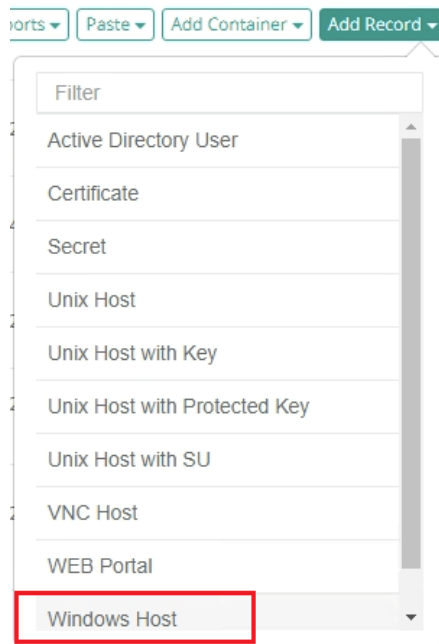
Much like folders, many configurable objects are associated to records to facilitate their sharing and use in PAM.

To better understand Records, we will begin by first creating one.

### Your First Record

To create a new record:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
  - a. If you still have it in your Favorites, then you can click **<IT Records>** in your left navigation menu for quick access to this folder.
2. Click the **Add Record** button and select the Record Type **“Windows Host”**. This will create a record that will be used to establish a browser based remote desktop connection to the configured Windows host.
  - a. This example will use a simple Windows Host record type, however if you would prefer to use the Unix Host type, the process will be similar.
  - b. To learn about the other standard Record Types or how-to custom create a new Record Type, please review the [User Manual](#) located on our website’s [Documentation](#) page.



Create a "Windows Host" Record

3. We'll begin by giving this new record a name and description
  - a. *Name*: Production Web Server.
  - b. *Description*: Record for our production web server.
  - c. *Reference Record* (optionally): [Use your previously created record](#). Default field is empty.
4. Now the connection details will need to be supplied.
  - a. *Host*: Enter the computer host that will be used for a remote desktop connection.
  - b. *Port*: Define the port that is open and available on this host for remote desktop. Default port for Windows is 3389. Unix or Linux is 22.
  - c. *User*: Enter the username ([user@domain.com](#) or domain\user) that has remote access to the host.
  - d. *Password*: Enter the password for this user account.
5. Click **Save and Return** when the fields have been populated.

## Record Edit

Home / Records List / **Production Web Server**

**Production Web Server**

**Name**

Production Web Server

**Description**

Record for our production web server

**Reference Record**

Web Server

✕ No Results Found

**Type**

Windows Host

**Host**

10.0.0.23

**Port**

10023

**User**

pam\itadmin

?

**Password**

@edWtSE}P137\*o

👁

📞

🔍

Password is Very Strong.

Save

Save and Return

Cancel

### "Windows Host" Record

Your first record is now created and can be viewed and edited within **<IT Records>** folder.

We will return to explore some of the other options within *Records* later in the guide.

## Connecting to Sessions

### Connecting to Sessions

One of the many features of Records is the ability to use them to establish a secured session.

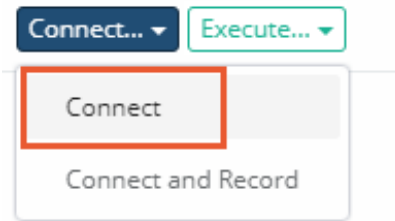
Sessions themselves can be established with or without recording enabled, which we will discuss further in another section of this guide.

For now, let's use our recently created "Production Web Server" record to create a secure session.

## Establishing your First Secure Session

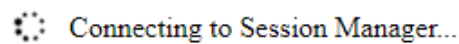
To establish your first session:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
  - a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Open the “Production Web Server” record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Once in this record’s View page, you will see several options both in the top and bottom rows. Locate the Connect button along the top, click it to expand the dropdown menu and then select the **Connect** option.



Connect to a Session

4. A new browser window or tab will appear with the message “Connecting to Session Manager”. This message will change to “Connecting to Host” after a few seconds and then finally, the remote desktop connection to your host will appear in your browser.



Session Manager Browser Connecting Message

1. This is a full remote desktop connection so feel free to explore the session’s functionality and responsiveness for a bit.
5. When you are ready to complete the session, you may do so by logging out of Windows (or Unix) as you normally would in a remote session or you could simply close this browser window.

Your first secure session is now complete. Before we proceed with establishing a recorded session, let’s take a quick look at the record’s Session History.

## Record’s Session History

Within PAM, every record’s session history is captured and made available throughout the system for quick and easy review.

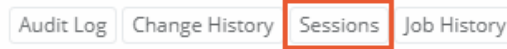
The session history will capture valuable information about each established session including who created the session, session start and end times, current activity status and whether it was recorded.

In this section, we are going to look specifically at the session history associated to our “Production Web Server” record.

To view our record’s Session History:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
  - a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.

2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate and click the **Sessions** button along the bottom row of options.





#### Record's Session History

4. A new view will load that provides details for all sessions (active or completed) associated to this specific record. You will notice that our previously established session is listed and as expected it displays your System Administrator account, the start and end time of the session, status as *“Completed”* and Recording as *“Not recorded”*.

System Sessions

Found 1 sessions.

Time: Last Day ▾ State: Any ▾ Columns ▾  

Show 50 ▾ entries Search:

CSV PDF XLSX PDF Protected CSV Protected XLSX Protected

Showing 1 to 1 of 1 entries

Record	User	Start Time	Completion Time	Type	Status	Rating	Recording
Viktoria	Service Administrator (xtamadmin) /Local	06/15/2021 15:34:18	06/15/2021 15:36:18	RDP	Completed	★★★★★	Available ...

First Previous 1 Next Last

#### Session History

5. At this time, please explore the assorted options that are available in this view including:
  - a. Filter options along the top to help filter based on time or state.
  - b. Number of display entries to load.
  - c. Search box to quickly locate specific events.
  - d. Export options to download and share the session history with others.
6. When you are ready to return, simply click your browser’s **Back** button. This will navigate you back to the record’s View page.

## Secure Session with Recording

Our first secure session was established without recording enabled.

This allowed the user to securely connect to the session and fully interact with the host using their browser without it being recorded, but now we want to introduce the option to add recording to this same session.

Recording is a great option to have because it maintains a record of everything that happened during the session beyond just the basic session history events of “who” and “when”.

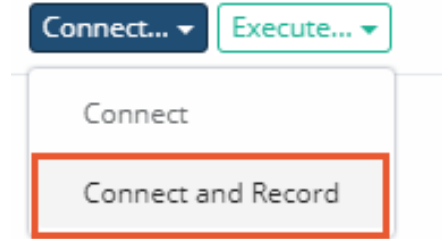
Using our same *“Production Web Server”* record, we are now doing to connect with recording enabled.

To establish a secure session with recording:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
  - a. If you still have it in your Favorites, then you can click **&ltIT Records>** in your left navigation menu for quick access to this folder.



- Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
- Locate the **Connect** button along the top, click it to expand the dropdown menu and then select the **Connect and Record** option.



#### Connect to and Record a Session

- As was with the earlier, non-recorded session, a new browser window or tab will appear and in a few seconds, you will be logged into the remote desktop session again.
  - Please note that the message above the session states “(with Recording)” to indicate to the user that this secure session is being recorded.
  - Feel free to use the session for a bit to perform some operations so that activity is recorded and can be reviewed later.
- Unlike earlier, when you are ready to continue with the exercise do not complete this session. Instead, return to your record view still open in another browser window. On the records’ view, open the Session history by clicking the **Session** button at the bottom of the record’s View page.
- When the Session page loads, you will see our earlier non-recorded session at the bottom and at the top of the list you will see our current Active session still running. Notice that this current session status is displayed as “Active” and recording shows “Recording...”. Take a moment to explore some of the other options available in the view. Stay on this page when you are ready to continue.

System Sessions

Found 5 sessions. Time: Last Month State: Any Columns Refresh Export

Show 50 entries Search:  CSV PDF XLSX PDF Protected CSV Protected XLSX Protected

Showing 1 to 5 of 5 entries

Record	User	Start Time	Completion Time	Type	Status	Rating	Recording
Viktoria	Service Administrator (xtamadmin) /Local	06/15/2021 15:34:18		RDP	Active		Recording... <span>...</span>
Viktoria	Service Administrator (xtamadmin) /Local	06/11/2021 16:08:42	06/11/2021 16:14:43	RDP	Completed	★★★★★	Available <span>...</span>
Unix Host Record	Service Administrator (xtamadmin) /Local	06/11/2021 16:01:34	06/11/2021 16:01:44	SSH	Completed	★★★★★	Available <span>...</span>
Unix Host Record	Service Administrator (xtamadmin) /Local	06/11/2021 15:54:39	06/11/2021 16:00:19	SSH	Completed	★★★★★	Available <span>...</span>
Unix Host Record	Service Administrator (xtamadmin) /Local	06/11/2021 15:57:03	06/11/2021 15:59:26	SSH	Completed	★★★★★	Available <span>...</span>

First Previous 1 Next Last

#### Session History with Active Session

- Return to the secure session currently running in your other browser window and complete the session as you did previously. You will receive a session completed message when this is done. You may now

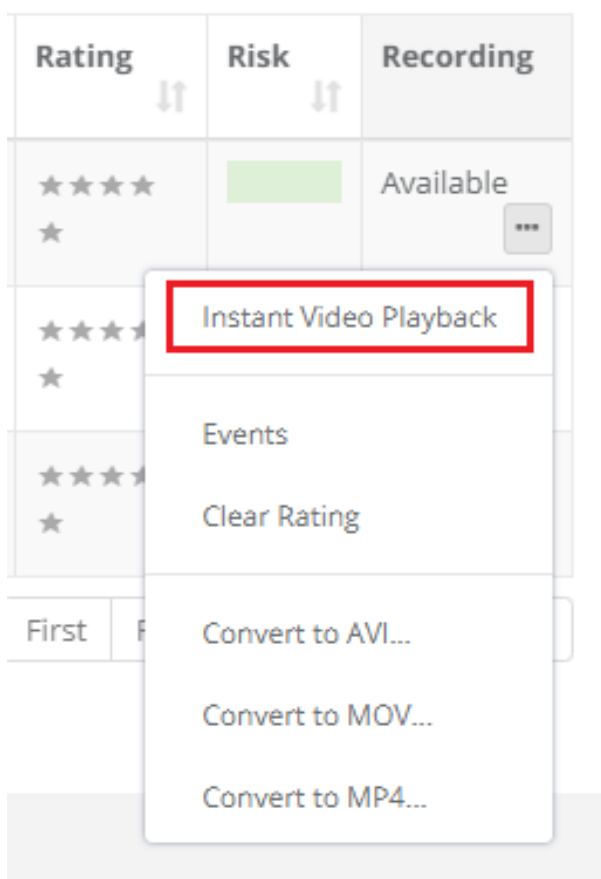
close this window or tab.

- Back in the *Session History* page, click the **Refresh** button. You will now see that the previously Active session is now “*Completed*” indicating that this session was closed. You should also note that the Recording status has changed to “*Available*” and has an action menu.

Record	User	Start Time	Completion Time	Type	Status	Rating	Recording
Viktoria	Service Administrator (xtamadmin) /Local	06/15/2021 15:34:18	06/15/2021 15:36:18	RDP	Completed	★★★★★	Available ...

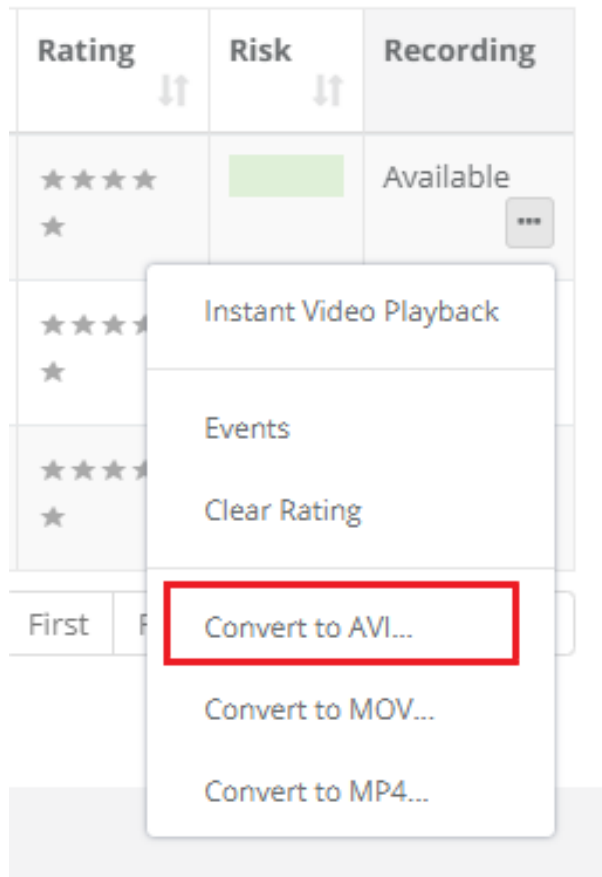
#### Completed Session with Recording

- All completed and recorded sessions will have this Available action menu to view the video playback immediately in your browser or to convert and download previously recorded secure sessions. Click the **Action menu** dropdown and select the **Instant Video Playback** option. A new browser window or tab will appear, ready to playback the selected session recording. Click the **Play** button along the bottom of the video to start the playback. You can click along the video timeline to jump forward or backwards.



#### Recorded Session Video Playback

- Optionally, you may wish to convert the session video recording into a file that can be downloaded. To do so, click either the **Convert to AVI**, **Convert to MOV** or **Convert to MP4** options then the file will be converted and a **Download** button will appear when it is ready.



Video Processing and Download

TIP: If your session included any Session Events (keystrokes, clipboard activity or file transfers), then you can click the **Events options** in the Action menu to display these events. From this *Session Events report* you can use the **Jump to Recording** option to automatically advance to that section of the video.

This concludes the steps required to establish a connection to a record with and without recording.

You may establish more sessions if you wish to further test the connections or even create additional records to test other types.

When satisfied with this exercise, please continue to the [next section of this guide](#).

## Setting your Preferred Session Window Size

When connecting to a secure Session, PAM allows for either a full screen browser connection, a smaller, windowed browser connection or opening in a new browser tab.

This setting is defined on a Global level so that it can be applied to all users' Sessions; however there is a User level setting that can also be defined by each PAM user.

The "User" level setting takes precedence over the "**Global**" setting assuming they are different.

## “Global” Session Start Mode

### Configuring the “Global” Session Start Mode (System Administrators only):

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Parameters.
3. Locate the parameter **“Session RDP Resize Method”** and select either “Fixed” or “Reconnect” from the dropdown menu. *Reconnect is the default mode.* Fixed will open to the exact resolution defined in the next parameter “Session RDP Screen Size” and Reconnect will allow for custom resolution by simply resizing the browser window.
4. Locate the parameter **“Session RDP Screen Size”** and enter a screen resolution (width x height in pixels). *1024x768 is the default size and is only applied when “Session RDP Resize Method” is set to Fixed.*
5. Locate the parameter **“Session Start Mode”** and select either “Full Screen”, “Window” or “Tab” from the dropdown menu. *Window is the default mode.*
6. When complete, click the **Save** button to their right.

Session RDP Resize Method	Reconnect	?	Save
Session RDP Screen Size	1024x768	?	Save
Session Start Mode	Window	?	Save

All users’ sessions will now open in this start mode unless they override it in their User level setting as shown in the next section.

## “User” Session Start Mode

1. Login to PAM with your user account.
2. Navigate to Management > My Profile > Preferences.
3. Locate the parameter **“Session RDP Resize Method”** and select either “Fixed” or “Reconnect” from the dropdown menu. *Reconnect is the default mode.* Fixed will open to the exact resolution defined in the next parameter “Session RDP Screen Size” and Reconnect will allow for custom resolution by simply resizing the browser window.
4. Locate the parameter **“Session RDP Screen Size”** and enter a screen resolution (width x height in pixels). *1024x768 is the default size and is only applied when “Session RDP Resize Method” is set to Fixed.*
5. Locate the parameter **“Session Start Mode”** and select either “Full Screen”, “Window” or “Tab” from the dropdown menu. *Window is the default mode.*

6. When complete, click the **Save** button to their right.

## User Profile

Home / My Profile

The screenshot shows a web interface for 'User Profile' with a breadcrumb 'Home / My Profile'. Below the title are three tabs: 'Profile', 'Subscriptions', and 'Preferences', with 'Preferences' being the active tab. The main content area has a header 'Found 3 parameters.' with a 'Refresh' button on the right. Below this are three settings, each with a label, a value field, a help icon, and a 'Save' button:

Setting	Value	Help	Action
Session RDP Resize Method	Reconnect	?	Save
Session RDP Screen Size	1024x768	?	Save
Session Start Mode	Full Screen	?	Save

Your personal sessions will now open in this start mode regardless of the setting that has been applied at the Global level.

## Transferring Files

How to quickly copy files into or out of remote sessions using drag and drop.

When you are within an secure, remote session you can copy files into the remote host and copy files out of the remote host using a simple drag and drop method.

The following describes the procedure for both Windows and Unix host sessions.

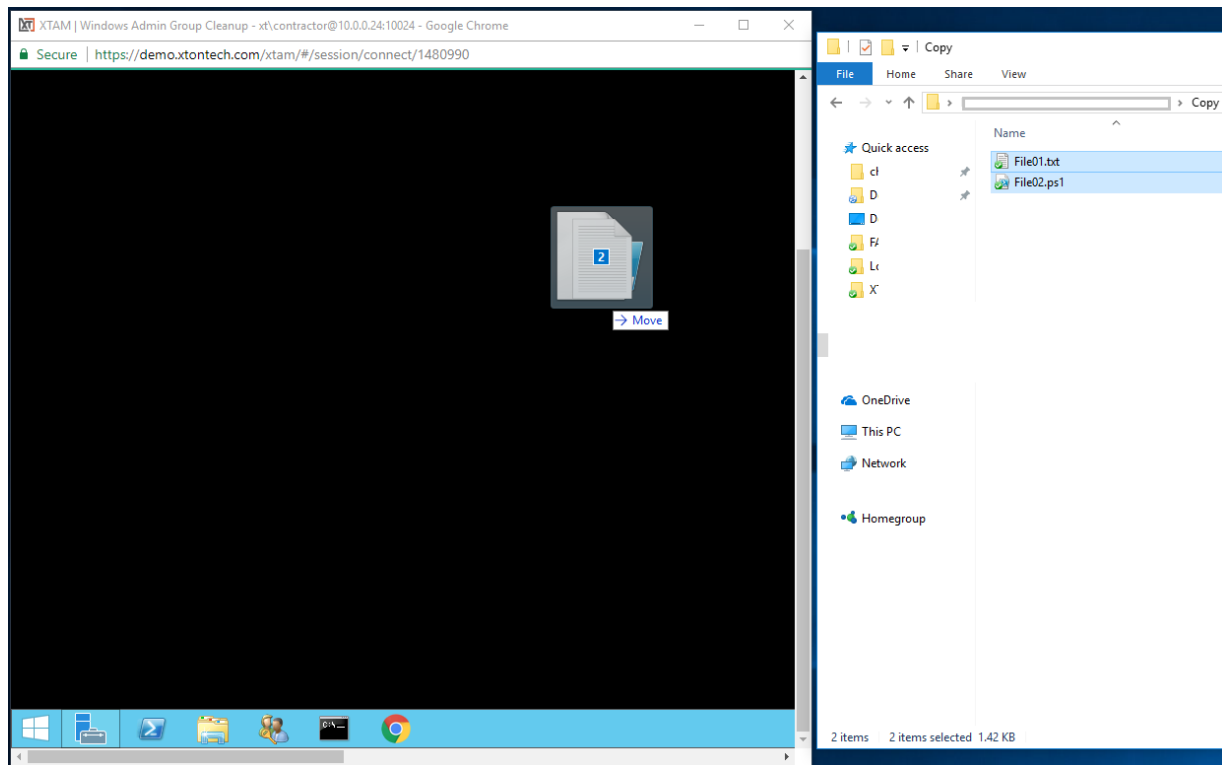
For clipboard or file copy, please see this [article](#).

To disable the ability to browse or transfer files during an in-browser session, click [here](#) for more information.

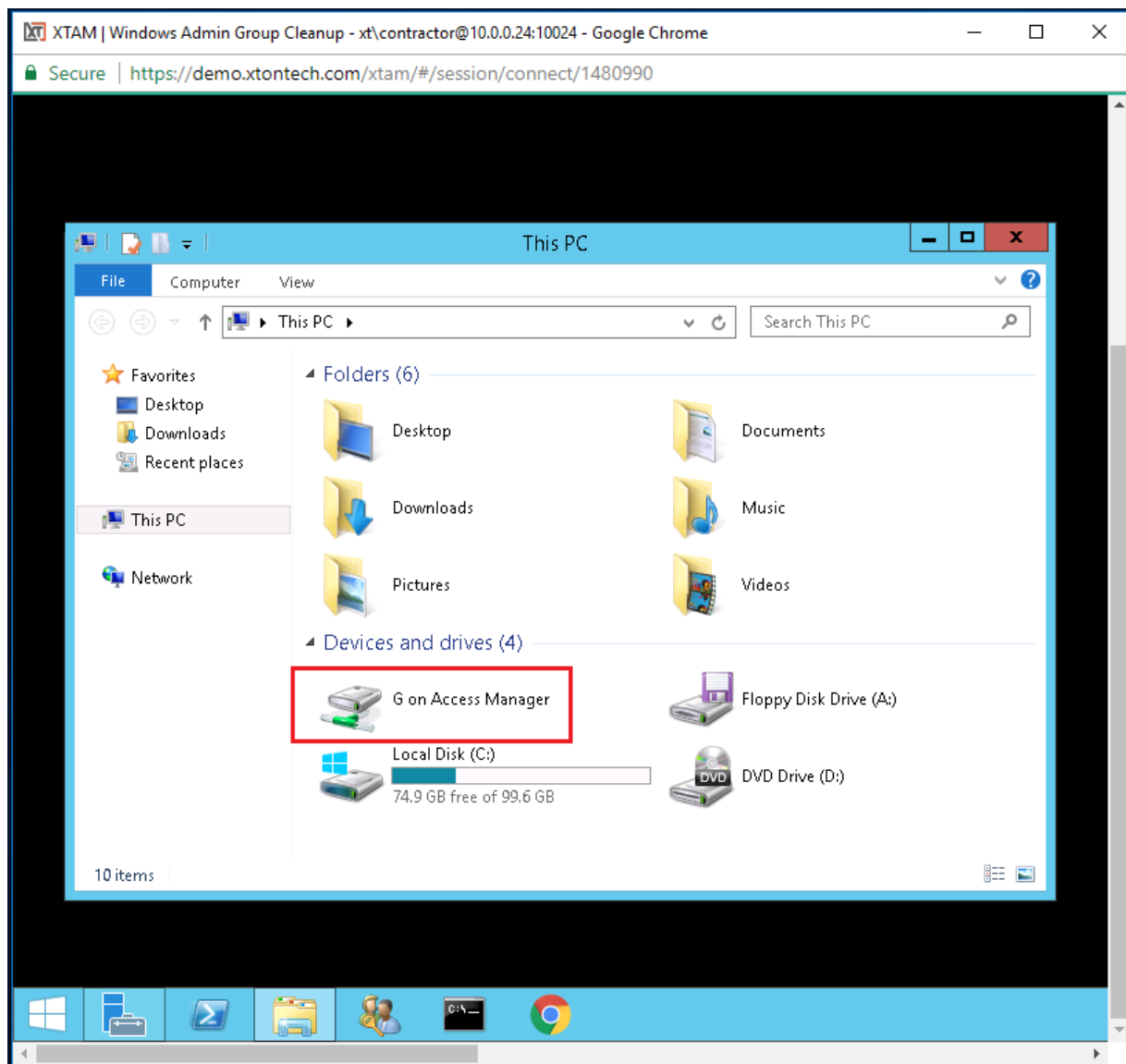
## In a Windows Remote Sessions

### To Copy Files in a Windows Remote Sessions:

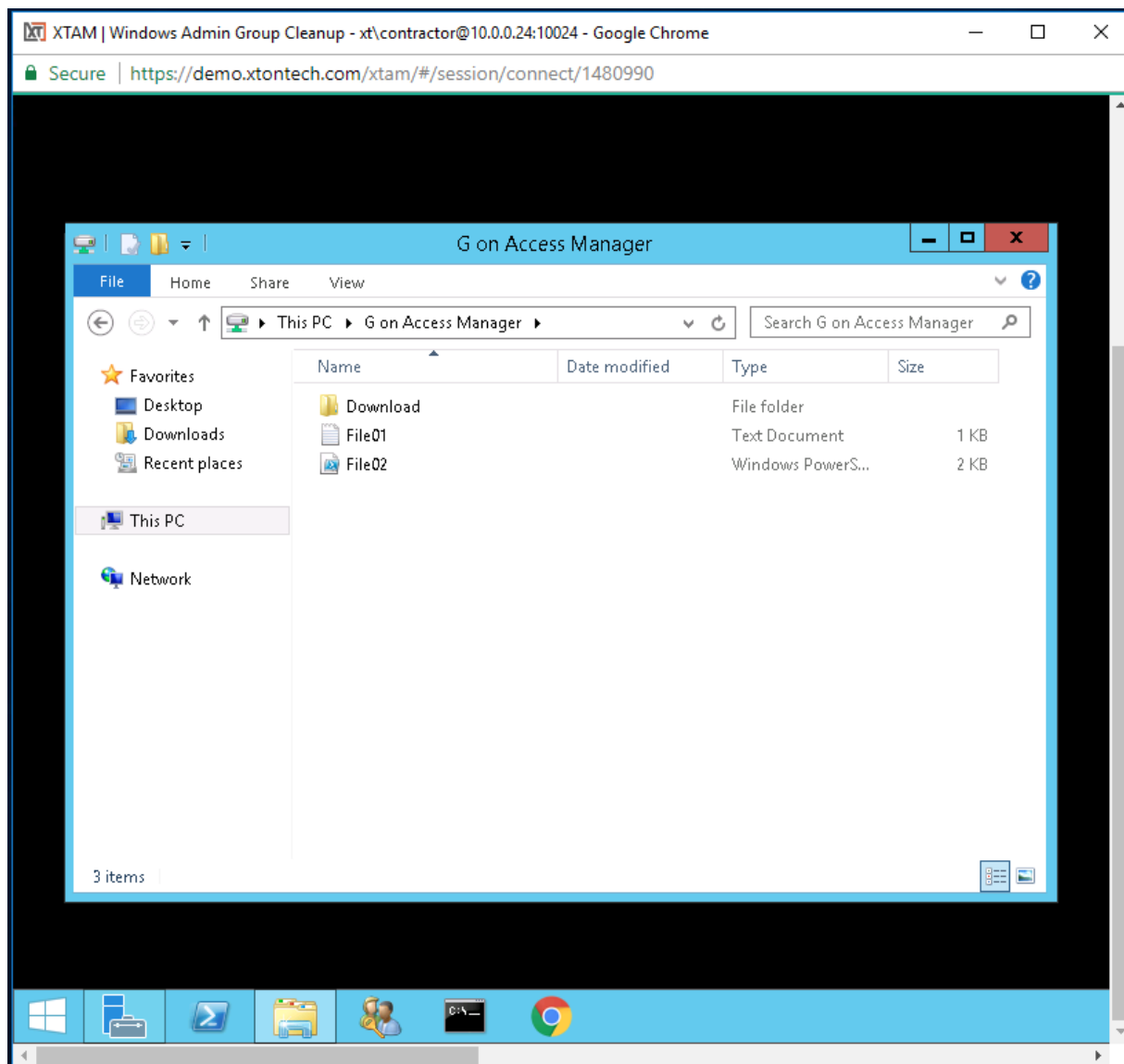
1. Connect to a Windows remote session.
2. From your local client, select the file(s) that you wish to copy to the remote host and drag those files into the browser tab or window where the remote session is running. *Folder copy is not currently supported.*



3. Drop the file(s) anywhere within the remote Windows host desktop.
4. The file(s) will immediately begin copying to the Windows host and upon completion they will be stored in the Privileged Access Management virtual drive G.



5. From this virtual G: drive, you can copy and paste the file(s) where needed on the remote host.

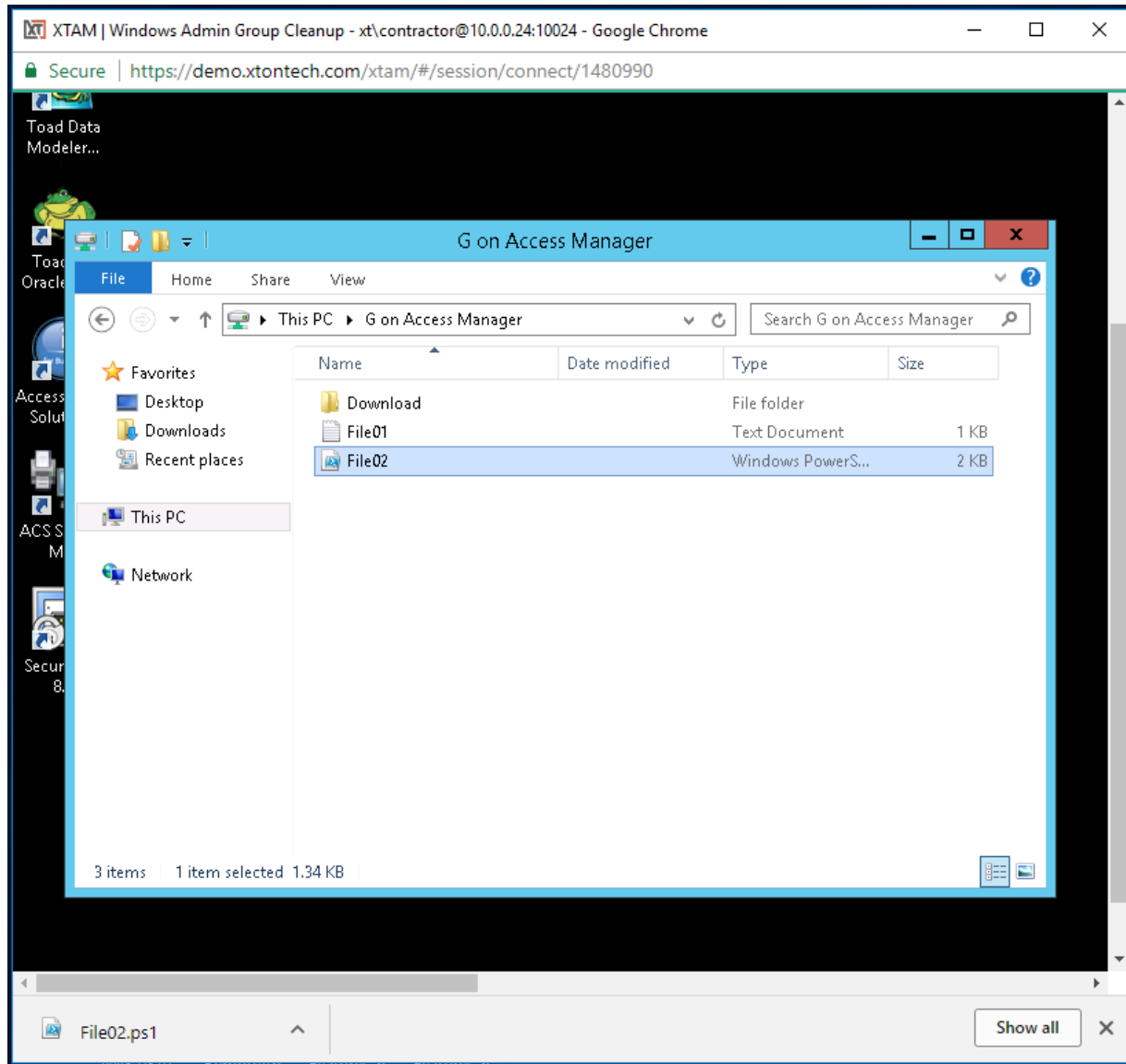


## Out of Windows Remote host

1. To copy files out of the Windows remote host, simply copy and paste the file (one at a time) from the remote host to the Download folder located in the Access Manager virtual drive **G:**.
2. Once the file has been copied to this **Download** folder, you will be prompted in your browser to download the file to your local computer.



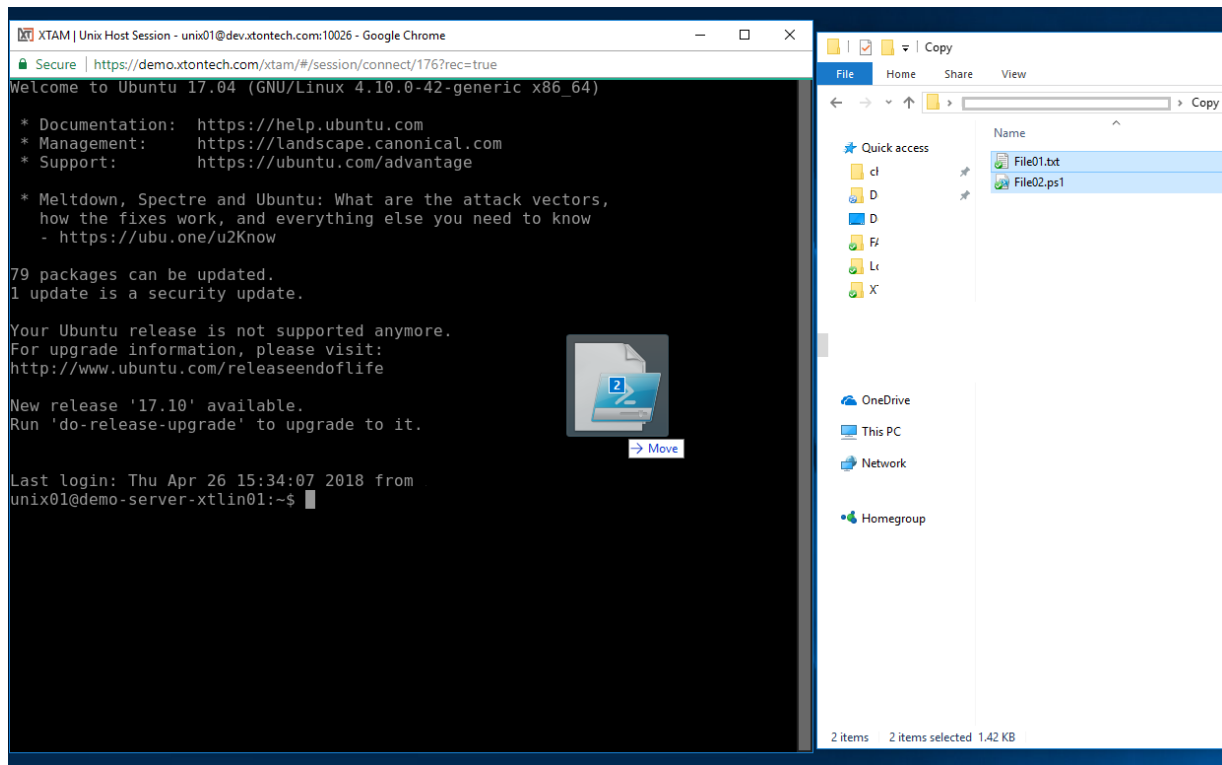
3. Accept the browser download prompt and the file will immediately begin copying to your local client.



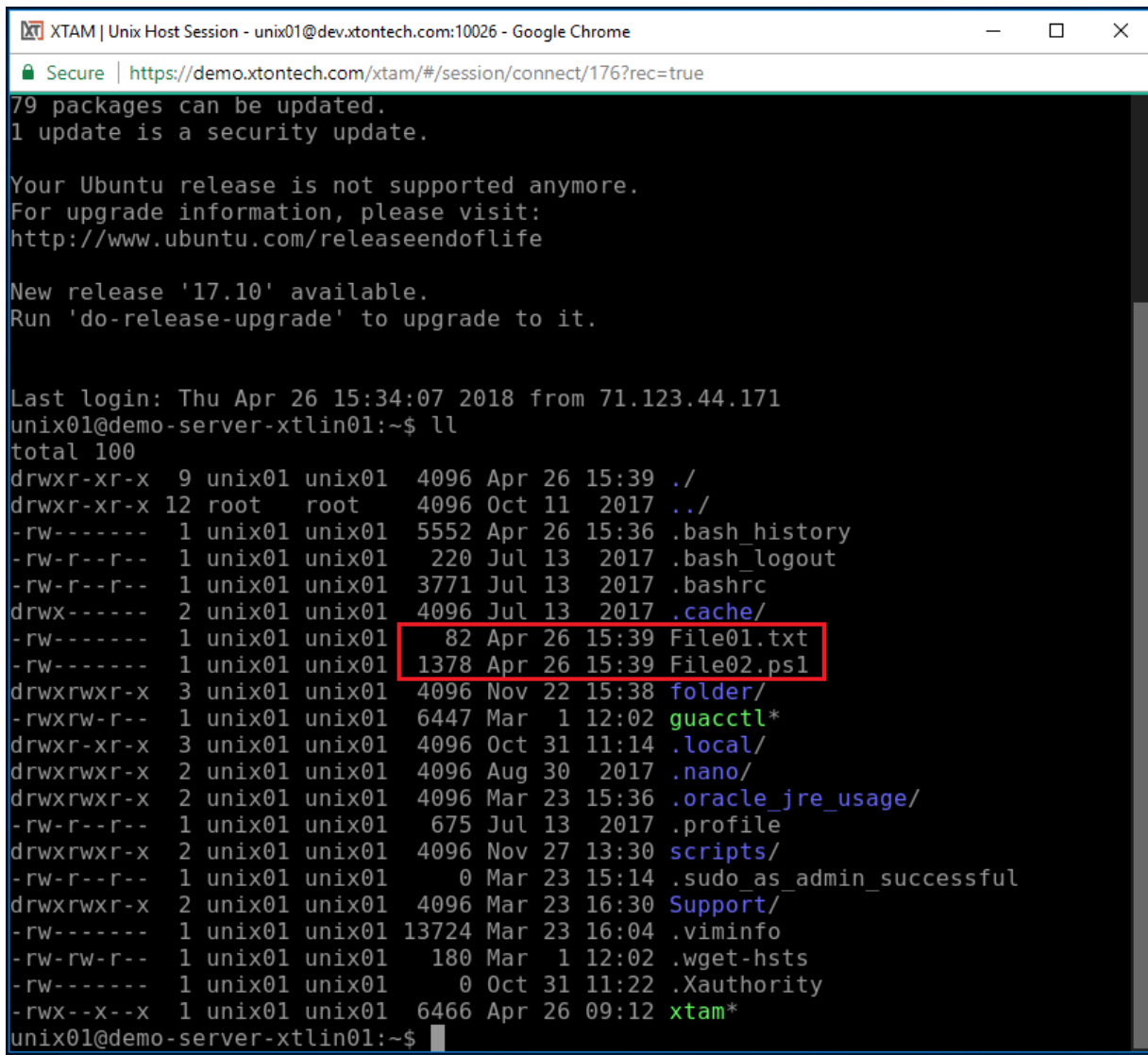
## In a Unix Remote Sessions

### To Copy Files in a Unix Remote Sessions:

1. Connect to a Unix remote session.
2. From your local client, select the file(s) that you wish to copy to the remote host and drag those files into the browser tab or window where the remote session is running. *Folder copy is not currently supported.*



3. Drop the file(s) anywhere within the remote Unix host session.
4. The file(s) will immediately begin copying to the Unix host and upon completion they will be stored in this user's Unix **Home** directory.



```
XTAM | Unix Host Session - unix01@dev.xtontech.com:10026 - Google Chrome
Secure | https://demo.xtontech.com/xtam/#/session/connect/176?rec=true

79 packages can be updated.
1 update is a security update.

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

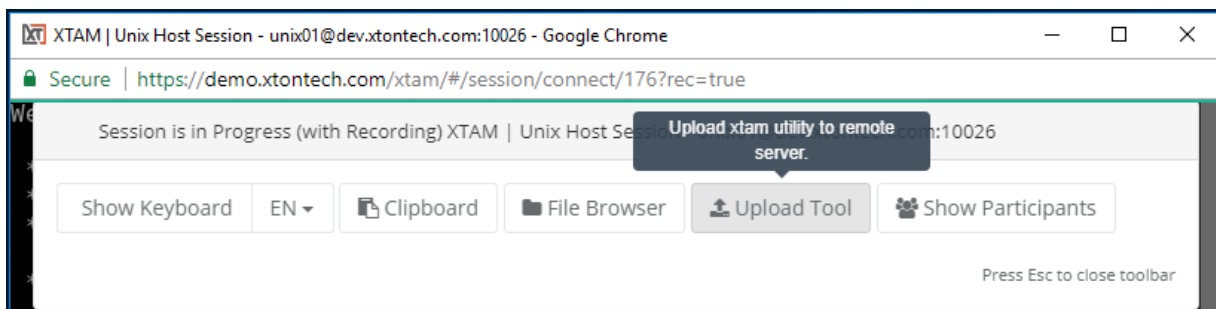
New release '17.10' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Apr 26 15:34:07 2018 from 71.123.44.171
unix01@demo-server-xtlin01:~$ ll
total 100
drwxr-xr-x  9 unix01 unix01  4096 Apr 26 15:39 ./
drwxr-xr-x 12 root    root    4096 Oct 11  2017 ../
-rw-r----- 1 unix01 unix01  5552 Apr 26 15:36 .bash_history
-rw-r----- 1 unix01 unix01   220 Jul 13  2017 .bash_logout
-rw-r----- 1 unix01 unix01  3771 Jul 13  2017 .bashrc
drwx----- 2 unix01 unix01  4096 Jul 13  2017 .cache/
-rw-r----- 1 unix01 unix01    82 Apr 26 15:39 File01.txt
-rw-r----- 1 unix01 unix01  1378 Apr 26 15:39 File02.ps1
drwxrwxr-x  3 unix01 unix01  4096 Nov 22 15:38 folder/
-rwxrwxr-x  1 unix01 unix01  6447 Mar  1 12:02 guacctl*
drwxr-xr-x  3 unix01 unix01  4096 Oct 31 11:14 .local/
drwxrwxr-x  2 unix01 unix01  4096 Aug 30  2017 .nano/
drwxrwxr-x  2 unix01 unix01  4096 Mar 23 15:36 .oracle_jre_usage/
-rw-r----- 1 unix01 unix01   675 Jul 13  2017 .profile
drwxrwxr-x  2 unix01 unix01  4096 Nov 27 13:30 scripts/
-rw-r----- 1 unix01 unix01     0 Mar 23 15:14 .sudo_as_admin_successful
drwxrwxr-x  2 unix01 unix01  4096 Mar 23 16:30 Support/
-rw-r----- 1 unix01 unix01 13724 Mar 23 16:04 .viminfo
-rw-rwxr-x  1 unix01 unix01   180 Mar  1 12:02 .wget-hsts
-rw-r----- 1 unix01 unix01     0 Oct 31 11:22 .Xauthority
-rwx--x--x  1 unix01 unix01  6466 Apr 26 09:12 xtam*
unix01@demo-server-xtlin01:~$
```

5. From this Home directory, you can copy and paste the file(s) where needed on the remote host.

## Out of the Unix remote host

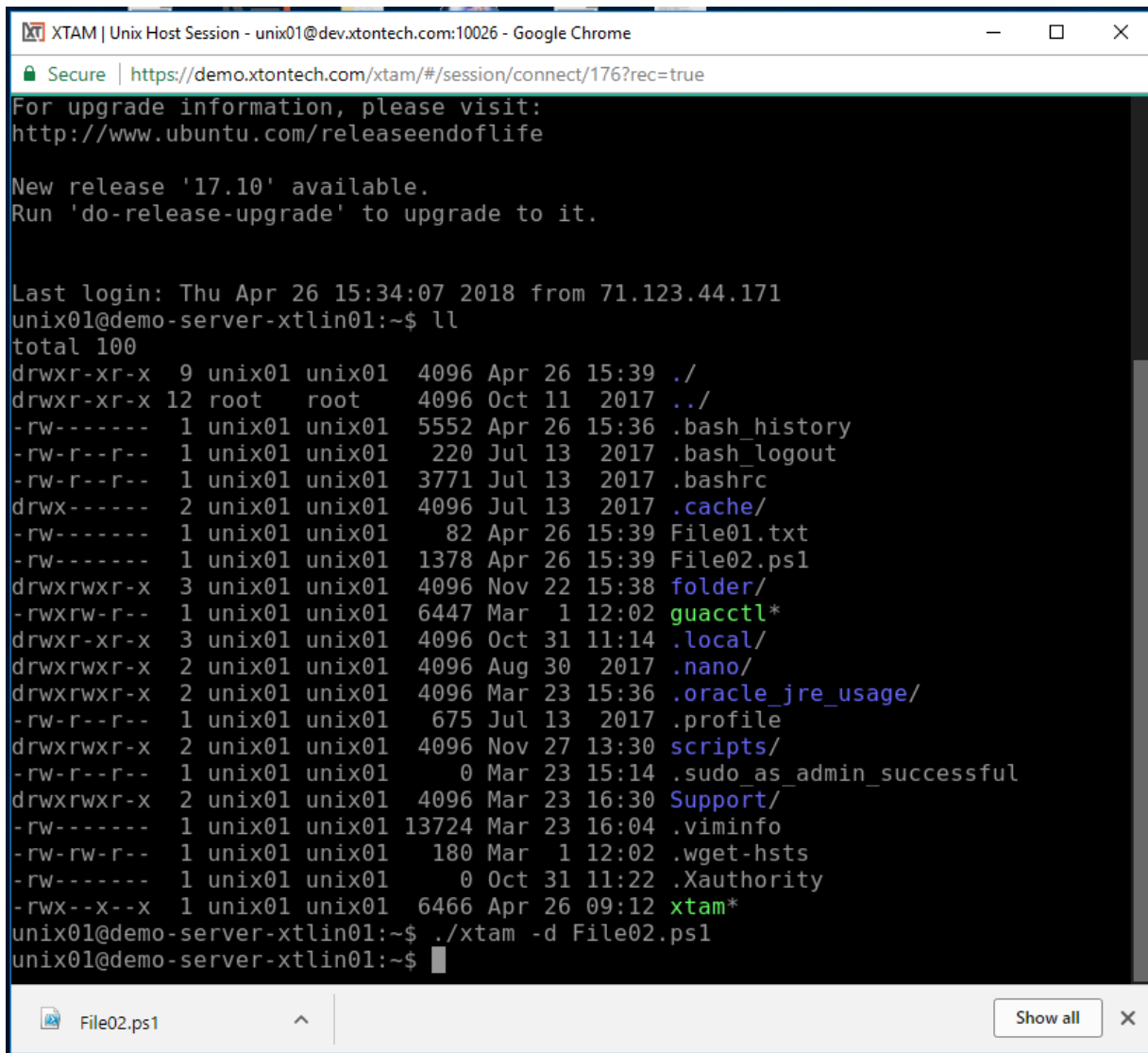
1. To copy files out of the Unix remote host, select the **Upload Tool** option from the remote sessions Quick Menu located at the top of the session. This will deploy an PAM command utility to the user's Unix Home directory.



2. Once the PAM utility is deployed, you can execute the copy by issuing this command:

```
1 | ./xtam -d filename # Name of the file to copy from the Unix host to your
   | local client
```

3. You will then be prompted by your browser to download the file. Accept the browser download prompt and the file(s) will immediately begin copying to your local client.



The screenshot shows a Google Chrome browser window titled "XTAM | Unix Host Session - unix01@dev.xtontech.com:10026". The address bar shows a secure connection to <https://demo.xtontech.com/xtam/#/session/connect/176?rec=true>. The main content area displays a terminal window with the following text:

```
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '17.10' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Apr 26 15:34:07 2018 from 71.123.44.171
unix01@demo-server-xtlin01:~$ ll
total 100
drwxr-xr-x  9 unix01 unix01  4096 Apr 26 15:39 ./
drwxr-xr-x 12 root   root   4096 Oct 11  2017 ../
-rw-r----- 1 unix01 unix01  5552 Apr 26 15:36 .bash_history
-rw-r--r--  1 unix01 unix01   220 Jul 13  2017 .bash_logout
-rw-r--r--  1 unix01 unix01  3771 Jul 13  2017 .bashrc
drwx----- 2 unix01 unix01  4096 Jul 13  2017 .cache/
-rw-r----- 1 unix01 unix01    82 Apr 26 15:39 File01.txt
-rw-r----- 1 unix01 unix01  1378 Apr 26 15:39 File02.ps1
drwxrwxr-x  3 unix01 unix01  4096 Nov 22 15:38 folder/
-rwxrw-r--  1 unix01 unix01  6447 Mar  1 12:02 guacctl*
drwxr-xr-x  3 unix01 unix01  4096 Oct 31 11:14 .local/
drwxrwxr-x  2 unix01 unix01  4096 Aug 30  2017 .nano/
drwxrwxr-x  2 unix01 unix01  4096 Mar 23 15:36 .oracle_jre_usage/
-rw-r--r--  1 unix01 unix01   675 Jul 13  2017 .profile
drwxrwxr-x  2 unix01 unix01  4096 Nov 27 13:30 scripts/
-rw-r--r--  1 unix01 unix01     0 Mar 23 15:14 .sudo_as_admin_successful
drwxrwxr-x  2 unix01 unix01  4096 Mar 23 16:30 Support/
-rw-r----- 1 unix01 unix01 13724 Mar 23 16:04 .viminfo
-rw-rw-r--  1 unix01 unix01   180 Mar  1 12:02 wget-hsts
-rw-r----- 1 unix01 unix01     0 Oct 31 11:22 .Xauthority
-rwx--x--x  1 unix01 unix01  6466 Apr 26 09:12 xtam*
unix01@demo-server-xtlin01:~$ ./xtam -d File02.ps1
unix01@demo-server-xtlin01:~$
```

At the bottom of the browser window, a download bar is visible showing a file icon, the name "File02.ps1", an upward arrow, and a "Show all" button with a close icon.

To maintain proper line formatting, ASCII Mode is supported in cases where files are transferred from remote Unix session hosts to Windows computers.

## File Copy Session Events

All files copied into or out of remote sessions will be captured via the Session Event log.

Using an account with the appropriate permissions, you can view these events using the following procedure.

1. Navigate to the specific Record and click the **Sessions** tab. Note that Events can also be found in the [Session Events report](#).
2. Active the Action menu associated to the Sessions and select the **Events** option.
3. Search, filter or sort by File Name of action (*FileUpload* indicates copying into and *FileDownload* indicates copying out of a session).

User	Start Time	End Time	Type	Preview	Action
Chris Kolodziejski (chrisk)	04/26/2018 15:28:44 ( +11m 25s )	04/26/2018 15:28:45 ( +11m 26s )	FileDownload	Filename: File02.ps1 MimeType: application/octet-stream Length: 1378	...
Chris Kolodziejski (chrisk)	04/26/2018 15:28:40 ( +11m 21s )	04/26/2018 15:28:40 ( +11m 21s )	KeySequence	Ctrl+c	...
Chris Kolodziejski (chrisk)	04/26/2018 15:27:13 ( +9m 54s )	04/26/2018 15:27:14 ( +9m 55s )	FileDownload	Filename: File01.txt MimeType: application/octet-stream Length: 82	...
Chris Kolodziejski (chrisk)	04/26/2018 15:23:01 ( +5m 41s )	04/26/2018 15:23:01 ( +5m 42s )	FileListing	Path: /	...
Chris Kolodziejski (chrisk)	04/26/2018 15:23:01 ( +5m 41s )	04/26/2018 15:23:01 ( +5m 41s )	FileListing	Path: /	...
Chris Kolodziejski (chrisk)	04/26/2018 15:23:00 ( +5m 41s )	04/26/2018 15:23:01 ( +5m 41s )	FileUpload	Filename: File01.txt MimeType: text/plain Length: 82	...
Chris Kolodziejski (chrisk)	04/26/2018 15:23:00 ( +5m 41s )	04/26/2018 15:23:01 ( +5m 41s )	FileUpload	Filename: File02.ps1 MimeType: Length: 1378	...

## Disable Session

### Disable Session File Browsing and Transfer.

If you want to disable the ability to browse or transfer files during in-browser remote sessions, then please configure the option described below.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Parameters > Session File Transfer.
3. Select the Disabled option from the dropdown menu.
4. Click the **Save** button next to this option.

## Overwrite Session

### Overwrite Session File Browsing and Transfer on an Individual Record.

You can overwrite the global *Session File Transfer* option described above, to allow or disallow file transfer on individual records. Please configure this overwrite mechanism as detailed next.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Record Types, locate the Record Type that is used for your Record where you want to overwrite the global configuration. Click this Record Type's **Edit** button.
3. Within this Record Type's Edit page, click the **Add Field** button. Create a new custom field using the following parameters:
  - Field Type: **Choice**
  - Name: **FileTransfer**
  - Display Name: **File Transfer Control**
  - Values: **Use Global,Enabled,Disabled**
4. Click **Save** to save your new field.
5. Back on the Record Type Edit page, once again click **Save** to save the changes made to your Record Type.

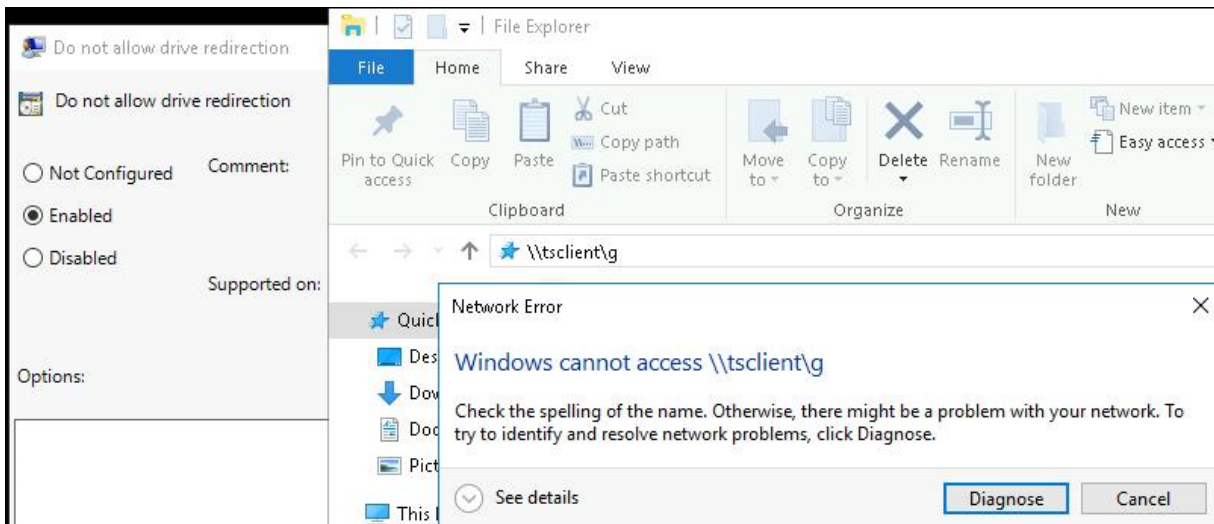
6. Now you can navigate to the Record itself that you want to enable this overwrite function, click the Record's **Edit** button and select the appropriate choice. The choices are:
  - **Use Global** (or no selection): This record will use the globally defined Session File Transfer configuration.
  - **Enabled**: This record will allow/enable Session File Transfers regardless of the globally defined Session File Transfer configuration.
  - **Disabled**: This record will not allow/disable Session File Transfers regardless of the globally defined Session File Transfer configuration.
7. After you have made the selection, click the **Save and Return** button to save your record.
8. Now you can test your record configuration by connecting to a new session.

## Troubleshooting: File transfer folder "G on Access Manager" (\\TSCLIENT\G) is not available

PAM has a Session File Transfer function. This allows for you to drag and drop files into the session. With RDP, the drag-and-dropped files appear in a drive shown as "G on Access Manager". This uses a UNC path of `\\TSCLIENT\G`.



Even though the File Transfer function is enabled, dragging and dropping a file does not result in this file being seen, and accessing the `\\TSCLIENT\G` location results in an error showing.



If G on Access Manager is not showing as a drive, try browsing to the share `\\TSCLIENT\G`. Also, having a mapped G: drive will not affect this share.

## Troubleshooting

- Run `rsop.msc` on the server the session connects to.
- Browse to that GPO setting and see what policy has this enabled.

- If the RDP file transfer is needed, this GPO setting would need to be changed to *Not Configured* or *Disabled* to allow the use of the *TSCLIENT* share.
- Your Domain Admins can look into this.

## File Transfer - Change Access Manager File Drive Letter and name

Can you change the drive letter for file transfer in PAM to an unused drive letter?

- The following values can be added to the `catalina.properties` file on each node found under `$PAM_HOME\web\conf`:

```
1 | xtam.session.web.rdp.drive.name=Access Manager
2 | xtam.session.web.rdp.drive.letter=X
```

- After saving the change restart the PAM Management service
- The above name will result in a drive showing up on RDP sessions as "X on Access Manager".

Additional information on [file transfer folder troubleshooting](#).

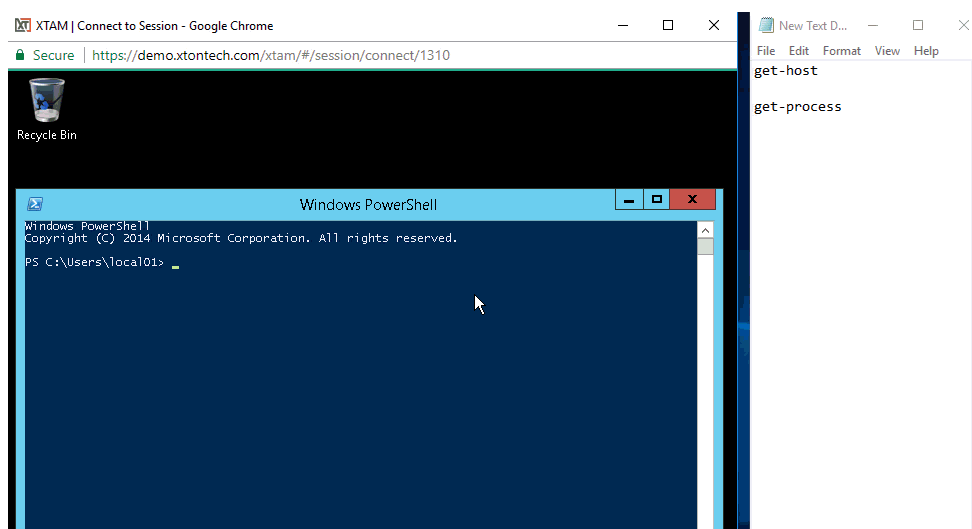
## Coping Files and Clipboard Text To and From Remote Sessions

PAM provides the ability to copy clipboard text and files between your local computer and remote sessions without needing to use FTP or other file transfer software.

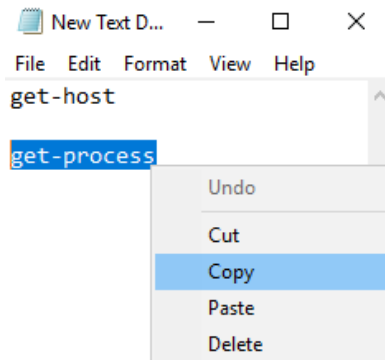
This also supports the transfer between Windows and Unix/Linux sessions Quick-File-Transfer and local computers.

### Clipboard text

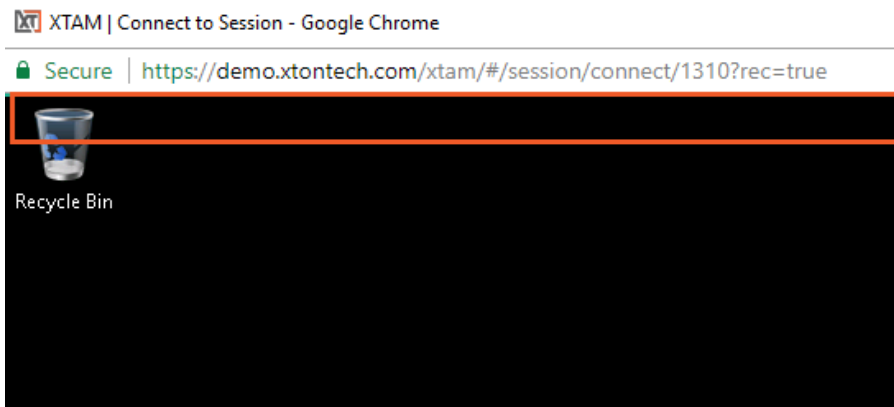
To copy clipboard text between a local computer and a remote session:



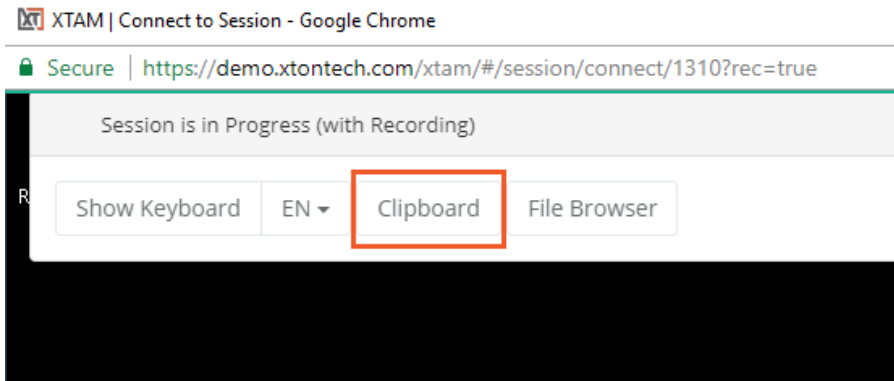
1. Select text from your local computer and **Copy** it to your clipboard.



2. In your Remote Session, hover your mouse pointer in the top 30 pixels of the remote session screen for at least one second.

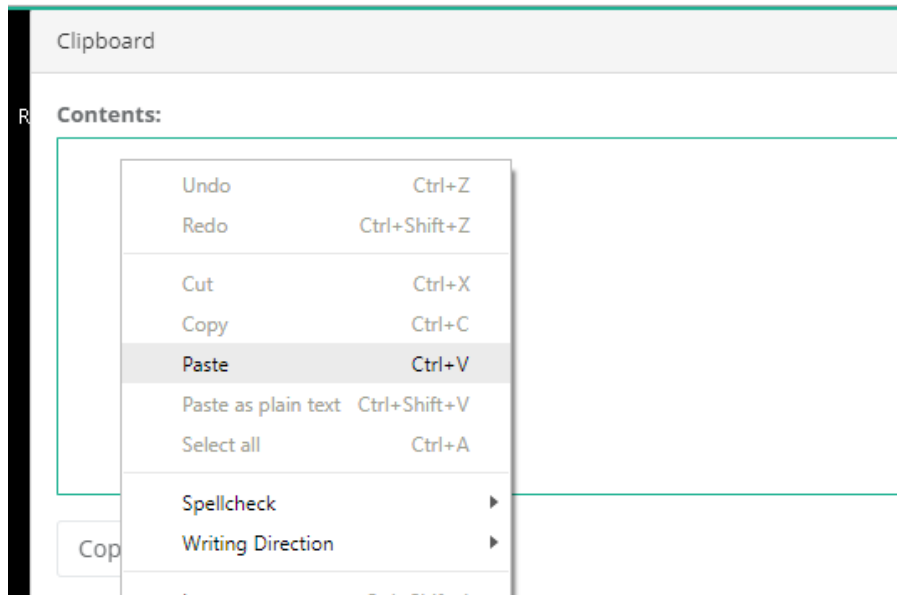


3. When the dropdown menu appears, click the **Clipboard** option.

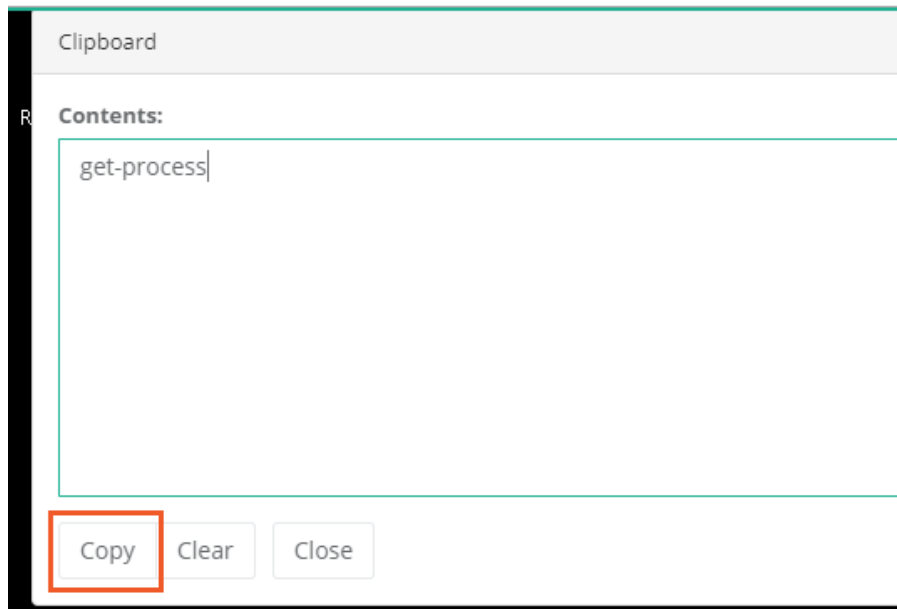


4. In the Clipboard field, right click and choose **Paste** or type text as needed.

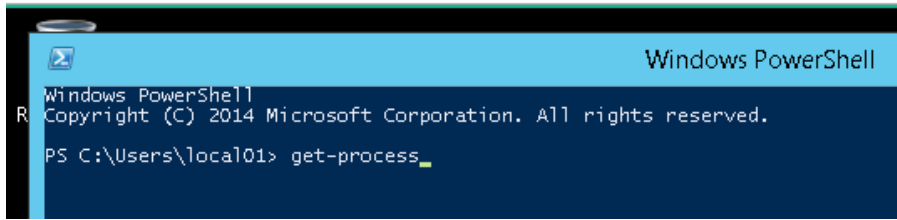




5. When you are ready to transfer the text to your Remote Session, click the **Copy** button.



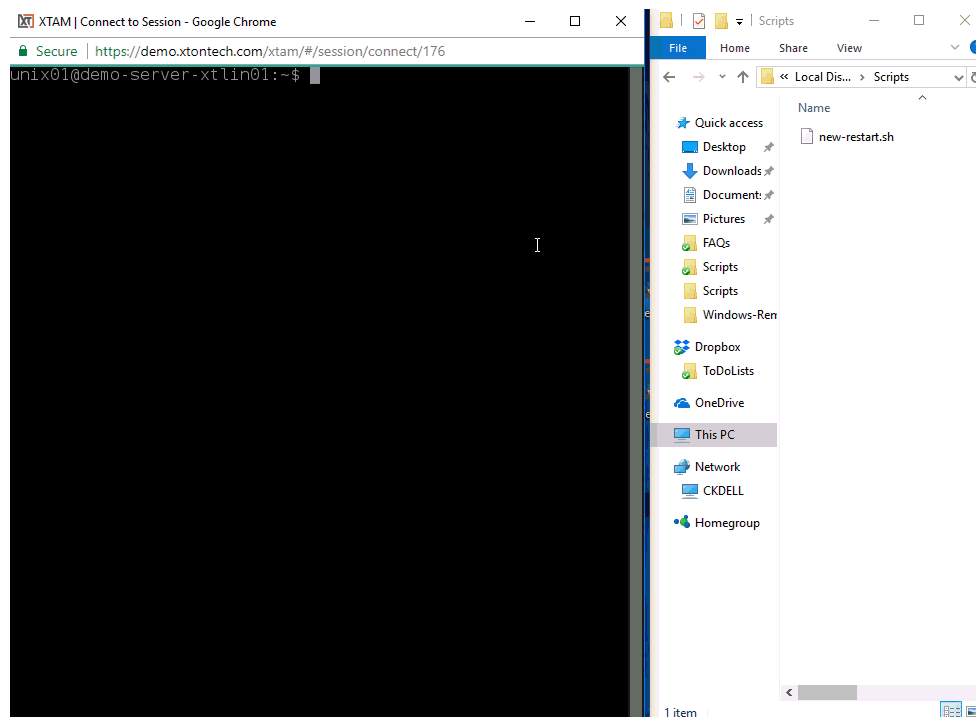
6. Back in your Remote Session, paste the text to complete the Clipboard transfer.



## Copy a file: local to remote

To copy a file from a local computer to a remote session:

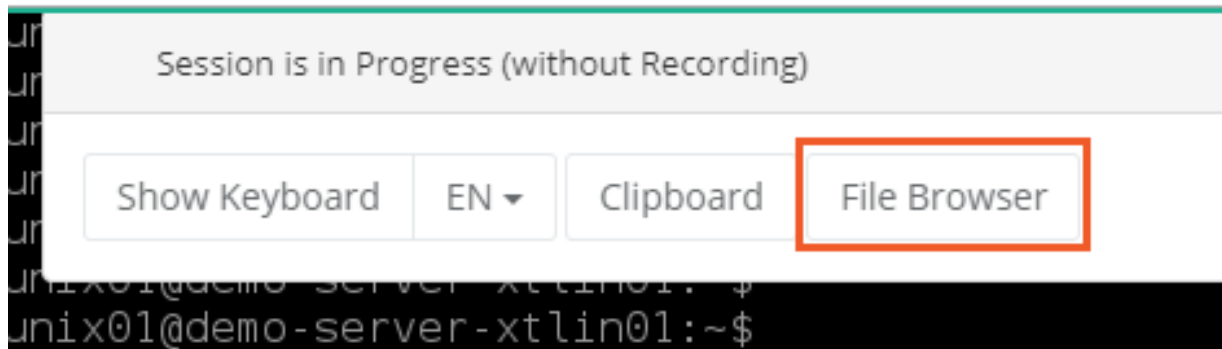
To disable the ability to browse or transfer files during an in-browser session, click [here](#) for more information.



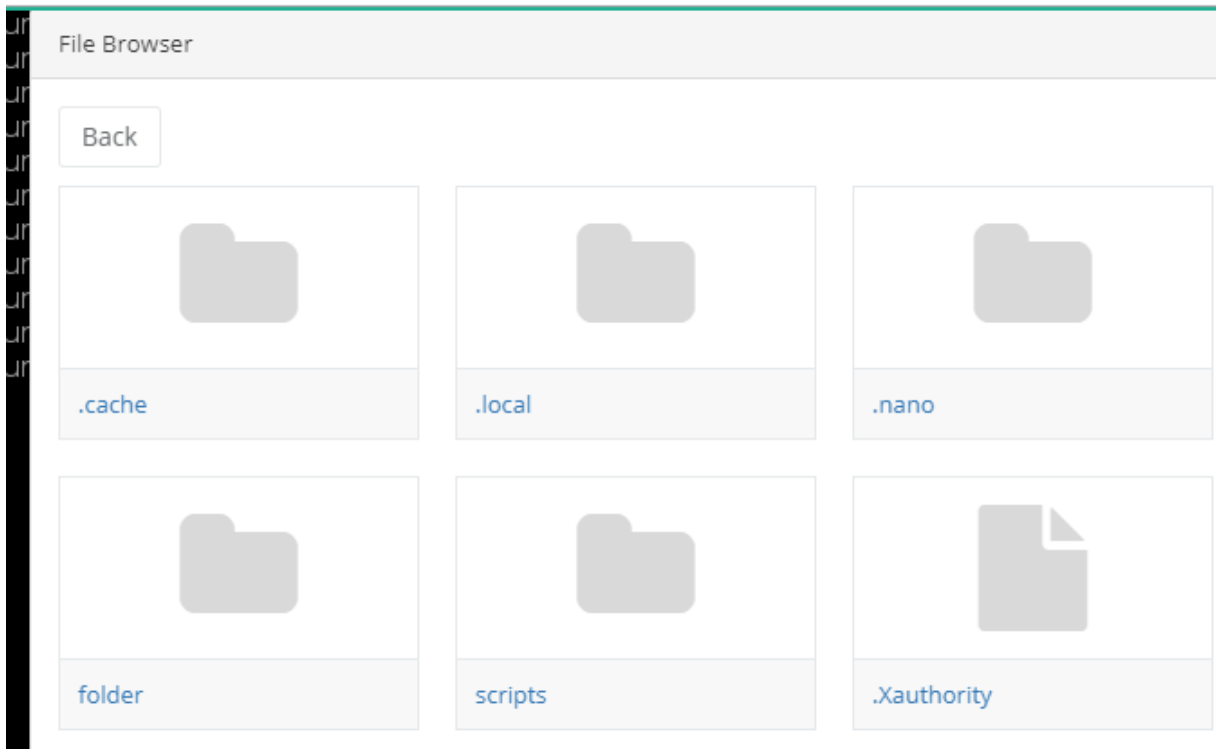
1. In your Remote Session, hover your mouse pointer in the top 30 pixels of the remote session screen for at least one second.

```
unix01@demo-server-xtlin01:~$  
unix01@demo-server-xtlin01:~$  
unix01@demo-server-xtlin01:~$  
unix01@demo-server-xtlin01:~$  
unix01@demo-server-xtlin01:~$  
unix01@demo-server-xtlin01:~$  
unix01@demo-server-xtlin01:~$  
unix01@demo-server-xtlin01:~$
```

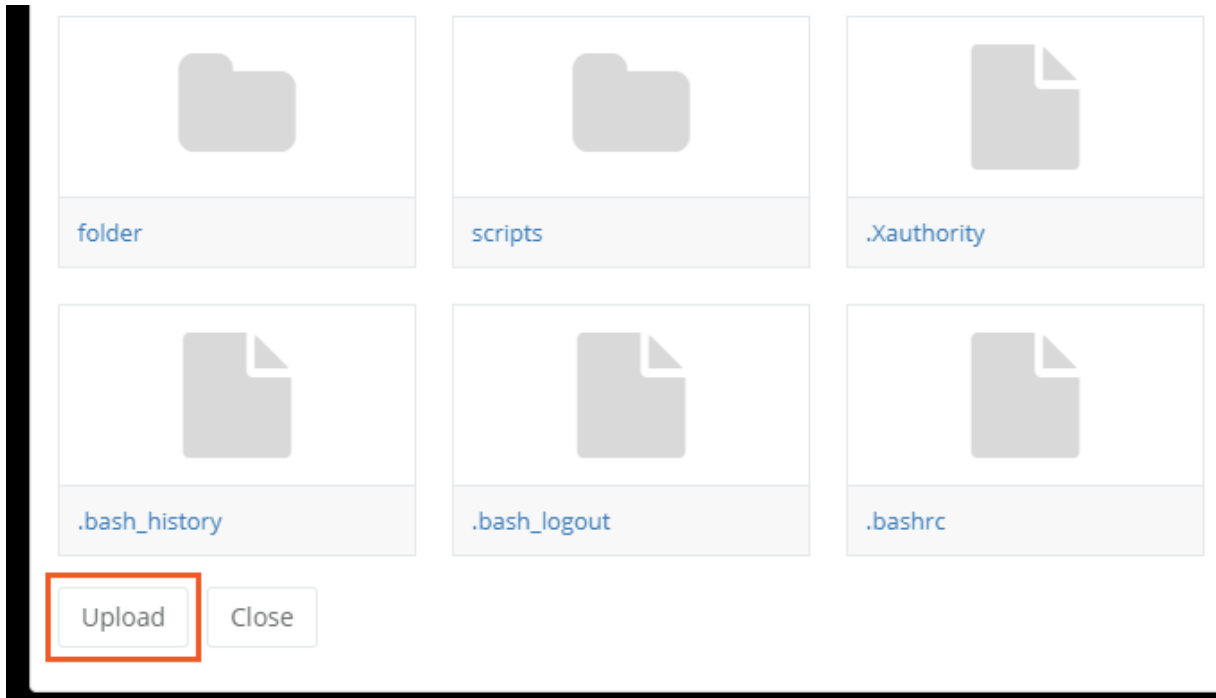
- When the dropdown menu appears, click the **File Browser** option.



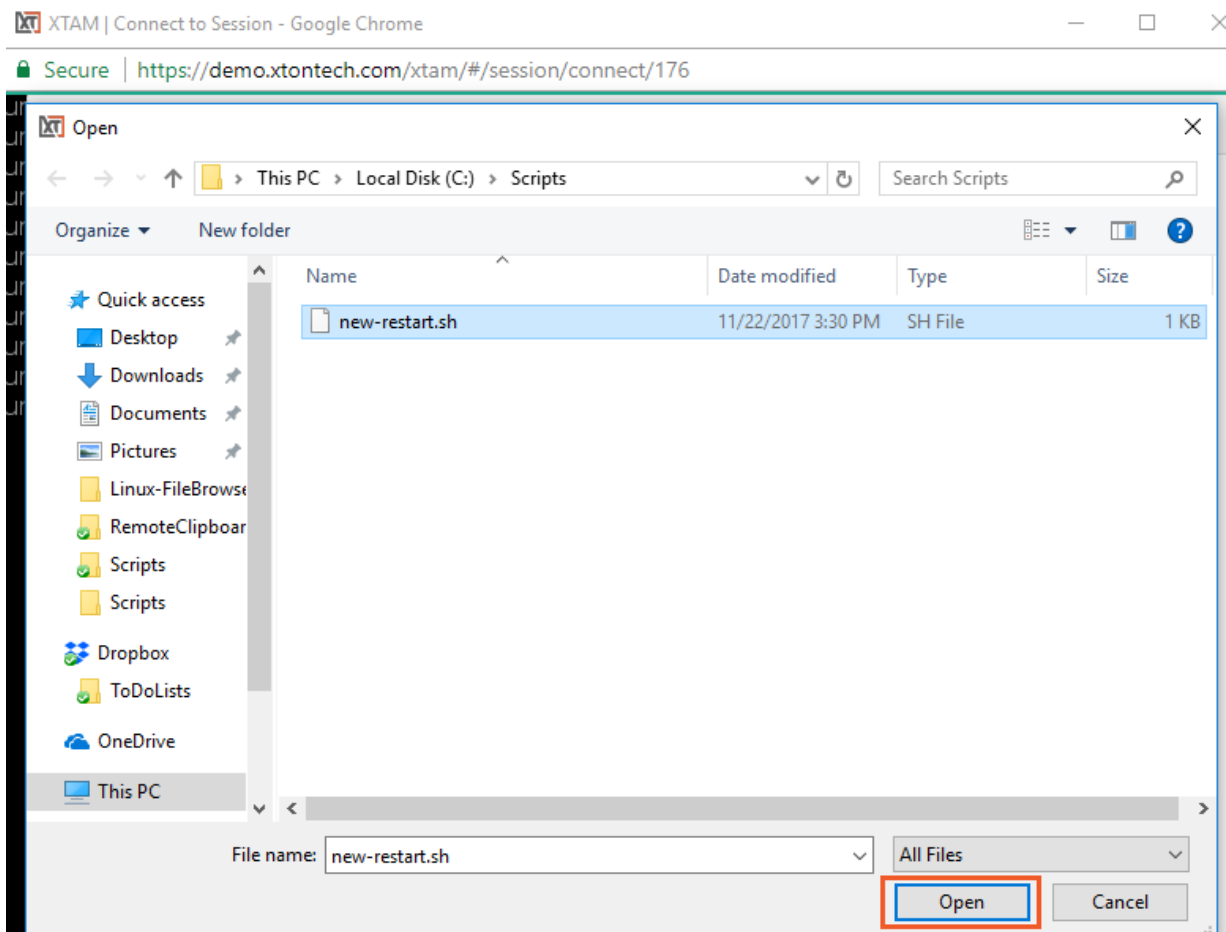
- Navigate to the target folder location where you wish to upload the file to on your Remote Host by clicking on each Folder.



4. Next, click the **Upload** button along the bottom of the dropdown menu.



5. When the File Selection dialog appears, locate and select your file. Click **Open** when ready.



6. The selected local file will now be uploaded to the target folder on your remote host.

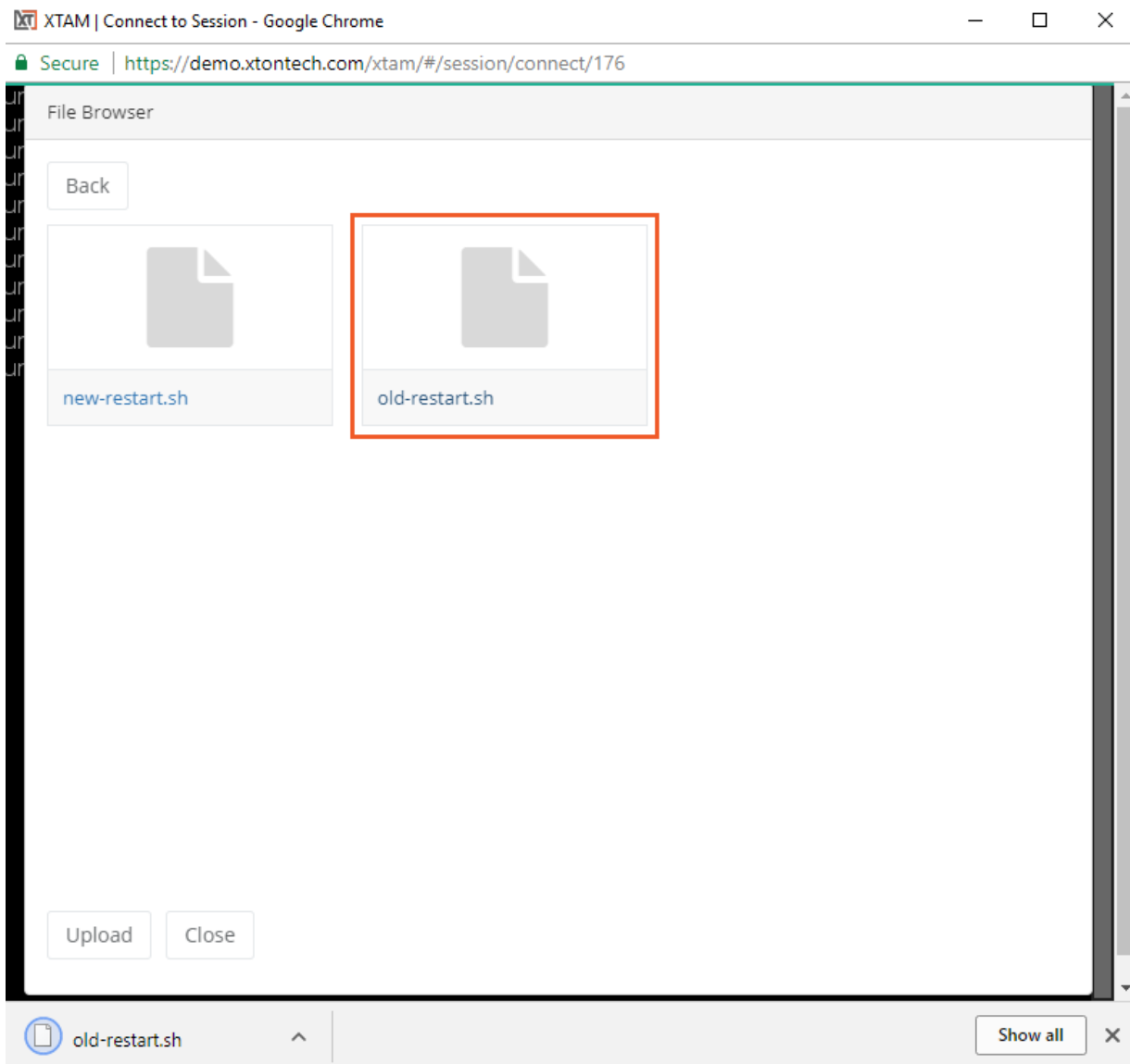
## Copy a file: remote to local

To copy a file from a remote session to a local computer:

To disable the ability to browse or transfer files during an in-browser session, click [here](#) for more information.

To maintain proper line formatting, ASCII Mode is supported in cases where files are transferred from remote Unix session hosts to Windows computers.

1. In your Remote Session, hover your mouse pointer in the top 30 pixels of the remote session screen for at least one second.
2. When the dropdown menu appears, click the **File Browser** option.
3. Locate the file you wish to copy from this Remote Host by navigating through its local folder structure by clicking on each file until the File is visible.
4. Once the file is located, simply click on it to begin the download process.



5. This file will be downloaded to your browser's default Download location on your local computer.

## Disable Session

### Disable Session File Browsing and Transfer.

If you want to disable the ability to browse or transfer files during in-browser remote sessions, then please configure the option described below.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Parameters > Session File Transfer.
3. Select the **Disabled** option from the dropdown menu.
4. Click the **Save** button next to this option.

## Overwrite Session

### Overwrite Session File Browsing and Transfer on an Individual Record.

You can overwrite the global *Session File Transfer* option described above, to allow or disallow file transfer on individual records. Please configure this overwrite mechanism as detailed next.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Record Types, locate the Record Type that is used for your Record where you want to overwrite the global configuration. Click this Record Type's **Edit** button.
3. Within this Record Type's Edit page, click the **Add Field** button. Create a new custom field using the following parameters
  - Field Type: **Choice**
  - Name: **FileTransfer**
  - Display Name: **File Transfer Control**
  - Values: **Use Global,Enabled,Disabled.**
4. Click **Save** to save your new field.
5. Back on the Record Type Edit page, once again click **Save** to save the changes made to your Record Type.
6. Now you can navigate to the Record itself that you want to enable this overwrite function, click the Record's **Edit** button and select the appropriate choice. The choices are:
  - **Use Global** (or no selection): This record will use the globally defined Session File Transfer configuration.
  - **Enabled**: This record will *allow/enable* Session File Transfers regardless of the globally defined Session File Transfer configuration.
  - **Disabled**: This record will not *allow/disable* Session File Transfers regardless of the globally defined Session File Transfer configuration.
7. After you have made the selection, click the **Save and Return** button to save your record.

Now you can test your record configuration by connecting to a new session.

## Connecting to a Windows Host

- Remote Windows desktop is displayed in the client browser directly using HTML5. There is no special software required on the client side including ActiveX, applets or anything else. The connection looks the same in any modern HTML5 browser on Windows or Linux desktop or mobile device. This approach simplifies deployment and maintenance of Privileged Access Management and provides better control over sessions.
- Privileged Access Management does not transmit the remote Windows account password to the client browser. The password is used by PAM server to connect to a remote Windows desktop.
- The session could be recorded to play back by administrators or auditors later.
- An auditor or an administrator might join or terminate the session while it is in progress.
- A user might open multiple sessions to different remote computers or devices at the same time.
- A user might be granted permissions to connect to a remote Windows computer with or without recording a session. In this case the user might choose the connection type. Alternatively, a user might be granted permissions to connect to a remote computer with session recording only. In this case the only **Connect** button would be available for the user on the PAM GUI.

## Resetting Privileged Passwords

Creating records, securing access and establishing sessions is a great first step to securing your privileged accounts.

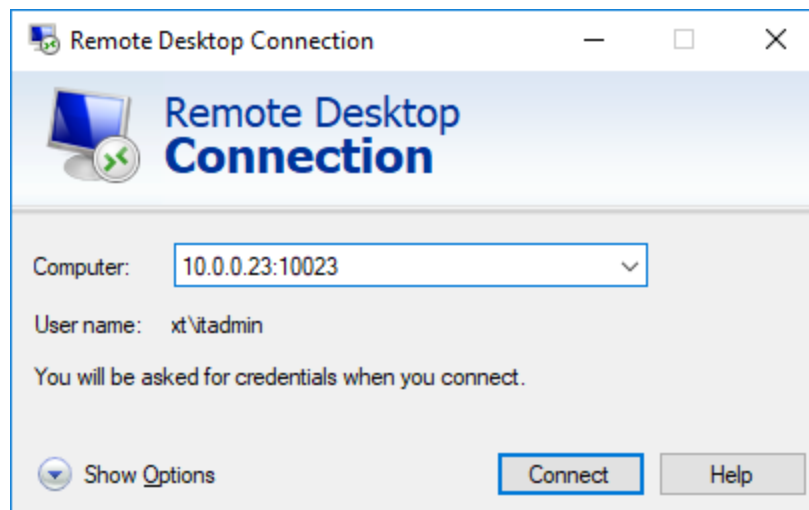
We are now going to take it one step further and introduce the concept of automated (or on demand) password resets.

This functionality takes security another step forward because it allows PAM to not only secure accounts but to also update their passwords in cases where events or triggers occurred.

In this section, we will configure and run an example of on demand password reset. Because we will be resetting an account password, it is highly recommended to use a test account for this exercise. If you do use an alternate test account, please be sure to update your “Production Web Server” record in PAM with this test account’s user and password.

To start and eventually validate the results, let’s establish a baseline use case.

1. Outside of PAM, open a standard Remote Desktop session and connect to the Windows host we have been using in our “*Production Web Server*” record.
2. When prompted, enter the user and password of your test account.
3. Ensure that Remote Desktop connects successfully.
4. **Sign out and close** Remote Desktop.



RDP Baseline Test Connection

Before we continue with the password reset exercise, we will take a few moments to examine the components that can be configured to execute this or other jobs in PAM.

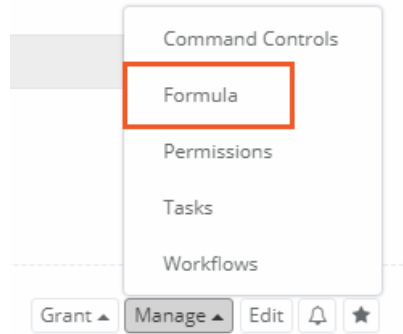
## Password Formulas

Formulas are configured to determine the strength and complexity of an automated or on demand password. It is here that you can configure password complexity to include such options as character length, include upper or lower case, numbers or special characters as well as history. To open and configure a formula:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
  - a. If you still have it in your Favorites, then you can click **<IT Records>** in your left navigation menu for quick access to this folder.



2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate and click the Manage >**Formula** button along the bottom of the record view.



Formula Button

4. The *Password Formula* page will load and display the default configuration. It is here where changes to this configuration can be made, but first we must decide if we want to change the inherited Formula (default) or to make it unique to this object and then change it as needed.
  - a. To learn more about inheritance throughout PAM, please read about [Inheritance](#).
5. For this exercise, we are going to make this Formula unique to this record. Continue by clicking the **Make Unique** button and then accepting the message that appears. The Formula will refresh and it is now unique to this record only.
6. Now we can change the Formula without it affecting any other records in the system.
  - a. Change the following settings or create your own:
    - i. *Minimum Password Length*: 25
    - ii. *Maximum Password Length*: 30

## Password Formula for Production Web Server

Inherit from Parent

Save



Minimum Password Length

25

Maximum Password Length

30

Minimum Number of Upper Case Characters

5

Minimum Number of Lower Case Characters

5

Minimum Number of Numeric Characters

5

Minimum Number of Special Characters

5

!@#\$%^&\*()\_+<>?:~=-{}[]

Minimum Number of Whitespace Characters

0

Forbid Using User Name

☐

### Creating a Unique Formula

- Click **Save**.
- Click your browser's **Back** button to return to the record.

The Formula is customized and has been saved to this record only (*made unique*).

## Record Tasks

A Record's Task consists of two elements, a Script and a Policy.

The Script component is what will be executed against the record (password reset or custom written) and the Policy is when it will be executed. In our example, we will be executing the default "out of the box" Password Reset script for our Windows Host record type.

Since this task is already available for our Windows Host record type (via inheritance), we do not have to make any changes, we can simply proceed to the next component in our Task which is the Policy.

[Inherit from Parent](#) [Add Task](#) [Save](#) [↺](#)

Shadow Account



Time Window

---

Script	Policy	Actions
Password Reset Remote Windows	On demand	

## Record Task View

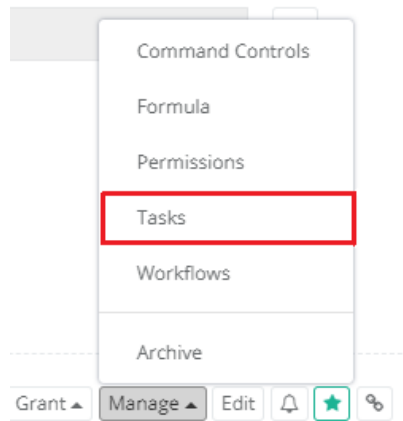
## Record Policies

The next area of job execution is the schedule or trigger that causes the script execution which are called Policies.

This can be associated to specific events detected on a record like an edit operation, it could be a trigger on a specific day or it can be configured as an “on demand” action.

To access the Policies:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
  - a. If you still have it in your Favorites, then you can click **<IT Records>** in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate and click the Manage **>Tasks** button along the bottom of the record view.



### Tasks Button

4. The Tasks page will load and display the default configuration. It is here where changes to this configuration can be made, but first we must decide if we want to change the inherited Policy or to make it unique to this object and then change it as needed.
  - To learn more about inheritance throughout PAM, please review [What is Inheritance?](#) article.
5. For this exercise, we will be executing the Password Reset Task using the Policy “On demand” and because the inherited default policy already includes this option we will not be making it unique like we did with the Formula. However, if you want to experiment with a unique Policy, click **Make Unique** and customize as needed by using the **Edit Policy** option located in the *Actions* menu. To continue along with this exercise, be sure “On demand” is enabled and the Task is saved.

**Script** Password Reset Remote Windows

**Target Record** Record Itself

**Event**

- ☐ After Approval
- ☒ After creating or updating a record
- ☐ After Expire
- ☐ After Check-In
- ☐ After Session ☐ Check to defer execution until completion of the last active session
- ☐  minutes after unlock
- ☐ Every  th day of each month
- ☐ Every
- ☒ On Demand
- ☐ Every  th day
- ☐ Every  to  days

### Unique Policy on Task

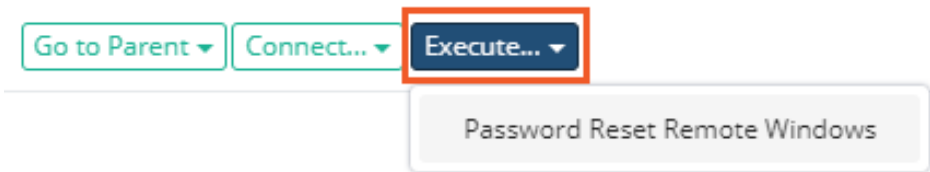
6. Click your browser's **Back** button to return to the record.

Our task already included the On Demand policy option, so we are going to continue without making any changes to it.

## Password Resetting

We have configured our basic password reset job (more complex formula and on demand policy in our task), so our next step is to run it. To run this password reset job:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
  - a. If you still have it in your Favorites, then you can click **<IT Records>** in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate and click the **Execute** button along the top of the record view and then select our *Password Reset* task.



#### Execute Password Reset

4. The Schedule Job page will now display. Before we continue, let's look at the information and options on this page.
  - a. Along the top, an automatically generated password will appear in the Password field that satisfies the formula we defined earlier. If you were to continue now, the password displayed in this field will become the new password for the account associated to this record when the reset job completes.
  - b. You can click the **Generate** button to its right to cycle through randomly generated passwords that also satisfy the formula.
  - c. You can also manually type in a password if you prefer but it must satisfy the formula rules before you can continue. Use the **Validate** button to ensure your password meets these requirements and adjust as necessary.

Schedule Job for Production Web Server Cancel Schedule Job

Password 
Validate Generate

Formula Rules

- Lowercase : 5
- Max : 30
- Min : 25
- Numbers : 5
- SpecialCharacters : 5
- Uppercase : 5

#### Password Generation

5. When you are happy with the password, click **Schedule Job** to execute the reset.
  - a. On demand jobs like this will be immediately added to the Job Queue and processed based on availability and PAM's queue. In this newly installed system, this job should begin processing almost immediately.
6. The system will navigate you back to the record's View page. The **Job Queue** field will show that the job has been generated and set to process.

Job Queue: [\(click to refresh\)](#)  
 ● 07/25/2017 11:47, OnDemand, generated

#### Record's Job Queue

7. Locate and click the **Job History** button. It will be in this view where you can view information about any currently running or scheduled jobs associated to this record.

### Job History Button

8. You will see our “On Demand” job displayed with a specific state. Navigate around the page to explore the options that are available for Job History and after a minute or two, click **Refresh**.
9. When the job completes, the **State** will be shown as “Completed”.

**Job History** (Production Web Server)

---

Found 1 queue records. Refresh

Show  entries Search:

Copy CSV Excel PDF Print

Showing 1 to 1 of 1 entries

Time	Type	Object	Task	State	
07/25/2017 11:47	OnDemand	Production Web Server	Password Reset Remote Windows	Completed	<a href="#">Details</a>

Previous 1 Next

### Job History Completed

The password reset job is now complete, but we need to validate our results before we continue.

To do this, let’s repeat our baseline test from the beginning of this section.

Outside of PAM, open your Remote Desktop session and attempt to connect using the original test account’s user and password.

Now, unlike earlier, you should fail to connect because either the username or password is wrong. We know it is the password because we just changed it.

At this point in the exercise, we have totally secured this connection.

The only way to connect to this host is by using a secure privileged session in PAM because the password to the account is not known to anyone besides the system.

With that stated, there are very valid reasons when the password must be shown or shared between users, so you are still able to expose (unlock) it when needed.

The process is quite simple and we demonstrate that now.

## Password Unlocking

Unlocking a password is the act of exposing a password to the user of PAM.

A couple of points to highlight before we begin the exercise:

- The user must be granted the appropriate permission to unlock a password. Permissions will be discussed in the next section.
- Secured passwords are never stored on any client computer. Passwords remain secured in the database of secrets until and only when they are required. In this example, the user requests an unlock and it is delivered to their browser where it is stored temporarily for this browser session only.
- All password *Lock* and *Unlock* events are captured in PAM’s Audit Log.

Now let's try out a password unlock. Using our recently password reset "Production Web Server" record as our example, to unlock a password:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
  - a. If you still have it in your Favorites, then you can click **<IT Records>** in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate the Password field. To its right, click the **Unlock** button.

Password

\*\*\*\*\*

Password Locked

Password

(Unlocked. Please use Show Password or Copy to Clipboard Button.)

Password Unlocked

4. Once Unlocked, you can click the **Show** button to display the password in the field or click the **Copy** button to copy the password to your clipboard.
5. After unlocking with the **Show** button, **NATO Phonetic Alphabet** appears to show the password for transmitting over the phone or retyping the password to the other location.

Type

VNC Host

Host

192.168.1.50

Port

5901

Password

E0Lp2yQ3X00JpGjhP

E - ECHO  
O - OSCAR  
L - LIMA  
p - papa  
2 - two  
y - yankee  
Q - QUEBEC  
? three

NATO  
Phonetic  
Alphabet

Password is Very Strong.

NATO Phonetic Alphabet for Password

6. The password is requested by the client and is delivered to your web session from the secured database of secrets.
  - a. Observe that it is no longer the password that we used in our baseline Remote Desktop test and that it validates against the unique Formula rule we created in the previous exercise.
7. You can click the **Unlock** button again or refresh your browser to return this field to its default Locked state.

And there it is. A fully automated (on demand) password reset job to a complexity (formula) you defined and secured in such a manner that most users will only be able to connect to the host using a secure, recorded session in PAM.



# Securing Objects with Permissions and Sharing

Permissions and sharing are concepts applied to both Folder and Records.

The act of granting permissions is providing a user or group (of users) the ability to access folders and records with a pre-determined set of security levels.

Permissions can range from the low end “Viewer” up to “System Administrator” at the top and several steps in between.

Throughout this section, we will discuss these core permission concepts and perform a few exercises to help illustrate how they are applied to users.

## User and Groups

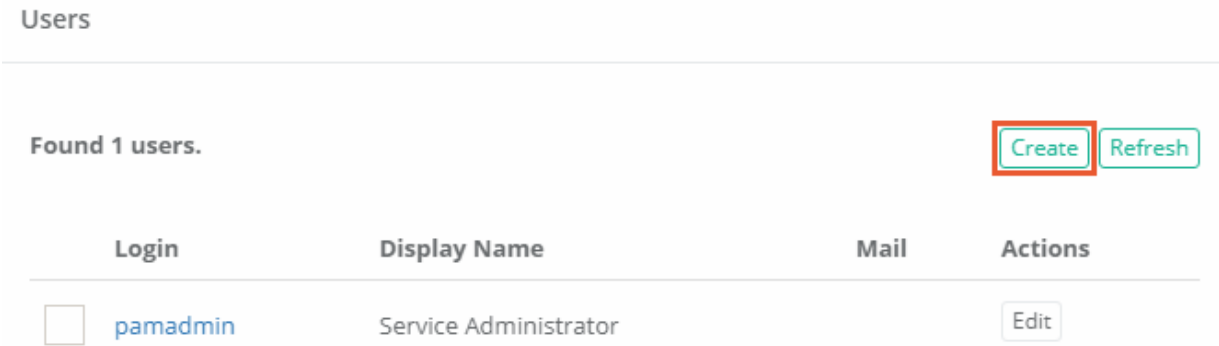
Permissions are granted to specific users or groups of users. If you have connected PAM with your Active Directory or LDAP server, then most likely these permissioned users or groups will originate from there.

If you did not, then the users and groups will be created locally in PAM’s Directory Service component.

If you will use your Active Directory or LDAP connections solely in PAM, then you may jump to the next topic [Grant Permissions](#), otherwise let’s continue with creating your first users and groups locally in the system.

### To create a new user in PAM:

1. If not already, login to PAM as a System Administrator.
2. Expand the Administration section of the left navigation menu and select **Local Users**.
3. Click the **Create** button:



#### Create Local Users

4. Enter the following information into the User fields:
  - a. *Login*: ituser
  - b. *First Name*: IT
  - c. *Last Name*: User
  - d. *Mail*: leave empty (*used to send alerts and notifications when configured*)
  - e. *Password*: choose a password
  - f. *Repeat Password*: reenter the password
5. Click **Save** to create this new user.

# If you also want to organize local users into local groups:

- 1. If not already, login to PAM as a System Administrator.
- 2. Expand the Administration section of the left navigation menu and select **Local Groups**.
- 3. Click the **Create** button.
- 4. Enter the following information into the Group fields:
  - a. *Name*: IT Department
  - b. *Description*: IT Department Group

Group IT Department

Cancel

Save Group

Name

IT Department

Description

IT Department Group

## Create Local Groups

- 5. Click **Save Group**to create this new group.
- 6. Click on the new IT Department group to open it and then click **Add** to add a new member.

Group IT Department

Found 1 members.

Cancel

Save Group

Delete Group

Name

IT Department

Description

IT Department Group

Member	User or Group	Directory
<input type="checkbox"/> Service Administrator (pamadmin)	User	Local

Add Member

Remove Members

Bulk Actions ▾

## Add New Group Members

7. In the principal field, type “ituser” and then click **Add**.
8. When “IT User” appears as a Selected Principal, click **Select** to add this user to the group. IT User is now a member of the IT Department group.

Please note that the user who creates the local group will automatically become its first member. In this exercise that is our Service Administrator.

## Grant Access

### Principal

**Add**

### Selected Principals

### Add Local User to Local Group

Please note that Active Directory or LDAP Users can be added to Local Groups, however Local Users or Groups cannot be added to Active Directory or LDAP Groups.

## Grant Permissions

Once users and / or groups (local or AD) have been added to PAM, you can begin to grant permissions to folders and records. The act of granting permissions will give this user or group varying levels of access to this object, so it is important for you to understand the following points in your system:

- What are the PAM permission “roles”?
- What options do these roles grant to users and groups?
- Who do you want to assign these roles?
- How granular do you wish to control permissions (inheritance vs unique)?

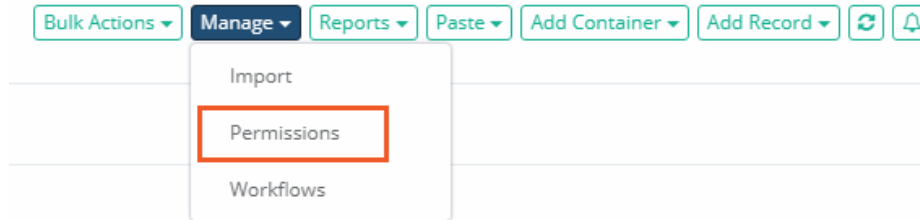
A user or group giving the wrong permissions can result in inappropriate access to privileged accounts, sessions or jobs.

For this scenario, let’s return to our original “IT Records” folder and begin granting permissions.

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.

- If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.

- Once you are inside the IT Records folder, locate and click the Manage > **Permissions** button along the top.



Permissions Button

- The IT Records permissions page will load. Before proceeding, it is good practice to always confirm that you are looking at the correct object before modifying permissions. In our example, you will see this:
  - “Permissions for IT Records / inherited from Root Folder”
    - This means we are working on the Permissions of the object “IT Records” which currently inherits permissions from its parent “Default Root”. *Default Root or Root Folder is simply the home or root of the All Records view.*
    - You will also notice the **Make Unique** button. When the option to Make Unique is available, that implies this object is currently inheriting from its parent.

Permissions for IT Records / inherited from [Default Root](#)

Found 1 records.

[Make Unique](#)

Principal	Type	Record Control	Session Control	Task Control	Actions
<input type="checkbox"/> Service Administrator (xtamadmin)	User	Owner	Connect (Always Recording with Session Events)	Manage	<a href="#">Edit</a>

Inherited Permissions on our IT Records Folder

- Now that we are certain about the object, click the **Make Unique** button so we can modify the folder’s permission. Click **OK** to accept the confirmation message.
  - To learn more about inheritance throughout PAM, please review [What is Inheritance?](#)
- The permissions view will refresh and display “Permissions for IT Records” correctly indicating that it has unique permissions now and is no longer inheriting from its parent Root Folder.

If you want to revert and go back to inheriting permissions, simply click the **Inherit from Parent** button. However, for this exercise, we are going to proceed with unique permissions.

- Click **Grant Permissions**



Grant Permissions

7. In the Principal field, enter “IT Department” and click **Add**. The group IT Department will be listed under Selected Principals.
  - If you want to grant additional permissions, you could add more users or groups during this operation by simply repeating this step as often as needed.
8. Choose the Permissions options (For additional descriptions of PAM permissions, please review our page [here](#)):
  - a. *Record Control*: Viewer
  - b. *Session Control*: None
  - c. *Task Control*: None
9. Click **Select** to complete the operation and grant the selected permissions to the IT Department group.

Permissions for IT Records

---

Found 2 records.

Grant Permission Revoke Permission Inherit from Parent ↺

Principal	Type	Record Control	Session Control	Task Control	Actions
<input type="checkbox"/> IT Department	Group	Viewer	None	None	<span>Edit</span>
<input type="checkbox"/> Service Administrator (xtamadmin)	User	Owner	Connect (Always Recording with Session Events)	Manage	<span>Edit</span>

### Unique Permissions

You have now granted the group “IT Department”, and subsequently all its members, with the Viewer role, No session control and No task control to this folder.

Something very important to remember is that inheritance is enabled by default for all records and folders in PAM, so whatever child objects reside in this folder (now or in the future) the IT Department group also automatically has the same View role and No session control to them as well.

To illustrate this point, let’s look at the permissions to the record “Production Web Server” currently residing in the IT Records folder where inheritance is enabled.

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
  - If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate and click the **Manage > Permissions** button along the bottom of the record’s View.
4. When the record’s permissions load, you will notice two things:
  - a. As expected, “Permissions for Production Web Server / inherited from IT Records” appears along the top. This record inherits permissions from its parent IT Records because that is the default mode and we never made the permissions unique (**Make Unique** button).
  - b. The group IT Department therefore has permission (Viewer, None and None) to this record.

Found 2 records.

Make Unique 

Principal	Type	Record Control	Session Control	Task Control	Actions
<input type="checkbox"/> IT Department	Group	Viewer	None	None	<a href="#">Edit</a>
<input type="checkbox"/> Service Administrator (xtamadmin)	User	Owner	Connect (Always Recording with Session Events)	Manage	<a href="#">Edit</a>

### Inherited Permissions on a Child Record

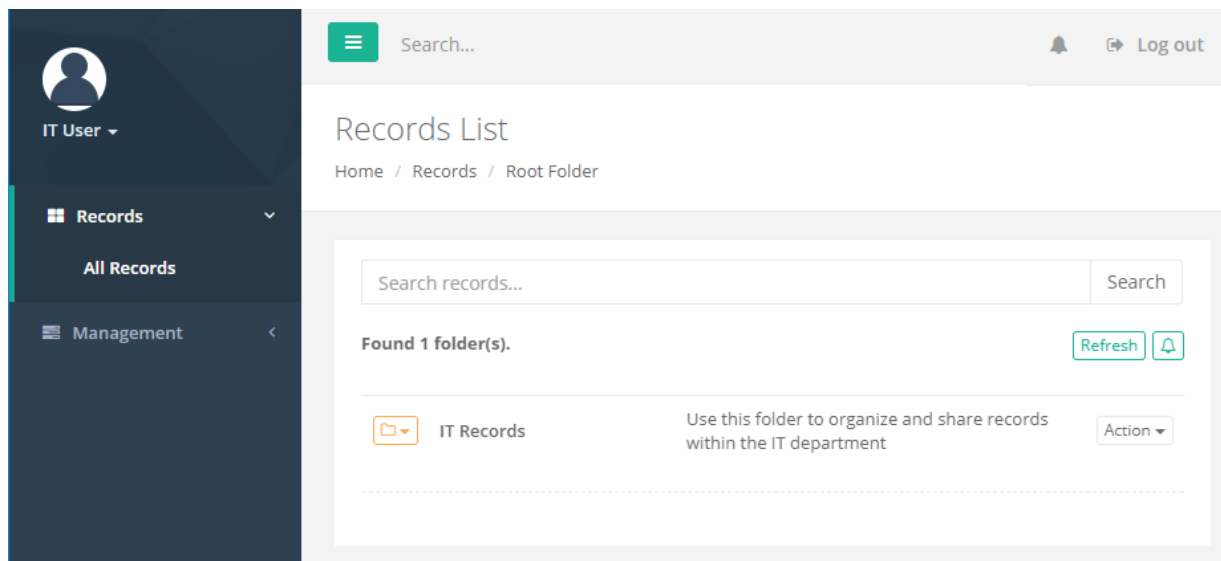
This highlights the ease of use and flexibility of working with permission inheritance throughout the PAM system.

On the other hand, it also highlights the importance of truly understanding all parent-child relationships and ensuring only the required users or groups have the base level of permissions to all required objects.

## Permissions in Action

Now that we have completed the exercise and implemented some basic level of object permissions, let's see how that looks from an end user's perspective.

1. Open a new browser or a new private/incognito browser session.
2. Login to PAM using the user account "ituser" that was created in the previous section.
3. A few observations to note when you first login with this account:
  - a. This is not a System Administrator account so the entire Administration section of the left navigation menu is hidden and inaccessible.
  - b. Under the Records section, the favorite <IT Records> is not displayed because **Favorites** are specific to a user and are not shared globally across the system.



### "IT User" Logged In View (non-Admin)

4. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.

5. Within this folder, observe that all the options along the top are hidden and inaccessible. Compare this view with that of the System Administrator in your other browser session.
6. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
7. Within this record, observe again that all the options along the top and bottom are hidden and inaccessible to this user. Compare against your System Administrator view and take special note that the edit, configuration, unlock and connect buttons are not available. This user has minimum permissions to View this folder and record only.

### Production Web Server

<b>Name</b>	Production Web Server
<b>Description</b>	Record for our production web server

---

<b>Host</b>	10.0.0.23
<b>Port</b>	10023
<b>User</b>	xt\itadmin
<b>Password</b>	*****

Record Type: Windows Host  
Created By: pamadmin at Jul 25, 2017, 11:13 AM  
Last Modified By: pamadmin at Jul 25, 2017, 11:56 AM

---

#### Record with Viewer Only Permissions

Let's modify the permissions of "ituser" slightly to see how permissions can be adjusted to grant or revoke specific functionality in real-time.

1. Back in your System Administrator's PAM session, modify the permissions on the IT Records folder.
2. Select the permission record for IT Department (the group 'ituser' is a member of) and click **Edit**
3. Make the following changes:
  - a. *Record Control*: Editor
  - b. *Session Control*: Connect (Always Recording with Session Events)
  - c. *Task Control*: Manage
4. Click **Select** to save the change.

Principal	Type	Record Control	Session Control	Task Control	Actions
<input type="checkbox"/> IT Department	Group	Editor	Connect (Always Recording with Session Events)	Manage	<button>Edit</button>

### IT Department Permissions after Modification

- Return to ituser's browser session and refresh your browser.
- Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
- Within this folder, observe the options along the top that are visible and accessible to this user.
- Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
- Within this record, observe that the options along the top and bottom are visible and accessible by this user now. Including both the **Unlock** button for the password field, the **Connect** button to establish a secure session as well as the **Execute** option.

Production Web Server

Go to Parent
Connect...
Execute...

Name

Production Web Server

Description

Record for our production web server

---

Host

10.0.0.23

Port

10023

User

xt\itadmin

Password

\*\*\*\*\*

☐

Record Type: Windows Host  
Created By: pamadmin at Jul 25, 2017, 11:13 AM  
Last Modified By: pamadmin at Jul 25, 2017, 11:56 AM

---

Audit Log

Sessions

Formula

Tasks

Permissions

Edit Record

☐

### Record with Edit and Connection Permissions

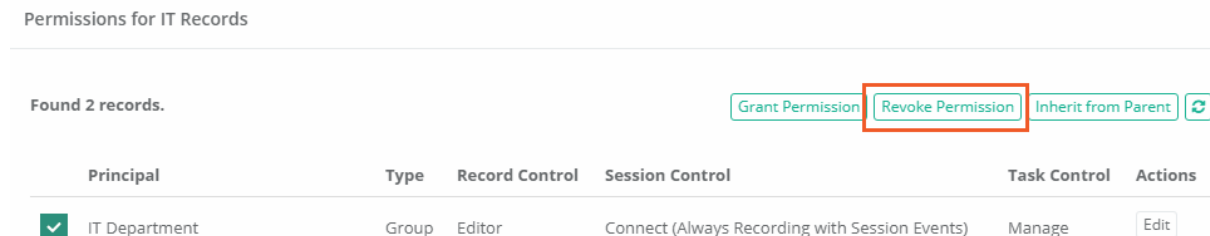
To recap, we covered the relationship between users and groups, how permission inheritance is defined by default and when making them unique as well as how permissions can be modified and what that means to the end user's access to the system.

## Revoke Permissions

Revoking permissions is quite simply removing permissions to an object that were originally granted to a user or group or users. To demonstrate this principle, let's revoke "ituser" from the permissions we just granted it.

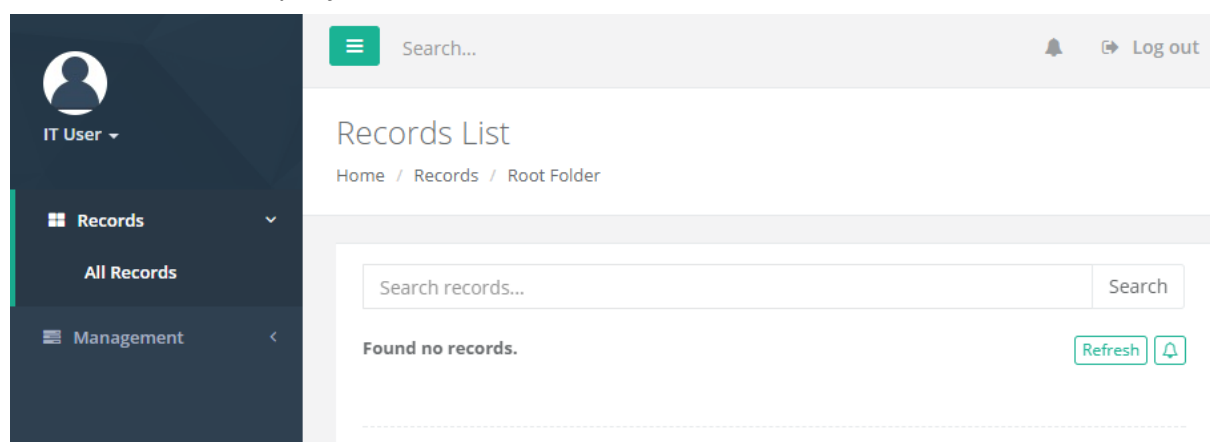


1. From the System Administrator's session, modify the permissions on the IT Records folder.
2. Locate and select the box next to IT Department.
3. Click the **Revoke Permissions** button. IT Department is immediately removed from the permissions of this folder and all child objects that are set to inherit from it (our "Production Web Server" record in this folder).



### Revoke Permissions

4. Refresh the browser that ituser is logged in and you will notice that they can no longer see nor access the IT Records folder or any object that inherits from it.



"IT User" with Revoked Permissions

## System Administrators

The System Administrator role is defined as the top most permission any user or group can be granted in PAM. The default installation account will become the first System Administrator and from this starting point, other users and groups can be given this role. It is extremely important to know that this role has complete and total control over all objects including folders, records, password unlocks, sessions, deletion, PAM configuration and view access to all logging. They also can grant AND remove any other users as System Administrators. Please only grant this permission to trusted users.

### To grant a user or group the System Administrator role:

1. If you are not already, login to PAM as a System Administrator.
2. Navigate to and expand the Administration section of the left navigation menu and select **Global Roles**.
3. Click the **Add** button.
4. Enter the user "ituser" and click **Add**. IT User will appear as a Selected Principal.

- 5. Choose **"System Administrator"** from the Global Role dropdown.
- 6. Click **Select** to complete the operation.

Global Roles

Found 2 records.

Refresh

Add

Remove

Principal	Type	Role
<input type="checkbox"/> Service Administrator	User	System Administrator
<input type="checkbox"/> IT User	User	System Administrator

System Administrators

- 7. Refresh the browser that *"ituser"* is logged in and you will notice that the Administration section is now visible and accessible. Also, this user can now view, access, connect and has full control over the **IT Records** folder and all other records and folders regardless of the specific permissions assigned to the object's permissions.

IT User

Records

All Records

Administration

Management

Search...

Log out

Records List

Home / Records / Root Folder

Search records...

Search

Found 1 folder(s).

Refresh

Paste

Permissions

Policy

Add Folder

Add Record

IT Records

Use this folder to organize and share records within the IT department

Action

"IT User" with System Administrator Permissions

System Administrator has full control over all components within the PAM system and should only be granted to trusted users.

Please *revoke* the System Administrator role from the user "IT User" before continuing with this guide. It's good practice to always revoke untrusted, outdated or test accounts from this permission role.

# Search Query Options

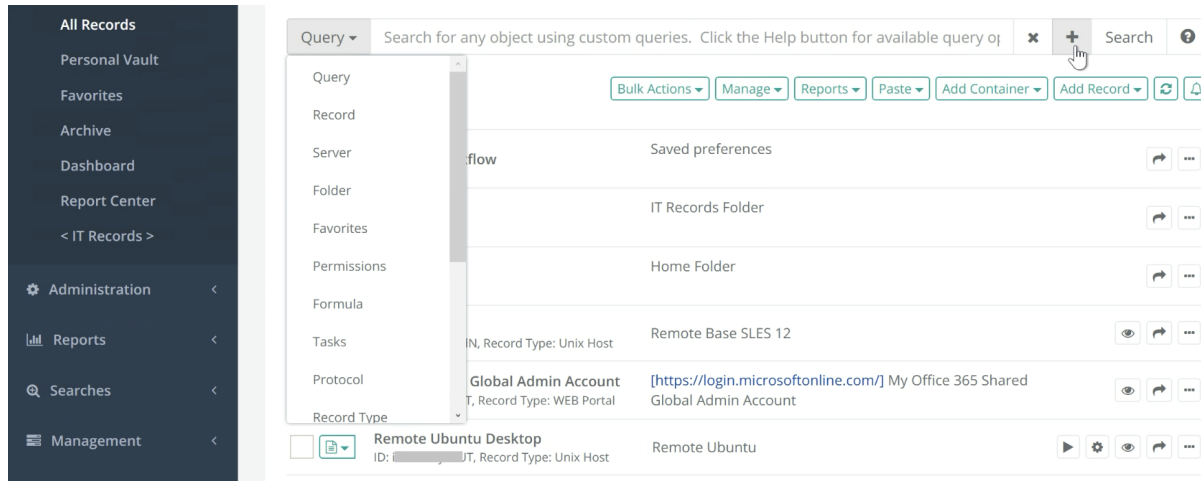
[Privileged Access Management \(PAM\)](#) can quickly find records that match PAM search criteria. By default, PAM search query finds records by record name, description and a host name on a record.

However, PAM also uses special conventions to look for special record parameters such as permissions, record types or connection method.

This article discusses different queries that could be executed using the PAM search bar located on the record list screen.

The preset PAM search query options are available in drop-down list.

To make user's search more unique, PAM additional multiple search is available there user can add more than one search field or option.



## Records Visibility

Note that PAM will only display records a currently logged in user has permission to view. However, some of the records a user can view might come from folders the current user has no access to browse. In this case, the user might see records they **cannot** browse through regular folder hierarchy. For quick access to such records user might use the Search option again.

Alternatively, users can “favorite” these records to access them through **Favorites link** in the application menu. Yet another way to access visible records located in invisible folders is to use the **Shared with Me** link to review items shared with the current user from other users.

## PAM Manual Search Criteria Options

1. Search by record name, description or host name.

Type a search criteria in the PAM search bar, click **Search** button to find records that contain the search criteria in record name, description or a host name.

2. Clear search.

Remove search criteria from PAM search box, click **Search** button to return to the folder hierarchy browser.

3. Access Search.

Type one of the search queries below to the PAM Search bar and then click **Search** button to find all records the provided *USER* can view:

- **acl:USER**
- **a:USER**
- **permissions:USER**

4. Find items with unique permissions.

Type one of the search queries below to the PAM Search bar and then click **Search** button to find all folder and records with unique permissions:

- **acl:unique**
- **a:unique**
- **permissions:unique**

Note that when folder or record has unique permissions changing permissions of the parent of this record does not affect permissions of this item. It is much easier to manage items that inherit permissions from their parents because permissions could be managed in fewer places. Design the permission architecture so that items will naturally fall into the folder hierarchy with few uniquely permissioned folders.

5. Find records with unique formula.

Type one of the search queries below to the PAM Search bar and then click **Search** button to find all records with unique password formula:

- **formula:unique**
- **fm:unique**

By default, the record type defines the password formula for all records of this type. However, making a password formula unique for a record to define record-specific formula complexity is possible. When the inheritance of the password formula from the record type is broken, the change of the password formula on the record type level does not affect the complexity formula of the record with a unique password formula. This query is a quick way to find records with unique password formulas to understand the reason behind this uniqueness.

When many records have similar unique password formulas, it might be easier to create a special record type for the records with a specific password formula to manage formulas in a single place for multiple records.

6. Find records with unique task set.

Type one of the search queries below to the PAM Search bar and then click **Search** button to find all records with unique set of tasks:

- **tasks:unique**
- **tm:unique**

By default, record type defines task set for all records of this type. However, it is possible to make a task set unique for a record to define record specific tasks with the scripts and event based execution policy. When inheritance of the task set from the record type is broken the change of the tasks on the record type level does not affect the tasks of the record with unique tasks. This query is a quick way to find records with unique task set to understand the reason behind this uniqueness.

In the situations when many records have similar unique tasks (including scripts and execution schedule), it might be easier to create a special record type for the records with specific tasks to manage tasks in a single place for multiple records.

#### 7. Find records by connection type.

- Type one of the search queries below to the PAM Search bar and then click **Search** button to find all records with specific connection type such as RDP, SSH or RemoteApp:

- **session:TYPE**
- **sm:TYPE**

Below are some examples of such query:

- Query **sm:RDP** will find all RDP records while **sm:RemoteApp** will find all RemoteApp records.

#### 8. Find records by record type.

Type one of the search queries below to the PAM Search bar and then click **Search** button to find all records with selected record type:

- **type:TYPE**
- **t:TYPE**

All PAM records are of a certain record type. This query helps to identify all records of a specified record type.

Below are some examples of such query:

- Query **type:Windows Host** will find all Windows Host records while **t:Unix Host** will find all Unix Host records.

#### 9. Find archived records.

Type the search query below to the PAM Search bar and then click **Search** button to find all archived records:

- **arch:**

#### 10. Find folders.

Type one of the search queries below to the PAM Search bar and then click **Search** button to find all folders visible to the current user by folder name and description criteria:

- **folder:query**
- **folders:query**

Below are some examples of such query:

- Query **folders:auto** will find all folders with name or description containing the substring *auto*.

11. Find referencing records.

Type one of the search queries below to the PAM Search bar and then click **Search** button to find all records visible to the current user by referencing a record found by provided name, description, host and indexed metadata criteria:

- **reference:query**
- **ref:query**

Below are some examples of such query:

- Query **ref:Domain Admin** will find all records referencing records found by *Domain Admin* criteria.

12. Find records using specified record as a shadow account.

Type one of the search queries below to the PAM Search bar and then click **Search** button to find all records visible to the current user using a record found by provided name, description, host and indexed metadata criteria as a shadow account for their task execution or password reset scripts:

- **shadow:query**

13. Precise search option to locate exact record match.

Exact search option to only find records that match the entered search criteria precisely without an automatic assumption of wildcard-based search. This way, the search initiated for 10.0.0.1 will not display 10.0.0.12 or 110.0.0.1 records. To initiate such a search, use enclosing double quotes around search criteria.

- **"10.0.0.1"**

Precise search allows *wildcard* % specification in the certain position of the criteria. For example, the following criteria will search for all records that start with the provided string:

- **"10.0.0.1%"**

14. Find recently created records.

Type one of the search queries below to the PAM Search bar and then click **Search** button to find all recently created records (note that search criteria new: without qualified will default to records created during last hour):

- **new:hour**
- **new:day**
- **new:week**
- **new:month**
- **new:**

15. Find records with associated anonymous links.

Type the search query below to the PAM Search bar and then click **Search** button to find all records that have associated anonymous links. you can use **Audit Log report** to review historical data about sharing records using anonymous links including link authors, terms and viewers but the search query below will list records with the currently associated links.

16. Compound Query Search.

With Search Type selected as Query the system accepts compound queries including different criteria connected with the predicate AND.

For example, use the following query to find archived Unix Host records.

- **type:***Unix Host* **AND archived:**

Another example is to find all Windows Host records that contain pass in the name, description or indexed field with permissions granted to UserA.

- **type:***Windows Host* **AND pass** **AND a:***userA*

#### 17. Find records by record ID.

Type the search query ID:Record-ID to find exact record with the specified ID. The search query will find records by either long and short record IDs.

- **id:***RECORD-ID*

## Multiple Search Criteria Options

Combine two or more search criteria options into a single query for advanced search scenarios.

Compound queries can be entered manually or graphically using the **Search Center**.

Choose the *Query* selector and then enter your first search option.

There are drop-down search selectors:

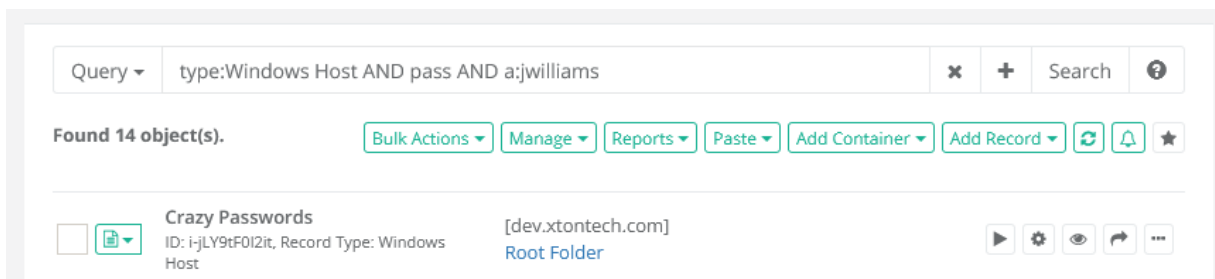
- **Query** - find records by query: record name, description or host name.
- **Record**- find records by [record](#).
- **Server** - find records by used server.
- **Folder** - find records by used Folders.
- **Favorites** - find records added to [Favorites](#).
- **Permissions** - find records by [Permissions](#).
- **Formula** - find records by [Formula](#).
- **Tasks** - find records with unique [task](#) set.
- **Protocol** - find records by used protocol.
- **Record Type** - find records by [record type](#).
- **Reference Record** - find [referencing records](#).
- **Shadow Record** - find records using specified record as a [shadow account](#).
- **New** - find recently created records.
- **Anonymous Links** - find records with associated [anonymous links](#).
- **Orphaned Objects** - find orphaned records.
- **Archived Records** - find [archived records](#).
- **ID** - find records by record ID.

To manually enter a compound search, choose the *Query* selector and then enter your first search option.

Between this first search and your next, separate them with the predicate AND, OR (in capital letters) if you want to add the parameter of search.

For example, if you want to create a compound query to search for all *Windows Host* records that contain the value pass in the Name, Description or indexed field with permissions granted to the user *jwilliams*, enter this into the Query:

**type:Windows Host AND pass AND a:jwilliams**

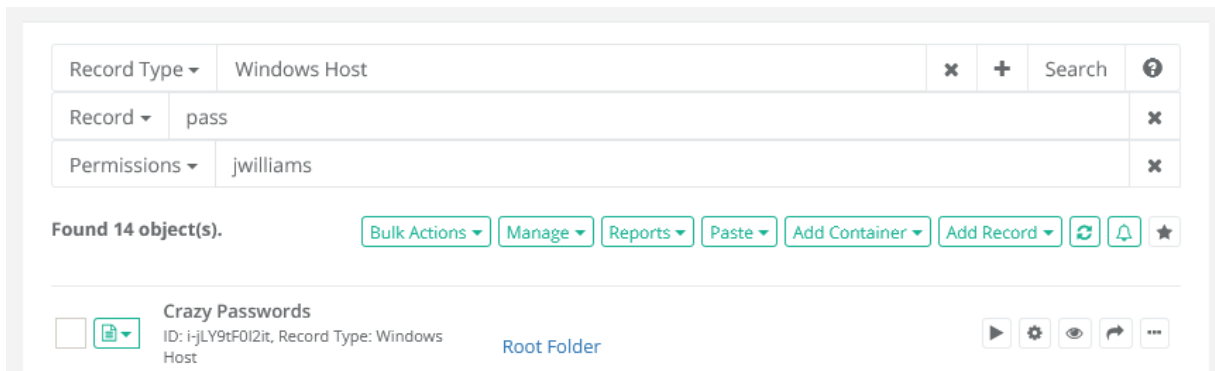


And, for example, if you want to create a compound query to search for all *Unix Host* records that contain the value *pass* in the Name, Description or indexed field with permissions granted to the user *pamadmin*, enter this into the Query:

**type:Unix Host OR a:pamadmin**

To create the same compound search using the graphical Search Center you enter your first Search, then click the plus (+) sign to add the second and finally the plus sign again to add your third. Use (-) button to remote extra condition.

As a last step once your compound search has been created, click the **Search** button to find your results.



## Reviewing the Audit Log

One of the most important sections of the PAM system is the [Audit Log](#).

The System's Audit Log is accessible only by users who have been given the [System Administrator role](#).

The System's Audit Log contains captured events that have taken place across the entire PAM system.

These events include record creation, modifications, session connections, system configuration and more.

### To access the Audit Log:

1. If you are not already, login to PAM as a System Administrator.
2. Navigate to and expand the Reports section of the left navigation menu and select **Audit Log**.
3. Wait a few moments for the Audit Log to load the most recent events.
4. When the events appear, scroll down through the list and observe all the activities that we have performed during this walk through.
5. Please also explore the options available along the top that include filtering, search and export.



Found 54 audit log records.

Time: Last Day ▾

Category: Any ▾

Level: Any ▾

Columns ▾



Show 50 ▾ entries

Search: 

CSV

PDF

XLSX

PDF Protected

CSV Protected

XLSX Protected

Showing 1 to 50 of 54 entries

Time ▴ ▾	User ▴ ▾	Category ▴ ▾	Level ▴ ▾	Event ▴ ▾	Message ▴ ▾
06/15/2021 16:02:43	Service Service (pamservice) /Local	Application	INFO	Summary Collection	Collected 27 daily summaries
06/15/2021 16:02:43	Service Service (pamservice) /Local	Application	INFO	Summary Collection	Collected 1 hourly summaries

## System Audit Log

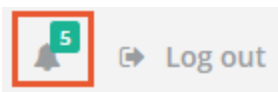
## Notifications and Alerts

If you remember back to the beginning of this guide, when we first created our **IT Records** folder we started with setting up an Alert to notify on permission events.

We did this so our permission modifications in the previous section would be captured.

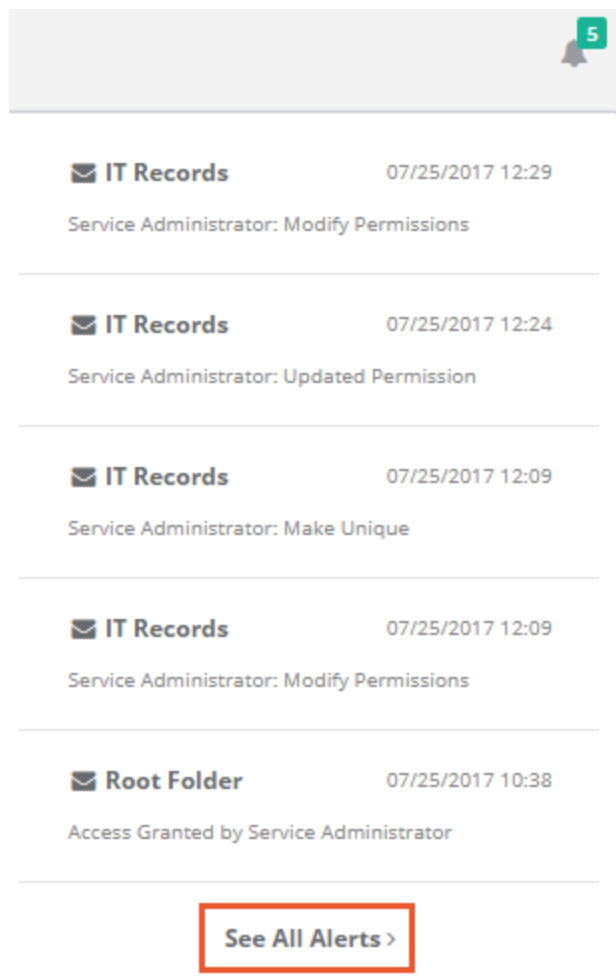
User alerts can be accessed in two locations and will display the event that triggered the notification. Let's look at our Alerts from today:

1. Along the top of the PAM interface, accessible from any view, click the **Alert** button. If you followed along closely, you should see a badge indicating several alerts have been generated.



## Top Bar Alert Notifications with Badge

2. Clicking the **Alerts** button will open the dropdown menu displaying a handful of recent notifications, sorted from the most recent to the oldest. In this dropdown, you will see several notifications related to the permissions we updated on the **IT Records** folder during earlier exercises.
3. At the bottom of this dropdown, click the **See All Alerts** option.



Open My Alerts

4. This will open the full list of all Alerts including some additional information and descriptions.

As with most event based views in PAM, there are many options to explore including filters, search and export.

Look around and continue to the next section when you are ready.

## Unsubscribe to Alerts

When you no longer want, or need to receive Alerts about an object, you can very easily unsubscribe from it and these notifications will no longer be generated for you.

Let's quickly unsubscribe from the IT Records folder:

1. Navigate to and expand the Management section of the left navigation menu and select **My Profile**.
2. When My Profile loads, click over to the **Subscriptions** tab.
3. Locate and select the **IT Records** object by clicking its checkbox.
4. Click **Unsubscribe**.
5. The view will refresh and IT Records will be removed from the list.

Found 2 subscriptions.

Subscriptions: Alerts ▾ [Subscribe](#) [Unsubscribe](#)

Object	Object Type	Category	Level	Event
<a href="#">IT Records</a>	Folder	All	All	

### Unsubscribe from Alerts

You have successfully unsubscribed from receiving notifications related to this object.

## Managing my User Profile

Users can update and configure several options that are specific to their PAM User Profile to customize their experience.

### Update your User Profile

- If you are using an PAM Local User account, you navigate to Management > My Profile > **Profile** to update your First Name, Last Name, Email, Profile Picture and Password.
- If you are using an integrated Active Directory User account, you navigate to Management > My Profile > Profile to reset your AD password (self-password reset). Your *First Name*, *Last Name*, *Email* and *Profile Picture* are maintained in [Active Directory](#) and cannot be updated in PAM.

### Configure your PAM Preferences

- Navigate to My Management > My Profile > Preferences and adjust the settings as desired. There are several options available to customize your preferences when using PAM including options to define session parameters, skin type, start mode and more. Remember to click the **Save** button after you change any parameter.

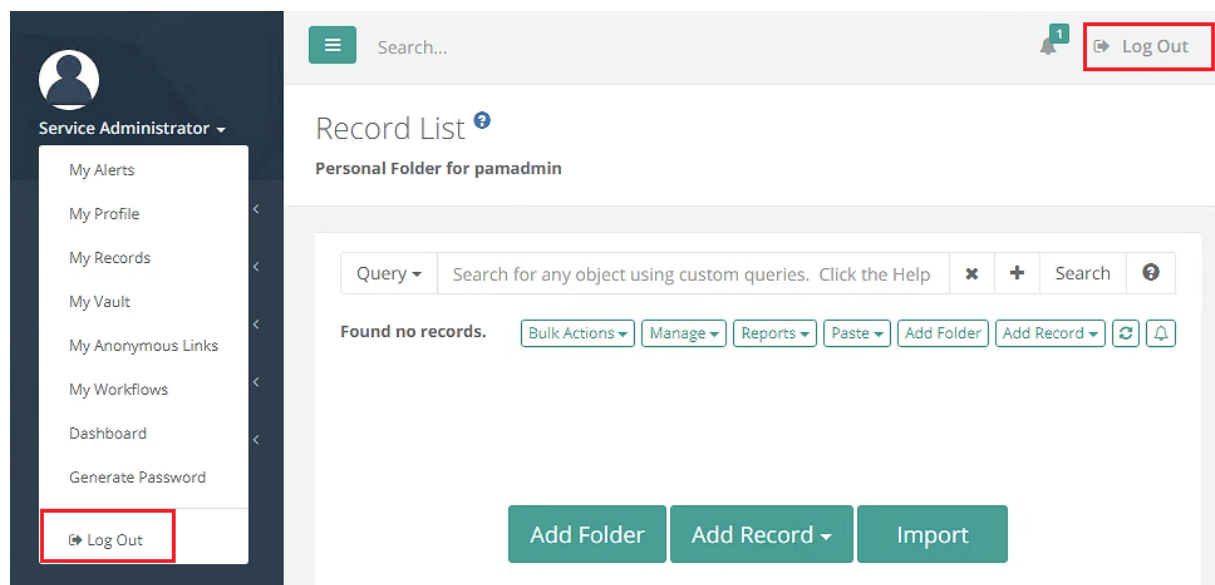
## Logging Out

When you are done working with PAM, it is highly recommended to securely log out of the system.

You should never walk away from your computer when logged into a session of PAM as anyone could walk by and have control of the software.

To securely log out of PAM:

1. Click the **Log out** button located in the upper right corner of PAM or **Logout** located under the User Profile located in the upper left.



Logout Options

2. The application will log your account out.
3. **Exit** your web browser to ensure the session is completely logged out.

If you have not already, logout and exit your browser that was used for our “IT User” exercises too.

## Appendix

### Inheritance

PAM utilizes the concept of inheritance in several areas to make the management and configuration of objects more streamlined and easily organized. Inheritance defines the relationship between a parent and child object and specifically what is inherited down from the parent to the child which resides beneath it.

Inheritance in PAM can be found in the following areas:

- **Permissions**
  - Permissions are inherited by default from parent folder to child objects (subfolders or records). If permissions are modified on the parent folder, then all child objects will reflect this change.
  - To make permissions unique means to stop this parent to child inheritance and instead have the child contain its own set of permissions which may in turn inherit down to its own children.
- **Formulas**
  - Formulas are inherited by default from [Record Types](#). If the formula on a parent record type is modified, then all child types will reflect this change.
  - To make formulas unique means to stop this parent to child type inheritance and instead have the child contain its own formula which may in turn inherit down to its own children.
- **Strategies**
  - Strategies are inherited by default from [Record Types](#). If the strategy on a parent record type is modified, then all child types will reflect this change.

- To make strategies unique means to stop this parent to child type inheritance and instead have the child contain its own strategy which may in turn inherit down to its own children.

- **Policies**

- [Policies](#) are inherited by default from parent folder to child objects (subfolders or records). If a policy is modified on the parent folder, then all child objects will reflect this change.
- To make policies unique means to stop this parent to child inheritance and instead have the child contain its own policy which may in turn inherit down to its own children.

The “pros” of inheritance is that it allows for ease of use and flexibility when configuring and using the system while the “cons” are that the more *unique* objects you create, the more difficult and cumbersome it becomes to understand and manage the structure of your system.

## Wrapping Up

That concludes this Getting Started Guide. If you followed along through each section, you should now feel more comfortable with PAM and have an introductory working knowledge of its features and functionality.

We encourage you to revisit each section and try new options and configurations.

Also, explore the many areas that were not included in this guide like [Discovery Queries](#), [Custom Record Types](#) and [Reports](#) at your own pace.

## Technical Support

If questions remain or issues arise while using PAM, please contact our Support Team

<https://support.imprivata.com/communitylogin>.

## Web Browser Extension

### What is the Browser Extension

The Imprivata Privileged Access Management Browser Extension is a native browser extension that can be utilized by PAM users to auto-populate Web login forms using records that are stored within the Privileged Access Management Identity Vault.

Once logged into PAM within the [browser extension](#), it will securely communicate with the Identity Vault to locate any records associated to the currently displayed login form and if found, will give the user the ability to populate the *username* and *password* fields with a single click.

- Google Chrome ([external link to the Imprivata PAM Broker Browser Extension - Chrome Web Store](#));
- Mozilla Firefox ([link to the file with the Imprivata Access Manager extension for Firefox](#));
- Microsoft Edge (Chromium) ([external link to the Imprivata PAM Broker Browser Extension - Microsoft Store](#));
- Opera (see installation procedure [here](#)).

# Using the Browser Extension

1. Create a new record in PAM using the type **WEB Portal**.

Within this record, enter the following parameters:

**Name:** Enter an easily recognizable name for this record that will be used for selection in the extension.

**Description:** Optionally enter a description for this record. The description will not appear in the Extension.

**URL:** Enter the URL to the login or signin page that contains the web login form.

**User:** Enter the username to be populated.

**Password:** Enter the password for the username.

<b>Name</b>	My Office 365 Global Admin Account
<b>Description</b>	Office 365 Shared Global Admin Account
<hr/>	
<b>Url</b>	<input type="text" value="https://login.microsoftonline.com"/>
<b>User</b>	<input type="text" value="globalAdmin@xtontech.onmicrosoft.com"/>
<b>Password</b>	<input type="password" value="*****"/>

2. Once the record is created, share this record with a user or group with at least the *Unlock* role. You may now configure PAM to include users with [Viewer permissions](#).

## Grant Access

### Principal

<input type="text" value="Enter User or Group Name..."/>	<input type="button" value="Add"/>
--	------------------------------------

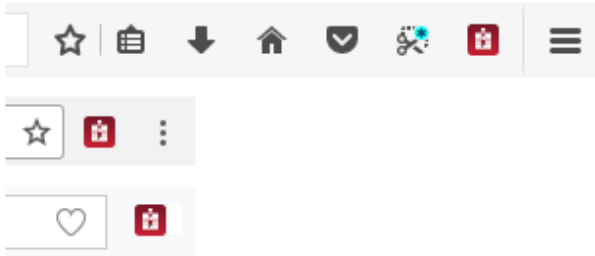
### Selected Principals

<input type="text" value="John Williams"/>
--

### Role

<input type="text" value="Unlock"/>
-------------------------------------

3. In either Mozilla Firefox, Google Chrome, Microsoft Edge or Opera, open the Extension store and add the Imprivata Privileged Access Management extension to your browser.
  - Google Chrome ([external link to the Privileged Access Management extension for Chrome](#))
  - Microsoft Edge (Chromium) ([external link to the Imprivata PAM Broker Browser Extension](#))
  - Mozilla Firefox ([external link to the Imprivata PAM extension for Firefox](#))
4. When the Extension is deployed, locate and click the Privileged Access Management extension in your browser window to open it for the first time.



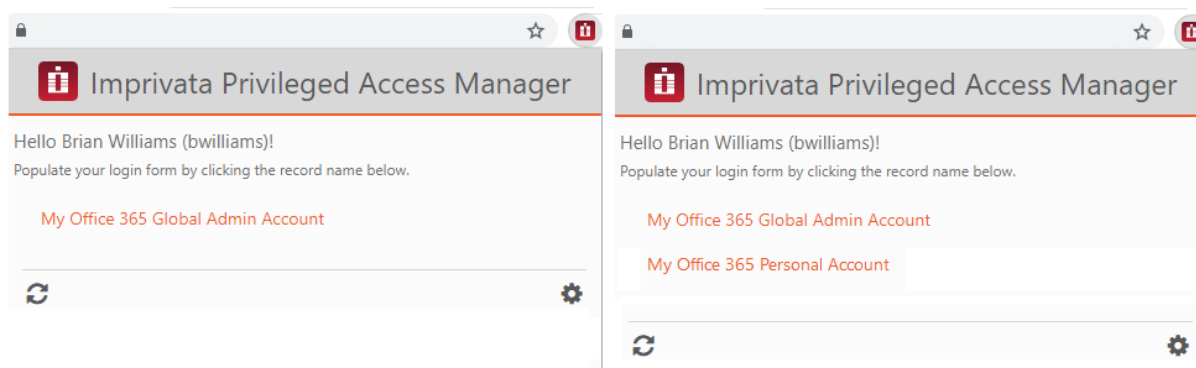
Browser Extension location in default configurations. Mozilla Firefox (top), Google Chrome (middle) and Opera (bottom).

5. Enter or copy/paste the URL to Privileged Access Management into the field and click the **Login** button. The PAM URL is the one that is used to initially login to the system. The default URL is **http://-localhost:8080/xtam** but often times this is modified.

If you are unsure, please contact your Privileged Access Management Administrator for assistance.

The image shows the Imprivata Privileged Access Manager login form. At the top, there is a header with the Imprivata logo and the text 'Imprivata Privileged Access Manager'. Below the header, there is a message: 'Enter your Imprivata Privileged Access Manager URL and then click Login to complete your configuration.' Below this message, there is a text input field containing the URL 'https://localhost:8080/xtam'. To the right of the input field is a 'Login' button. Below the input field and the 'Login' button is a 'Cancel' button.

6. A new browser tab or window will open and load the Privileged Access Management login page. Enter your PAM username and password and then log in as usual.
7. Once logged into PAM, you may close this browser window or tab and return to your previous. Open the Extension again to load your records.
8. In the Extension, select the record and then click the web page's login or signin button to complete the login procedure. If only one record for this login was found, the Extension will automatically populate the credentials once opened. If two or more records are found, then you must choose and click the Record Name to populate the desired credentials.



A user's view of one record displayed in the Extension (left) and multiple records (right).

And that's it.

PAM System Administrators have access to every record in the system, including records from other users private vaults. In that reason the PAM Browser Extension will show all records that the user has access to, including the records from other users private vaults.

PAM Users with PAM [System Administrators role](#) who are using a Web browser that has the PAM Browser Extension enabled, browse to a website login page, can see the records for all users who have stored credentials for that site.

It is highly recommended that your daily use User's accounts, including daily use Administrator's account, are not granted the role of System Administrator. Instead create a PAM Local User account (or a separate AD account) so that Administrators they can then login and administer PAM as needed.

You can continue to [create additional records in PAM](#) server for other web portal login forms and share these with your users and teams.

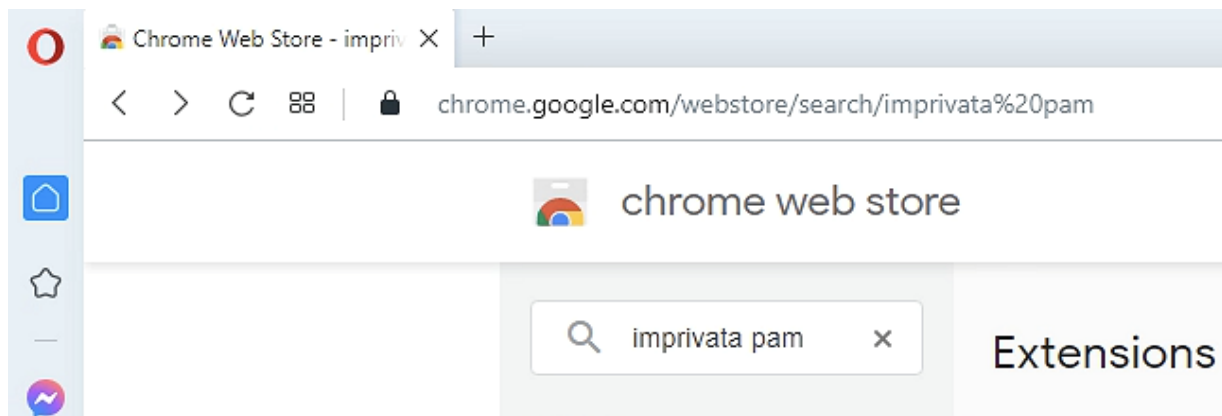
## Extension supported in Opera browser

The Imprivata Privileged Access Management Browser Extension is supported as an extension for the Opera browser; however, it is not available within the Opera Extension marketplace.

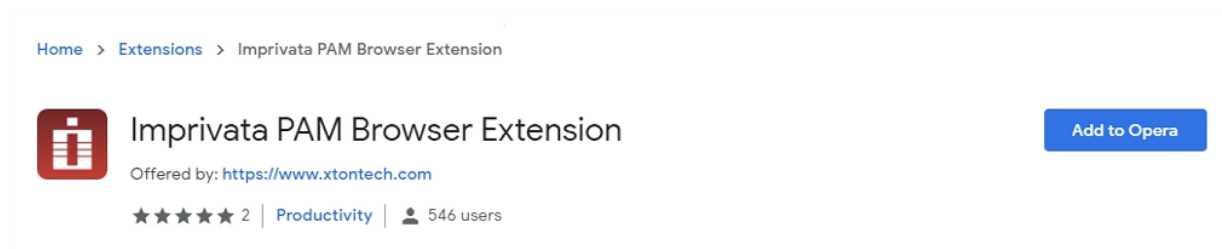
If you are using Opera, please follow this procedure to deploy the Imprivata Privileged Access Management Browser Extension.

1. Install the Opera extension "Download Chrome Extension" ([external link](#)) to your Opera browser by clicking the **Add to Opera** button.
2. The extension should be deployed and enabled by default, if it is disabled, then from within Opera open the Extensions page (Ctrl+Shift+E) and click the **Enable** button for the extension Download Chrome Extension.



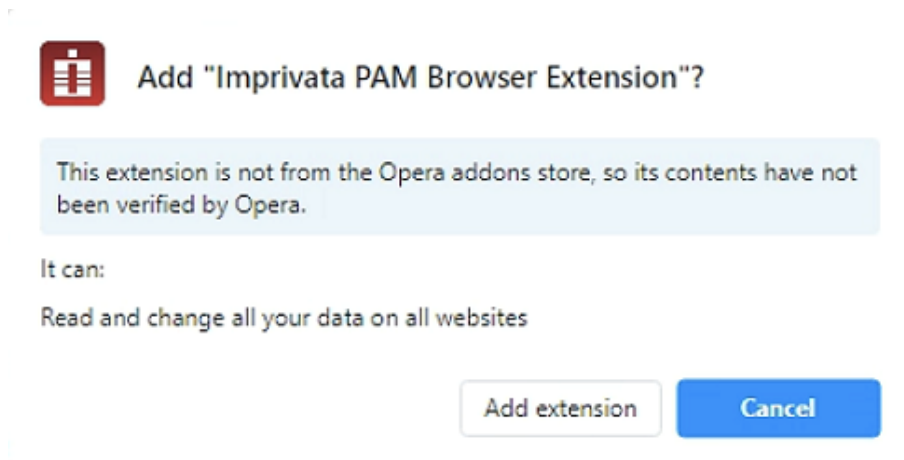


3. Now open the Imprivata PAM Browser Extension for Chrome ([external link](#)) to download and install the extension.
4. From within the Chrome Extension page for Imprivata PAM Browser Extension, click the **Add to Opera** button.

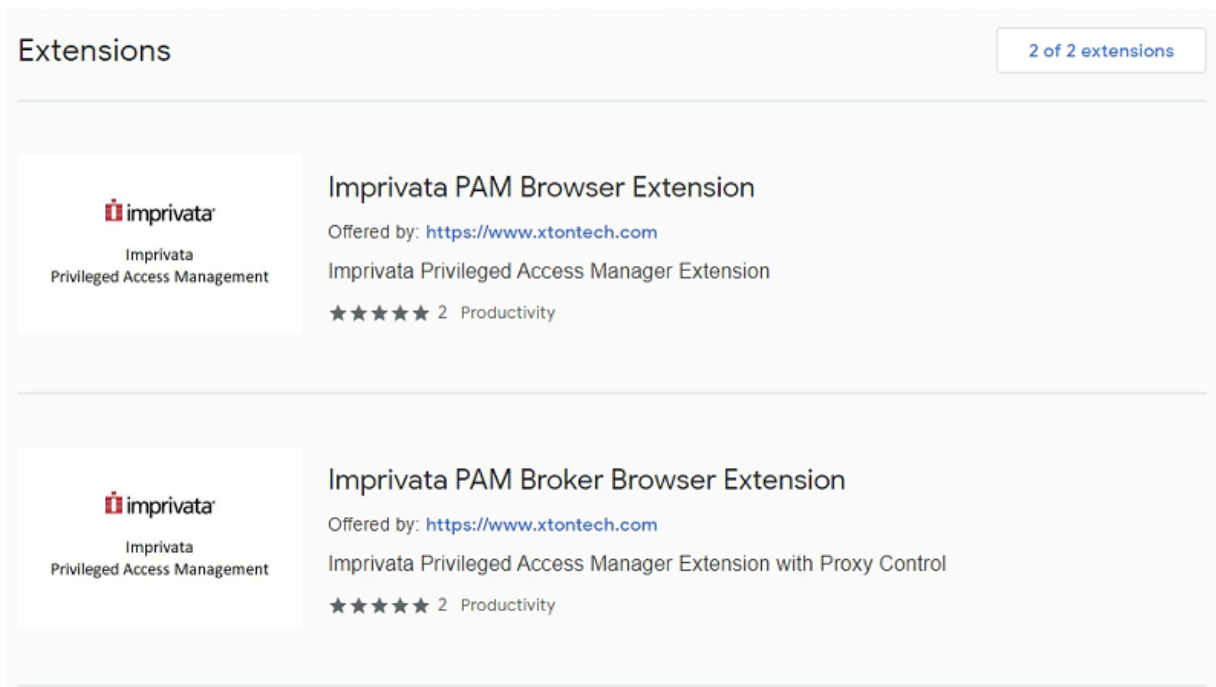


Click the **Add to Opera** button.

5. Read and then click **OK** on the confirmation dialog to continue.

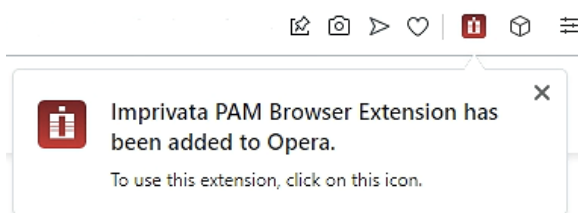


6. In the Opera Extensions page, locate the "Imprivata PAM Browser Extension" extension and click the **Install** button for it.



Install the PAM Browser Extension from Opera's extension page.

7. The Extension will now be installed to your Opera browser and become available in the bar along the top.



The PAM Browser Extension is installed to Opera and ready for use.

Now that the Extension has been successfully installed to Opera, read [how to use this Extension](#) to learn how to configure and use it.

## Extension records for Viewer only

Within PAM, a user is required to have at least Unlock permissions on a record to see or reveal its secured field, like a password.

By default, the PAM Browser Extension uses this same requirement; however System Administrators can lower or decrease this requirement to allow users with Viewer permissions to load shared credentials from within the extension.

This maintains the security around these fields in PAM, while extending the functionality of loading login forms to more users.

While our default and recommended setting remains set to **Unlock**, if your organization fully secures the user browser and endpoints with sufficient enterprise policies, you may now update this requirement to support your use case.

To change the minimum permission level for the PAM browser extension plugin, please perform the procedure detailed on this [page](#).

# Using the Browser Extension with Viewer Permissions

The PAM browser extension loads records that a user has at least *Unlock* permissions to by default; however System Administrators may decrease or lower this requirement to include users with a minimum of Viewer permissions.

If lowered, then the [Browser Extension](#) will display these records but these user's will still not be permitted to *Unlock* the passwords in PAM.

Please note that if you are going to lower this requirement to Viewer, you should ensure that your client browsers and endpoints are fully secured so that the password cannot be detected by these users.

To lower the requirement, perform this quick procedure:

1. Login to PAM with a System Administrator account.
2. Navigate to Administration > Settings > Parameters.
3. Locate the parameter **Plugin Level** and use the dropdown menu to switch the choice to **Viewer**. The default value is *Unlock*.

Plugin Level  

4. Click the **Save** button to the right of this parameter.

The setting has now been saved and will be immediately available to all [Browser Extension](#) users.

## My input fields are not auto-populating

The [Extension](#) attempts to automatically read and detect input fields of various web configurations, but sometimes it does not always detect fields with alternative configurations.

If the Extension is not detecting your user or password field on your web login page, the following [page](#) will detail some steps to resolve this behavior.

## Configure Web Form Input Fields

Much like everything else on the internet, input fields on web login forms can be and are often different.

Some developers use common IDs like “username”, “user”, “email” or “password” to define the input field on forms while others use more exotic naming conventions.

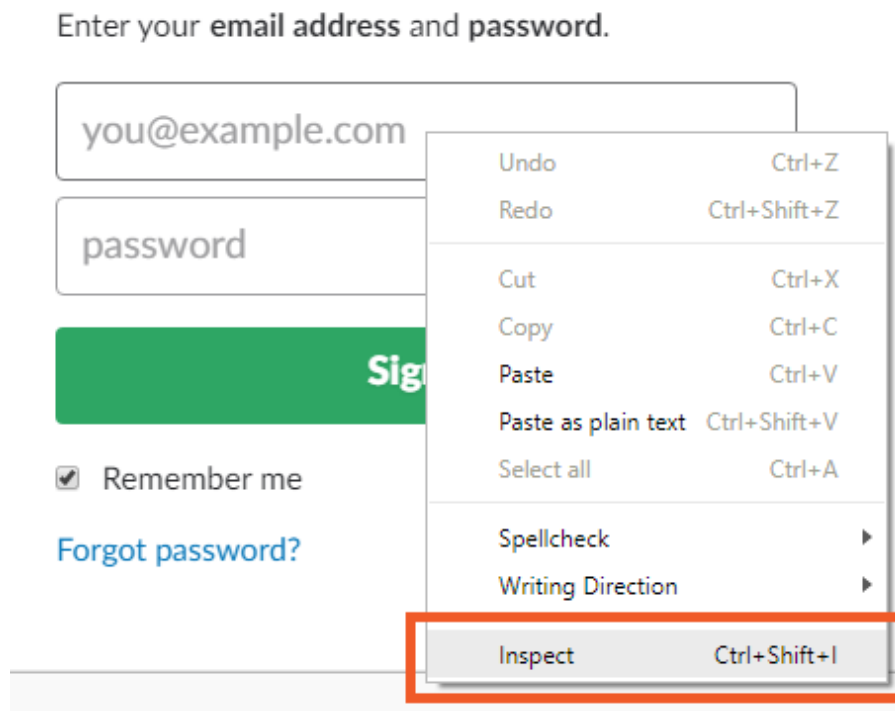
Regardless of what is used for your particular input field IDs, the extension attempts to auto-detect as many as possible; however, sometimes it needs to be told the ID explicitly.

The PAM browser extension is looking for the form input fields that contain the following as a part of its *ID*, *Name* or *Placeholder* attribute to identify the field as a user field: *Username*, *User name*, *email*, *user*, *login*, *identifier*. In addition, the input field with email type is considered a user field.

**Password fields are identified as input fields of a password type.**

If the extension is not populating your *username* or *password* field properly, please perform the following procedure.

1. Open your the web page that contains your form, right click on the input field that is not populating and select the **Inspect** or **Inspect Element** option. If you are using Microsoft Edge, you will need to first open the Developer Tools (F12 key).



2. The Developer view of your browser will now open and detail the various elements associated with your selected input field. From here, locate and copy the value defined in the "id" element of your input.

```
▼ <p class="no_bottom_margin">
...
  <input type="email" id="email" name=
    "email" size="40" value placeholder=
    "you@example.com"> == $0
  </p>
```

3. Now, log in to PAM server as a System Administrator and open the server parameters (Administration > Settings > Parameters).
4. In the **Plugin Fields** input field, paste the value copied from step 2 and click **Save**.

Content Location	<input type="text" value="\${PAM_HOME}/content"/>		Save
Content Storage	<input type="text" value="File System"/>		Save
Export Location	<input type="text" value="\${PAM_HOME}/export"/>		Save
Managed Path	<input type="text" value="http://localhost:8080/PamWeb/"/>		Save
Plugin Fields	<input type="text" value="email/"/>		Save
Session Idle Timeout	<input type="text" value="0"/>		Save
Temporary Location	<input type="text" value="\${PAM_HOME}/content/tmp"/>		Save

Please note the format of this value is *customUserID/customPasswordID*. For example, if you need to enter only a custom ID for the username field, simply enter the value followed by a slash (/). If you need to enter both a username and password field ID, then enter both with a slash (/) between them.

- Return to the browser and either *open/close* the extension or click the **Refresh** button along the bottom and try again. If it is still not working as expected, please contact our Support Team <https://support.imprivata.com/communitylogin> for assistance.

## Additional functionality of the Browser Extension

### Broker extension only [Deprecated]

The use of this extension will allow for the automatic configuration of the proxy settings (Enable and Disable) so the end-user does not need to modify settings, scripts or files manually, for example, an extension fills the placeholders (pamuser / pampassword001):

- User: **pamuser**
- Password: **pampassword001**

There are two settings for the PAM [Browser extension](#) you can set globally by navigating to Administration > Settings > Parameters > **Plugin for HTTP Proxy**.

Application Settings

Home / System Settings

Application Nodes

Proximity Groups

Database

Registration

Parameters

Mail Server

AD

Syslog

Tenants

Browser Extension

Plugin Fields

Save

Plugin for HTTP Proxy

Zero Trust

Pass Through

Zero Trust

Unblock

Save

Plugin Level

Save

If **Zero Trust** is selected, the extension will work using the placeholder credentials for login or fixed parameters in forms for managed sites (from domains), if the plugin has the Enable HTTP Broker option checked.

If **Pass Through** is selected, the extension fills user / password from your record in the same way as a **Form Filler**, not as a **Broker plugin**.

## Global parameter for Plugin for HTTP Proxy [Deprecated]

The PAM Administrator can use the Global parameter value Plugin for HTTP Proxy for all records to set *Pass Through* or *Zero Trust* to all records by default.

Note, if you set the parameter **Pass Through** for Plugin for HTTP Proxy globally, this setting will be the default for all your records and PAM users. Otherwise, you can always set the parameter locally for each record.

Even if the parameter Pass Through for Plugin for HTTP Proxy is set globally, you can do *Zero Trust* for your record. But if you set **Zero Trust** Plugin for HTTP Proxy **globally**, you cannot change this parameter in your record locally. This was made for backward compatibility with existing deployments.

Service Administrator users can add [the additional field to the record](#) to set the parameter for the browser extension. [More about available fields for additional functionality](#).

Record Type:

- Name: **PluginForHTTPProxy**
- Display name: **Plugin For HTTP Proxy**
- Type: **Choice**
- Values: **Pass Through, Zero Trust**

## Adding a Placeholder to the Record

The auto submit plugin is supported on most websites.

Some login forms have more than the user and password login fields, for example, account, company, etc. To fill the placeholder automatically using the PAM plugin, you need to create a new field in the record type with the same field name as the HTML input control name or id in this form.

If the placeholder is created, the [PAM Browser Extension](#) will take the placeholder's value and fill the form with user / password fields.

For example, <https://aws.amazon.com/> has three fields:

- Company
- Login
- Password

Usually, if the user connects to the record using the plugin PAM Browser Extension, it fills the login and password and the Company's placeholder user fills it manually.

For now, you can add the additional field and its values to your record.

Adding a new placeholder to the Record:

- Name: **The same as in the placeholder on the web portal (account ID)**
- Display Name: **How it looks like in record (whatever)**
- Type: **String**

## Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

Password

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

## Submit button

The PAM plugin works on web portals with a **Submit** button that activates the login process.

Add the **PluginAutoSubmit** to your record: display name, id or type for a login button and the Extension fills the placeholders and activates the button:

- Name: **PluginAutoSubmit**
- Display name: **Plugin Auto Submit**
- Type: **String**

The user has no login or password: Record will log in automatically using the extension.

Note: some websites make a password placeholder with a checkbox “**Look at the password**”. If you use the form filler, your password can be easily taken by the user, who can activate this checkbox and get the password. If you use the extension, it activates the submit button and the registration form moves faster. It’s still possible to get the password, but it’s hard to do if you’re using the PAM broker extension.

## Records in the Extension for Users

Records appearing in the [Extension](#) for my users.

The list of records that appear and can be selected from within the Imprivata Privileged Access Management Extension is determined by a few elements defined in Imprivata Privileged Access Management(server).

In order for records to appear, the following record and properties need to be created within PAM (server).

- A record that contains the URL to the login web portal. Most commonly, users will use the WEB Portal record type but any record type can be used as long it contains the URL (*for example, you could enter the URL into a record's Description field*).
- Within this record, the following properties need to be defined:
  - **Name:** Enter an easily recognizable name for this record that will be used for selection in the extension.
  - **URL:** Enter the URL to the login or sign in page that contains the web login form. Please note if your record type does not contain a URL field, you can enter the URL into the Description.
  - **User:** Enter the username to be populated.
  - **Password:** Enter the password for the username.

<b>Name</b>	My Office 365 Global Admin Account
<b>Description</b>	Office 365 Shared Global Admin Account
<hr/>	
<b>Url</b>	<input type="text" value="https://login.microsoftonline.com"/>
<b>User</b>	<input type="text" value="globalAdmin@xtontech.onmicrosoft.com"/>
<b>Password</b>	<input type="password" value="*****"/>

An example WEB Portal record created in PAM server to auto-populate a Microsoft Office 365 or [Azure](#) login.

- This record must be Shared to all users/groups (that you want to grant access to) with at least the **Unlock** role. You may now configure PAM to include users with [Viewer permission](#).

Grant Access

**Principal**

**Selected Principals**

John Williams ▾

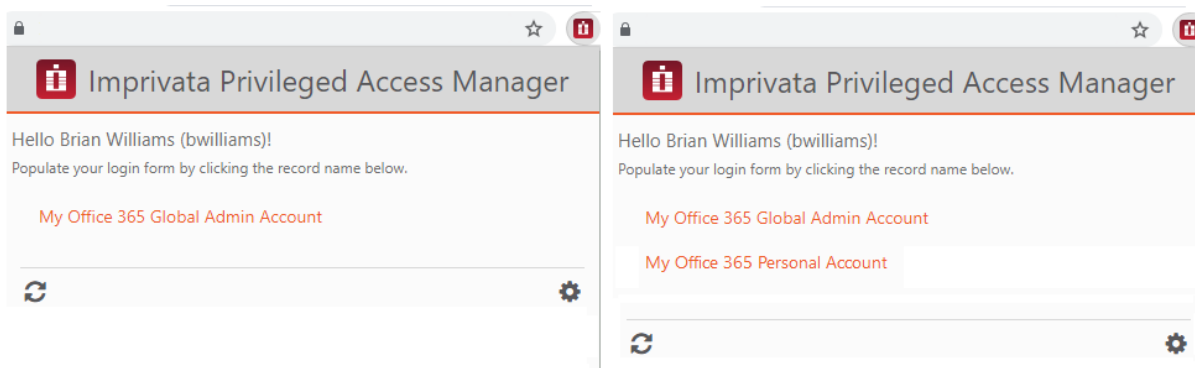
**Role**

Unlock ▾

Once this record has been created and shared, simply open your browser and navigate to the login page. Click the Imprivata Privileged Access Management extension to open and finally click the **Record Name** to auto-populate the credentials.

If only one record for this login was found, the [Extension](#) will automatically populate the credentials once opened. If two or more records are found, then the user must select and click the **Record Name** to populate the desired credentials.





A user's view of one record displayed in the Extension (left) and multiple records (right).

The Extension and Imprivata Privileged Access Management (server) communicate in real-time and do not sync nor store credentials locally on the user's computer.

If changes are made to the record or the record's shared permissions, the user can simply **open/close** the Extension **or** click the **Refresh** button to load the modifications.

## Records in Extension

The Extension reads and displays records that are stored in PAM sever's 256-bit encrypted Identity Vault. Based on the stored records and its associated permissions, the extension determines when and to whom it will allow access to the record.

To learn more about this, please read the following [page](#).

## PAM Browser Extension does not login when logging onto PAM

After installing the Imprivata PAM Broker Browser Extension, logging into the PAM website does not result in the PAM Extension being logged in.

## Troubleshooting

1. Log out of the PAM site.
2. Close all browser instances and ensure that there are no processes left running for the browser (msedge.exe, chrome.exe).
3. Re-open the browser to a bank page.
4. Clear the browser Cookies and cached images and files for the time period since installing the last 24 hours.
5. Open the browser extension and enter the correct PAM URL and then click **Login**.
6. The PAM website opens.
7. Login to the PAM website.
8. The PAM browser extension should now be auto-logged in every time you log into the PAM site.

# Recover a Lost System Administrator Account Password

The highest permission role in PAM is System Administrator and the account(s) assigned this role have elevated privileges to manage and maintain this software.

When the password for this account is lost or forgotten, it can become a potentially serious issue when it is needed to be used in PAM.

The good news is that you can recover from this situation in one of a few ways, assuming of course you have the required values.

This article will describe the methods that can be used to recover from a lost, forgotten or locked local System Administrator account password.

This article deals with local user accounts with the System Administrator role. If your System Administrator account(s) are from an external user directory like Active Directory, then of course you can manage password recoveries and unlocks from this user directory directly.

It is recommended to have at least two System Administrator accounts for this, and other reasons, related to best practices in PAM.

## Method #1

The first method describes how to reset a System Administrator account password when access to a second System Administrator account is available.

1. Login to PAM with your second System Administrator account.
2. Navigate to Administration > Local Users.
3. Locate the account of the lost or forgotten System Administrator password and click its **Edit** button.
4. Enter or generate a new password in the **Password** field.
5. Repeat the new password in the **Repeat Password** field.
6. Click the **Save** button to update the password.

You can now login to the other System Administrator account using its new password.

## Method #2

The second method describes how to reset a System Administrator account password when access to a second System Administrator account is not available. This method requires access to the PAM host server and the *Directory Password* that was generated during the installation of the software.

1. Login to the PAM host server and open a command prompt. This may require elevated or Admin privileges.
2. Using this prompt, navigate to the directory where the System is installed (`$PAM_HOME`).
3. From `$PAM_HOME`, enter the following command, replacing the placeholders in red with the values specific to your PAM instance.

Windows:

```
1 | bin\PamDirectory.cmd SetUserPassword web directoryServices.password  
systemAdmin.login -
```

Linux:

```
1 | bin/PamDirectory.sh SetUserPassword web directoryServices.password  
systemAdmin.login -
```

**directoryServices.password** – is the Directory Password that is generated when PAM is installed on the node.

**systemAdmin.login** – is the login name of the System Administrator account that will have its password reset.

For example, to reset the password of your *pamadmin* account:

Windows:

```
1 | bin\PamDirectory.cmd SetUserPassword web u8DwvPE3y7itAS pamadmin -
```

Linux:

```
1 | bin/PamDirectory.sh SetUserPassword web u8DwvPE3y7itAS pamadmin -
```

4. When prompted for **New Password:**, enter the new password for this System Administrator login account.

If successful, then you will receive an **Ok** response.

```
1 | c:\pam>bin\PamDirectory.cmd SetUserPassword web u8DwvPE3y7itAS pamadmin -  
2 | New Password:  
3 | Ok
```

You can now login to this System Administrator account using its new password.

## Method #3

The third method describes how to reset a System Administrator account password when access to a second System Administrator account is not available. This method requires access to the PAM host server and the *Master Password* that was generated during the installation of the software.

This method differs from the second method by creating a new local user account and then assigning this new account the System Administrator role. When completed, you can then use this new System Administrator account to reset the original System Administrator account using [Method #1](#).

1. Login to the PAM host server and open a command prompt. This may require elevated or Admin privileges.
2. Using this prompt, navigate to the directory where the System is installed (\$PAM\_HOME).
3. From \$PAM\_HOME, enter the following command to create a new local user, replacing the placeholders in red with the values specific to your PAM instance.

If you already have another existing local user account and do not wish to create a new one, you can skip this step for creating the account and proceed to the next to grant an existing one the System Administrator role.

Windows:

```
1 | bin\PamDirectory.cmd CreateUser web user.login user.firstname user.lastname user.password
```

Linux:

```
1 | bin/PamDirectory.sh CreateUser web user.login user.firstname user.lastname user.password
```

**user.login** – is the login name for the new local user account.

**user.firstname** – is the first name for the new local user account.

**user.lastname** – is the last name for the new local user account.

**user.password** – is the password for the new local user account.

For example, to create a new local account with the login *backupadmin*, the full name *Backup SysAdmin* and the password *Password123*:

Windows:

```
1 | bin\PamDirectory.cmd CreateUser web backupadmin Backup SysAdmin Password123
```

Linux:

```
1 | bin/PamDirectory.sh CreateUser web backupadmin Backup SysAdmin Password123
```

4. Next, we will assign this new local account or your existing local account the System Administrator role. From \$PAM\_HOME, enter the following command to assign the System Administrator role to a local account, replacing the placeholders in red with the values specific to your PAM instance.

Windows:

```
1 | bin\PamDirectory.cmd DBMakeAdmin web user.login master.password
```

Linux:

```
1 | bin/PamDirectory.sh DBMakeAdmin web user.login master.password
```

**user.login** – is the login name for the account that you wish to assign the System Administrator role.

**master.password** – is the Master Password that is generated when PAM is installed on the node.

For example, to assign the local account *backupadmin* the System Administrator role:

Windows:

```
1 | bin\PamDirectory.cmd DBMakeAdmin web backupadmin  
XzMFU88xFvgUeoKh03C6Tkman94KvN5M
```

Linux:

```
1 | bin/PamDirectory.sh DBMakeAdmin web backupadmin XzMFU88xFvgUeoKh03C6Tkman94KvN5M
```

If successful, then you will receive the response:

```
1 | c:\pam>bin\PamDirectory.cmd DBMakeAdmin web backupadmin  
XzMFU88xFvgUeoKh03C6Tkman94KvN5M  
2 | Found the user  
3 | Admin created
```

You can now login to PAM using the new account with the System Administrator role and use [Method #1](#) to reset the password of the first System Administrator account. Afterward, you can use the first System Administrator account to remove this new account's System Administrator role or keep it around as-is in case it is needed in the future.

Please keep in mind that this new account does indeed have the full privileges of the System Administrator role and should be secured with the same measures as all other System Administrator accounts.

## Locked System Administrator Account

This last method is not necessarily due to a lost or forgotten password, but could be the result of trying to login too many times with the incorrect password which resulted in the System Administrator account being locked.

1. In this situation, you could use a similar approach to Method #1 described above.
2. Login to PAM with your second System Administrator account.
3. Navigate to Administration > Local Users.

4. Locate the account of the locked System Administrator account and click its **Edit** button.
5. Click the **Unblock** button.

This account is now unlocked and you can try to login again.

If there is not a second System Administrator account, then you will need to use [Method #3](#) as described above to create a new local account or assign the System Administrator role to an existing account and then use this new account to Unblock your current System Administrator account.

## Licensing Guidelines

The following article describes the various license or activation guidelines that are implemented in PAM, why you may be out of compliance with your activated key and how to bring yourself back under compliance.

Of note, the license guidelines messages will only appear to those users with either the System Administrator or Auditor [global role](#).

## Application Node License

When activated, your license key contains a total number of Application Nodes that you have been issued.

When the total number of configured Nodes in your PAM deployment exceeds your license amount, the following message will appear within the software where x represents the total number of nodes allowed and y represents the total number of nodes currently in your deployment:

The application exceeded a number of x licensed nodes. Please remove any inactive nodes from your existing count of y using the [Administration / Settings / Application Nodes](#) page or contact your Account Representative for additional information.

To view the current Application Nodes in your deployment, navigate to the Administration > Settings > Application Nodes tab.

On this page, each Application Node will be displayed and is calculated by the number of unique nodes deployed.

A unique node is considered one that has a unique Host Name.

For instance, the following represents a common scenario where two application nodes are listed but are only counted as one because they have the same Host name **xtamServer**:

```
1 | xtamServer:Worker
2 | 2.3.201907212255 / 07/26/2019 12:04
3 | xtamServer:GUI
4 | 2.3.201907212255 / 07/26/2019 12:04
```

Another instance represents a common scenario where PAM is configured in a High Availability configuration where four application nodes are listed but are only counted as two:

```
1 | xtamServerNode-A:Worker
2 | 2.3.201907212255 / 07/26/2019 12:04
3 | xtamServerNode-A:GUI
4 | 2.3.201907212255 / 07/26/2019 12:04
5 | xtamServerNode-B:Worker
6 | 2.3.201907212255 / 07/26/2019 12:04
7 | xtamServerNode-B:GUI
8 | 2.3.201907212255 / 07/26/2019 12:04
```

If you find yourself out of compliance with your Application Node license guidelines, then the following options are available to bring yourself back into compliance:

- Uninstall or shutdown unused or extra nodes from your PAM server farm. After that, remove these nodes from your vault by clicking the **Edit** button located in your node's Actions menu and then click the **Remove** button. When the node appears online again, it will create a configuration record in the list of Application Nodes again with the default configuration. Or:
- Contact your Account Representative to purchase additional Application Nodes for your license.

## Remote Session Manager Node License

Similar to the above Application Nodes, you are also restricted by the number of Remote Session Manager nodes that can be included within your licensed PAM deployment.

When the total number of configured Session Manager Nodes (known as [Proximity Groups](#)) in your PAM deployment exceeds your license amount, the following message will appear within the software where **x** represents the total number of Proximity Groups allowed and **y** represents the total number of Proximity Groups currently in your deployment:

The application exceeded a number of **x** licensed remote session manager nodes. Please remove any inactive session managers nodes from your existing count of **y** nodes using the [Administration / Settings / Proximity Groups](#) page or contact your Account Representative for additional information.

To confirm your current deployment of Session Manager Nodes or [Proximity Groups](#), navigate to the Administration > Settings > Proximity Groups tab.

Each [Proximity Group](#) listed will be counted towards the license regardless of its current connectivity status.

If you find yourself out of compliance with your **Remote Session Manager Node** license guidelines, then the following options are available to bring yourself back into compliance:

- Remove any additional unused or extra nodes from your deployment by clicking the **Edit** button located in your proximity group's *Actions* menu and then click the **Delete** button. This will permanently remove this node from your PAM deployment so please understand the significance of each proximity group before removing it from your deployment. Or:
- Contact your Account Representative to purchase additional Remote Session Manager Nodes for your license.

# User Count License

When activated, your license key may contain a total number of Users that are permitted to use PAM. When the total number of Users in your PAM deployment exceeds your licensed amount, the following message will appear within the software where **x** represents the total number of users allowed and **y** represents the total number of users currently in your deployment.

The application exceeded a number of **x** licensed users. Note that the User Access report is collected once a day so there could be delay in calculation. Please review your [Access Report](#), listing **y** users, located at Administration / Global Permissions / Access Report or contact your Account Representative for additional information.

A user is counted against the license when they have been given permission to access an object in PAM, regardless if they ever logged in and accessed it. Keep in mind that users can be given permission to an object directly or by simply being a member of a group that was given permission to an object.

To generate a report containing your current list of licensed Users, navigate to Administration > Global Permissions > [Access Report](#).

This report will list all users that have permissions to access any object within PAM and the level and means by which they are granted this access.

If you find yourself out of compliance with your User Count license guidelines, then the following options are available to bring yourself back into compliance:

- Remove the permissions of any unused, test or extra Users from your PAM objects. This can be done by finding the user(s) in the Reports > [Users report](#), using the View Objects option to determine which objects they have permissions to and then removing them where necessary. Once all permissions have been removed for the user, they will no longer be counted towards the license's User Count. Or:
- Contact your Account Representative to purchase additional Users for your license.

# Record Count License

When activated, your license key may contain a total number of Records that are permitted to be created in PAM.

When the total number of Records in your PAM deployment exceeds your licensed amount, the following message will appear within the software where **x** represents the total number of records allowed and **y** represents the total number of records currently in your deployment.

The application exceeded a number of **x** licensed records. The current count is **y**. Please remove any extra records or contact your Account Representative for additional information.



To generate a report containing your current list of Records, navigate to Reports > Inventory.

This report will list all objects that are currently within the PAM Identity Vault.

In the [Inventory Report](#)'s Search box, enter the query records to filter out all *Vaults* and *Folders* so you have a complete report of only the *Records*.

If you find yourself out of compliance with your **Record Count** license guidelines, then the following options are available to bring yourself back into compliance:

- Delete any records that are no longer needed such as those that were being used for testing. Or:
- Contact your Account Representative to purchase additional Records for your license.

## Expired License

When your license expires, you will still have full access to all objects within PAM; however, you will not be permitted to *Create* new objects (Vaults, Folders or Records), *Connect a session*, or *Execute* tasks.

When your license has expired, you will see the following message:

The application license has expired. Please contact your Account Representative for additional information.

And if anyone attempts to create a new record, they will receive the following message:

New records cannot be created because the license has expired.

New folders cannot be created because the license has expired.

If a user attempts to Connect a session, they will receive the following message:

Connection could not be created because the license has expired.

If a user attempts to Execute a task, they will receive the following message:

Job could not be executed because the license has expired.

To extend or renew your license, you must contact your Account Representative.

If questions remain or issues arise while using PAM, please contact our Support team:

<https://support.imprivata.com/communitylogin>.

# Administrators and Power Users

---

## Getting Started

This guide is designed to provide both Administrators and Users of Privileged Access Management (referred to as PAM) details about how to locate and use the functionality within the software.

At the conclusion of this guide, a user should be proficient in the basic usage of the Imprivata Privileged Access Management solution.

NOTE: PAM is permission trimmed based on the current user's level of access. The documentation will detail available options regardless of your permissions, meaning some included options or features may not be visible to you due to a lack of permissions, because it has been disabled by the System Administrator or it is a limitation of your software license.

## Technical Support

If questions remain or issues arise while using PAM, please contact our Support team:

<https://support.imprivata.com/communitylogin>.

## Other Documentation

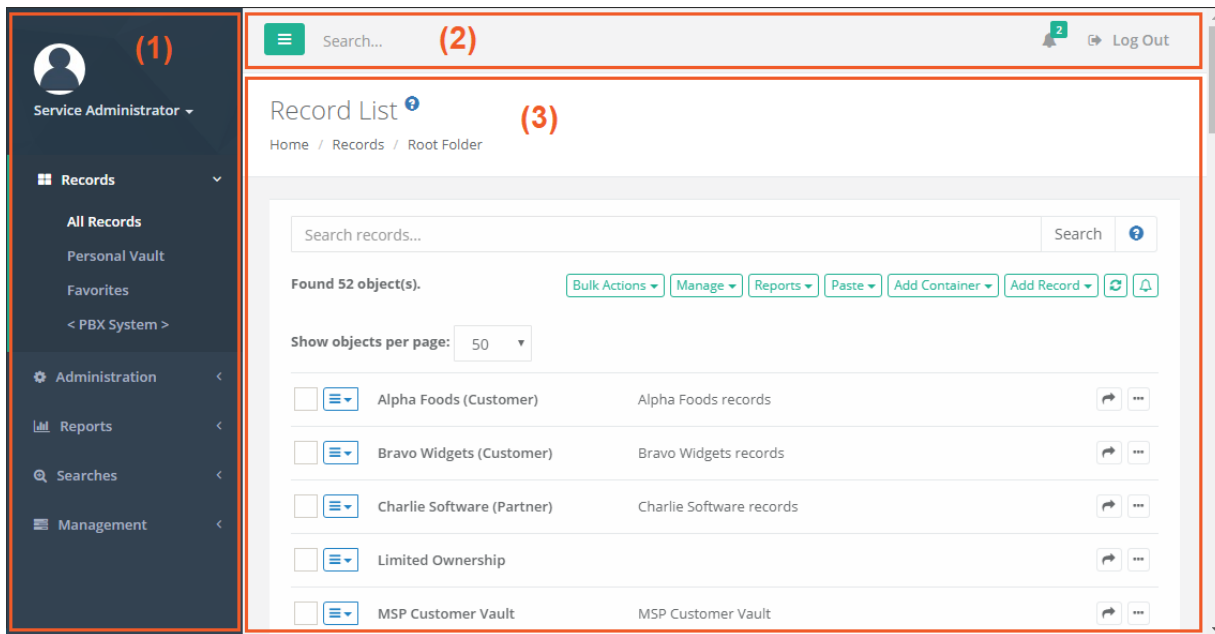
In addition to this guide, the following information is located on the website:

- [Windows Installation Guide](#)
- [Unix/Linux Installation Guide](#)
- [System Requirements](#)
- [System Recommendations](#)

## Navigating the User Interface

The Privileged Access Management (PAM) interface is divided into the following main sections:

1. [Navigation Menu](#)
2. [Application Toolbar](#)
3. [Record List](#)



**TIP:** Throughout the software you will notice many interactive Help buttons. If you are curious about what an option or function does, click its **Help button** for a short description or a link to an online FAQ article for more information.

## Navigation menu

The navigation menu along the left side of the interface is the main navigation used for PAM. For ease of use, it is divided into several sections:

### User Settings

The top most section that displays the currently logged in user name, their profile picture (displayed only if one is defined in Active Directory or the Local User account) and a dropdown menu of [individual user settings](#).

### Records

The location where all records and containers will be organized and accessible by users based on their shared permissions.

#### *All Records*

Displays all record and folders that this user has permissions to access. A user with at least the Viewer Record Control will see the object in the All Records view. If the user does not have Viewer, then the object will not appear in this or any view or search performed by them.

The All Records view is also known as the Root Folder or Default Root.

#### *Shared With Me*

Displays all records and containers that this user has permissions to access. This differs from the All Records view because it allows the user to see records in a simple flat view, without having to navigate through

folders to locate records.

If a user has permission to a record, but not the folder which contains this record, then they could use this **Shared With Me** view to locate the record. Note that System Administrators do not have a *Shared With Me* option because they have access to all objects.

### *Personal Vault*

Each user has their own Personal Vault for which they are owners. This allows them to create their own records and folders, maintain full control over each one and share or revoke permissions as needed.

### *Favorites*

Records and Folders that are favorited by a user will appear in this personalized view. Favorites are user profile specific meaning that only objects favorited by the currently logged in user will appear in their own Favorites view.

### *<Favorite Folders>*

When a user favorites a folder, this folder will appear in the *Favorites* section in addition to being shown within the *Records* section. This enables the favorited folder to become a quick navigation link to access its content.

Favorite folders appear on the navigation menu in this format *<Folder Name>*.

## Administration

This section is available to System Administrators and Auditors only (see [Global Roles](#)) and is used to configure administrative and global settings of PAM. Users without this permission will not be able to see or access this section.

### *Global Permissions*

Defines the users or groups who are granted global access via shared permissions. Users with global permissions will have access to all PAM records or containers regardless of the specific permissions that are configured on each object.

See the [Global Permissions](#) section for more information.

### *Global Roles*

Defines the users or groups who are granted system wide access of varying roles.

See the [Global Roles](#) section for more information.

### *Local Users*

Location where user accounts can be created and managed within PAM system. These users are stored within PAM only and cannot be used with Active Directory, LDAP or external groups.

See the [Local Users](#) section for more information.

### *Local Groups*

Location where groups can be created and managed within PAM system. These groups are stored within PAM only and cannot be used with Active Directory, LDAP or external groups.

See the [Local Groups](#) section for more information.

## *Discovery*

Location where activity based Privileged Account and System discovery queries are configured and their results can be viewed.

See the [Discovery Query](#) section for more information.

## *Scripts*

The location of all scripts that are stored in PAM that can be used with Task execution. Scripts located in this library can be created, modified and deleted.

See the [Scripts Library](#) section for more information.

## *Record Types*

Defines the out of the box and custom Record Types that are available for use in PAM.

See the [Record Types](#) section for more information.

## *Tokens*

Displays a list of all generated API tokens with the options to create, disable, expire or delete existing tokens.

See the [Authentication Tokens](#) section for more information.

## *Workflows*

The location where approval workflows are created and managed.

See the [Workflows](#) section for more information.

## *Command Control*

Displays a list of all Command Control policies with the options to create and manage existing policies.

See the [Command Control](#) section for more information.

## *MFA*

The location where PAM logins are configured to require a specific MFA provider for authentication. MFA providers can be assigned to individual users, groups or a default option can be applied globally for all logins including a *none* option to disable the MFA authentication requirement.

See the [MFA Configuration](#) section for more information.

## *Behavior Profiles*

The location where PAM Behavior Profiles are created and managed by System Administrators.

See the [Behavior Profiles](#) section for more information.

## *Settings*

The location where the PAM system is configured.

See the [Settings and Configuration](#) section for more information.

## *Updates*

Displays the current version of PAM and provides the ability to update to the latest available version.

See the [Updates](#) section for more information.

# Reports

A series of built-in reports that help to locate objects, find user activity, understand permissions and view audit events throughout the system are provided to PAM System Administrators and Auditors (see [Global Roles](#)). Users that lack this permission will not be able to access this section.

These reports have options to *Sort, Filter, Search, Refresh, Export, Email* and *Enable / Disable Columns* using their available commands.

Access	Provides a list of all users (unwound from groups) that have access to the selected object, their level of access and how they have been granted access (Group Membership, Individual ACL, Global Role or Global Permission).
Audit Log	Provides a report of audit events captured throughout the PAM solution by all users and activities. Use this report to investigate Audit Events in PAM.
Bindings	Provides a list of all users (unwound from groups) that have workflow bindings to the selected object, a summary of their binding configuration and how they are bound (group membership or by direct assignment).
Custom	Provides a location to create and view any custom reports that have been generated. These custom reports, written in the HQL querying language, are written and maintained by System Administrators.
Inventory	Provides a list of all objects (records and folders) along with their metadata and permissions. Use this report to find objects based on metadata, activity or permissions.
Job History	Provides a list of all Jobs or Tasks that have already been executed, along with their details. Use this report to find details about scheduled or previously executed tasks.
Job Summary	Provides a list of all Jobs or Tasks that have already been executed, aggregated to illustrate a summary of their results including a number of executions per task per day. The summary can be displayed in a data-table or presented in a line chart.
Requests	Provides a list of all Workflow Instances, including those that are active, approved and rejected. Use this report to find any information about Workflow instances and states.
Sessions	Provides a list of all Active and Completed remote sessions in PAM. Use this report to investigate session activity and to access video and keystroke recordings.
Session Events	Provides a list of all keystrokes, clipboard text and command sequences users entered during any remote session. Use this report to investigate session activity and search for keystroke or command entries throughout all sessions.
Statistics	Provides a graphical understanding of various categories of objects throughout the PAM system. Use these reports to understand system usage and various trends over time.


Subscriptions (Alerts)	Provides a list of alerts that the users' of PAM are subscribed to, along with their alert configuration and an option to Unsubscribe them from their selected alert(s).
Subscriptions (Reports)	Provides a list of reports that the users' of PAM are subscribed to, along with their report configuration and an option to Unsubscribe them from their selected report (s).
Tasks	Provides a list of all records that have at least one task associated to them, along with each task's details.
Users	Provides a list of all users and groups that have accessed PAM. Use this report to understand user behavior, activity, permissions and IP based locations.
Workflows	Provides a list of all PAM workflows along with their templates, bindings and configuration. Use this report to understand where Workflows are deployed and how they are configured.
Custom Reports	Provides the ability for System Administrators to create custom PAM reports using the HQL language.

For an expanded list of reports, their description and available options, please read our [Reports article](#).


## Searches

The Searches menu will provide quick access to all default search queries included with PAM and to any custom search queries that you have made a favorite. Any custom created search favorites are only available to the user who created it, they cannot be shared between multiple users or made to be a default system query.

To add a custom search query to your Searches menu:

1. Navigate to any Records page, enter your Search query into the *Search records...* field and execute the query by clicking the **Search** button.
2. Once the query is executed, click the **Add to Favorites** button (.
3. Your custom query will now be visible in your Searches menu.

### To remove a custom search query from your Searches menu:

1. Navigate to the Searches menu and click on your custom query that you would like to remove.
2. This will open and execute the selected Search query.
3. Once the query has executed, click the **Remove from Favorites** button () to remove your custom query.

## Management

While much of PAM is configured with Global Settings, there are several options that allows a user to configure PAM options for their personal preference. These personal settings are available to each user in the following locations:

- In the upper portion of the left navigation menu activated by a dropdown menu.
- In the lower portion of the left navigation menu located within the *Management* section.

The following settings are available:

## *My Sessions*

Displays a list of session activity that this user has permissions to access.

## *My Profile*

Displays information about this user's profile, including account parameters, subscribed notifications and custom user settings.

### **Profile**

Displays your account information.

For PAM user accounts that exist outside of the PAM local user directory, this will be a read only view of your account information as configured in your external user directory (for example, Active Directory).

For PAM local user accounts, this will be an editable view of your account information as configured in the PAM internal user directory. You can update your account information, including profile picture, name, email and password.

### **Subscriptions**

Displays all alerts and notifications that you are currently subscribed to and the ability to subscribe or unsubscribe from additional object notifications.

### **Anonymous Links**

Displays all active anonymous links that you have created.

You may create new anonymous links or expire currently active anonymous links that you have authored from this page.

### **Preferences**

Displays all current user specific profile options for your account in PAM.

Click the **Help** button ( ? ) available for each preference option for a description of the parameter.

After you update any preference setting, be sure to click its **Save** button before exiting the page.

## *My Alerts*

Displays all alerts that have been sent to this user.

## *My Workflows*

Displays all requests that a user has created, the *My Requests* tab, and all requests that this user must approve or reject, the *Requests for Approval* tab.


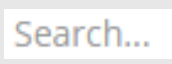


## *About*

Displays the copyright information and the current version number of the PAM system.



# Application Toolbar

The PAM application toolbar is located along the top of the interface. It contains these options:

	A menu option to collapse or expand the navigation menu to provide more a compact view for users with low screen resolutions.
	A <i>Search...</i> bar used to search for menu options in the left navigation menu or objects stored in the vault.
	An alerts indicator that provides a display of any unread user alerts and used as a quick link to open the user's <i>My Alerts</i> view.
	A logout button used to log out of the current user's session. After you successfully logout of PAM, be sure to exit or close your web browser.

## Login and Logout

Any user will be able to login to PAM using their account name and password. Depending on the configuration, this account may be the user's Active Directory login or a Local User created in PAM.

To login to PAM:

1. Open your browser to PAM login page. The default location is <https://localhost:6443/xtam> but may be different depending on your system. Contact your PAM System Administrator to access for your login page.
2. On the login page or login prompt, enter your account name and password. Click **Login** to continue.
3. Upon successful login, you will be directed to the PAM home page. If unsuccessful, please try again.

NOTE: If your login authentication requires the use of Multi-Factor Authentication, please refer to our online [MFA article](#) for detailed information about your first time use and device registration. If you use SSO, then click for the red SSO button on the login page to be redirected to your SSO sign-in portal. Speak with your PAM System Administrator for additional assistance using your MFA or SSO options.

To logout of PAM:






1. Locate and click the **Logout** button either in the dropdown menu beneath your login profile or in the application's toolbar.
2. Once logged out, for security measures, it is recommended to fully close your web browser.

## Record List

The Record List is a permission trimmed view of all objects (records, folders and vaults) that the currently logged in user has access to view. Vaults are displayed first, followed by Folders and finally Records in alphabetical order.

The object’s *Name*, *Description*, *Linked Parent paths*, *Record ID*, *Record Type* and *Host* are also displayed in this view.

Additional options are provided by clicking on the object’s Icon to activate its dropdown menu or by clicking the desired option in the list located on the right side of each object.

 Connect	The connect option establishes a remote connection to any record that supports this feature.
 Execute	The execute option opens a menu that displays a list of tasks that can be executed on this record.
 Quick View	The quick view option will open a view only display of the selected record. You can use this option to view, copy or unlock record fields, but it cannot be used to manage the record.
 Share	The share option opens the Grant Access dialog for quick sharing of objects. Using this share button will <u>automatically break inheritance</u> of this object. If you do not want to break inheritance, then open the object and use its Manage > Permission option to configure your sharing.
 Actions	The action menu opens a set of options that are also available in the object’s Icon dropdown menu on the left side.

Go to Parent

Bulk Actions ▾

Manage ▾

Reports ▾

Paste ▾

Add Folder

Add Record ▾







## Go to Parent

The Go to Parent option will navigate you to the current object’s parent. If the current record has multiple parents (i.e. linked objects) then the *Go to Parent* button will generate a dropdown menu for you to choose the desired parent.

## Bulk Actions

The Bulk Actions menu provides a list of operations that can performed when one or more objects in the Record List are selected.

Based on your account permissions, the following options may be accessible from the *Bulk Actions* menu

Select All	Selects all objects (vaults, folders and records) visible in the current record list view.
Select Records	Selects only the records visible in the current record list view.
Request Access	Used to submit the same Request Access workflow for the Connect action to all the selected records.

Request Unlock	Used to submit the same Request Access workflow for the Unlock action to all the selected records.
Request Execute	Used to submit the same Request Access workflow for the Execute action to all the selected records.
Execute	Used to bulk execute On-Demand tasks associated to the selected records.
Share	Used to bulk share the selected objects. Using this Share option will break permission inheritance on all selected objects.
Inherit Permissions	Used to set the permissions of the selected objects to inherit permissions from their parent.
Inherit Workflows	Used to set the bindings of the selected objects to inherit workflows from their parent.
Update	Used to assign a new Record Type or Reference Record for all selected records.
Unselect All	Unselect all the currently selected objects.
Copy	Add the selected objects to the clipboard to be copied to a new location.
Copy Folders	Add the selected folders, including their sub-folders and permissions, to the clipboard to be copied to a new location. This option does not include records.
Cut	Add the selected objects to the clipboard to be moved to a new location.
Delete	Deleted the selected objects.

## Manage

The Manage menu provides a list of operations that can be performed within the current container.

### *Import*

Import an existing list of records from a third-party provider using a common CSV format.

Please read our article for additional information about [importing records](#).

### *Permissions*

Grant, Edit or Revoke permissions associated to your current container.

### *Workflows*

Apply, Edit or Remove workflow bindings associated to your current container.

### *Local Users*

Create and Manage local users that are specific to this container.

Not available in the Root Folder, Personal Vaults or if the feature has been globally disabled by a System Administrator.

## Local Groups

Create and Manage local groups that are specific to this container.

Not available in the Root Folder, Personal Vaults or if the feature has been globally disabled by a System Administrator.

## Tokens

Create and Manage API tokens that are generated specific to this container.

Not available in the Root Folder, Personal Vaults or if the feature has been globally disabled by a System Administrator.

## Reports

Generate the selected report containing only the objects that reside within this current container.

## Paste

Paste or Paste as a Link your current clipboard object(s) to your current container.

## Add Container / Add Folder

Create a new Folder or Vault within your current container.

Please note that Vault containers can only be created in the root All Records view.

## Add Record

Create a new Record within your current container based on the Record Type that is selected from the dropdown menu.

## Refresh

Refresh the current Record List.

## Subscribe to Alerts

Subscribe to alerts associated to your current container.

## Add / Remove from Favorites

Creates a link in your Favorites menu to the selected record or container.

Click a second time to remove this object from your Favorites menu.

# Application Settings

## Global Parameters: Access

## Aggregated Email Notifications

Enable to aggregate multiple [email notifications](#) to reduce mail traffic for mass notifications.

## Alert Notification Attempts

The maximum number of notification delivery attempts for alerts.

Once this maximum number of attempts has been reached for an alert, the notification will no longer be processed.

## Anonymous Links

The parameter enables the option to share sensitive information with anonymous users using uniquely generated links with expiration terms.

Generic option disables [anonymous link](#) sharing for [records](#) while allowing sharing messages on the user profile.

## Create Audit Log for CAS Login Events

This parameter is responsible for creating an Audit Log for CAS login events.

## Date Format

This parameter defines the date and time format that is used in PAM.

For example, the default value **MM/dd/yyyy HH:mm:ss** represents 10/25/2023 15:27:33 (October 25, 2023 at 3:27:33 PM).

Use the following example patterns to help construct your date and time format:

**MM** to represent the two digit numerical month of the year using a zero pad if needed.

**dd** to represent the two digit numerical day of the month using a zero pad if needed.

**yyyy** to represent the four digit calendar year.

**HH** to represent the two digit hour of the day in a 24-hour cycle using a zero pad if needed.

**mm** to represent the two digit minute of the hour using a zero pad if needed.

**ss** to represent the two digit second of the minute using a zero pad if needed.

## Delegation of User Management

This parameter enables folder owners to manage vault- or folder-level users, groups and API tokens.

Note that vault- or folder-level users and groups could only be used in their home folder and its subfolders. API tokens could be only created for the folder-level users of the same folder.

## Group Cache TTL

Short term group membership cache TTL in minutes.

The application caches group membership information for a logged in user to optimize access to user directories.

The smaller this parameter is the more frequently the application queries user directory for the user group membership to check permissions to access certain objects or operations.

To force reset the cache before TTL expiration please use the control on the settings screen.

## Health Check Process

Enables or disables periodic [Health Check](#) Process that verifies the up-time status of various system components.

## Managed Path

Application URL to use by the clients.

## Password Expiration Warning

This parameter enables password expiration warning alert for [Active Directory](#) integrated users in 5 days to password expiration.

## Proxy Server

This parameter defines proxy server configuration to access application updates.

The parameter should be specified in the format *host:port*.

## Record Cache TTL

Short term record cache TTL in minutes. The application caches record information to optimize retrieval of frequently accessed records. The smaller this parameter is, the more frequently the application queries the record data from the database. The larger the value is, the memory usage will increase. If set to 0 then it will disable the cache. Enabling **xtam.perflog\*** properties will provide record cache usage information.

## Restrict Scripts View

This option limits which roles can view scripts within the software.

When Enabled, only users assigned the Global Role: System Administrator or Global Role: Auditor role may view scripts. When Disabled, which is the default state, more users with varying degrees of permissions are able to view scripts using the software.

It is recommended to leave this parameter **Disabled** to allow for the intended use and full functionality of task execution in the software. It is also recommended to not include sensitive or privileged credentials or values in a script, but rather use [Script Variables or Placeholders](#) to reference these if possible.

## Split View Role

This parameter enables the [Split View](#) option allowing to split passwords into different segments for two person access.

When enabled this parameter specifies whether the first or the last part of the password will be displayed to members of the [Split View](#) global role following the **Unlock** operation.

## User Input Validation

This parameter adds additional layer of validation for user inputs like records password.

Provide space-separated placeholders for more protection of user's input against command injection

There are two types of placeholders:

- **regex()** - accepts regular expression as a value
- **str()** - accepts single character of string value

Placeholders formatting rules:

- Placeholders must be separated by space
- Placeholders value can not be empty
- Placeholders value max size is 10 characters
- Placeholders can be put in any number and combination

Example: `str(whoami) regex(.*>.*) str(host) str(')` - will forbid any text in input like whoami, host or single quote character. Regular expression will validate against combination `/>` in input.

## Visible Unlock

The parameter enables the option to display the value of the secret field on the screen right after the unlocking operation without the need to click the **Reveal** button.

This option is disabled by default requiring a user to reveal the unlocked secret value or to copy it to the clipboard in attempt to avoid unnecessary secret exposure.

## Window Title

This parameter defines a prefix for the page title in the browser window.

Use the value blank to remove the prefix.

## Other System Settings

[Global Parameters: Access](#)

[Global Parameters: Browser Extension](#)

[Global Parameters: Discovery](#)

[Global Parameters: Drivers](#)

[Global Parameters: Jobs](#)

[Global Parameters: Preference](#)

[Global Parameters: Proxy](#)

[Global Parameters: Sessions](#)

[Global Parameters: Storage](#)

[Global Parameters: Workflow](#)

## Global Parameters: Browser Extension

### Access Request Scope

This global parameter controls the access request scope for WEB Portal records when used by the browser extension. Possible values are the following

**Unlock** (default) - Browser extension requires Unlock request approval to access WEB Portal credentials information. This is default behaviour for all records.

**Connect** - Browser extension requires 'Connect' request approval for records types with HTTP session manager to allow browser extension to access credential data to fill the WEB Portal form.

'Connect' option is useful in the situations when HTTP Proxy connect, protected by a workflow binding, follows the operation of filling the WEB Portal login form with the credentials from the same record (that by default requires Unlock access approval).

Note that enabling the 'Connect' option allows users with 'Unlock' permissions, but blocked by request requirements, to access credentials on record after requesting 'Connect' access by using the browser extension and debugging WEB Portal DOM model in their browser.

## Plugin Fields

Custom user and password field IDs on login forms for form filler plugin.

Specify a comma-separated list of user field patterns following by a slash and a comma-separated list of password field patterns.

## Plugin for HTTP Proxy

Defines Browser Extension Plugin integration strategy with HTTP Proxy when HTTP Proxy is enabled:

- [Pass Through](#) - Browser Extension Plugin will fill user and password fields from the selected record associated with the open WEB Portal.
- [Zero Trust](#) - Browser Extension Plugin will fill user and password fields from the user and password placeholders for HTTP Proxy to fill when submitted.

## Plugin Level

Defines the minimum permission level ([Record Control](#)) that a user must have in order to access the record using the [Browser Extension Plugin](#).

The default value is **Unlock** and is the recommended level. If the level is decreased to **Viewer** then you must ensure that your client browsers and endpoints are fully secured so that the password cannot be detected.

## Other System Settings

[Global Parameters: Access](#)

[Global Parameters: Browser Extension](#)

[Global Parameters: Discovery](#)

[Global Parameters: Drivers](#)

[Global Parameters: Jobs](#)

[Global Parameters: Preference](#)

[Global Parameters: Proxy](#)

[Global Parameters: Sessions](#)



[Global Parameters: Storage](#)

[Global Parameters: Workflow](#)

## Global Parameters: Discovery

### Discovery Query Execution Frequency

Discovery Query Execution Frequency in minutes.

### Other Global Parameters

[Global Parameters: Access](#)

[Global Parameters: Browser Extension](#)

[Global Parameters: Discovery](#)

[Global Parameters: Drivers](#)

[Global Parameters: Jobs](#)

[Global Parameters: Preference](#)

[Global Parameters: Proxy](#)

[Global Parameters: Sessions](#)

[Global Parameters: Storage](#)

[Global Parameters: Workflow](#)

## Global Parameters: Drivers

### Azure AD MFA Domain

Enter the Azure AD Account domain. This will be used for Azure AD MFA and extended current username. The login name will be automatically formatted like this: *'current-username'@'domain'*

### Azure App Id

Enter the App Id associated with your Azure tenant.

This will be used for resetting passwords for both [Azure and Office 365](#) accounts.

### JWT Signing Key

The system uses JWT Signing Key to sign REST API Tokens and to verify the signature of the tokens for REST API access using tokens in deployments including Federated Sign-In component.

The system automatically generates JWT Signing Key and deploys it to the [Federated Sign-In](#) module during the system initialization.

Use this parameter to update JWT Signing Key copied from the other system to reuse tokens generated by the other server.

To verify JWT Signing Key deployment in [Federated Sign-In](#) component and also to copy the key from the other server use the key reported in Management / About / SSO JWT Signing Key.

The version history all of previous JWT Signing Keys can be viewed from Management / About / SSO JWT Signing Key / History. An Admin would be able select one of the previous JWT keys to restore if needed.

## WS-Management Delay

WS-Management delay specifies the delay in seconds between authenticating in the remote Windows computer using WS-Management protocol and executing the remote command.

The parameter allows time for the WS-Management Host service to initialize from **Opening** to the **Opened** state.

## WS-Management Timeout

WS-Management timeout in seconds specifies network as well as command execution timeout for remote [PowerShell](#) commands.

## Other Global Parameters

[Global Parameters: Access](#)

[Global Parameters: Browser Extension](#)

[Global Parameters: Discovery](#)

[Global Parameters: Drivers](#)

[Global Parameters: Jobs](#)

[Global Parameters: Preference](#)

[Global Parameters: Proxy](#)

[Global Parameters: Sessions](#)

[Global Parameters: Storage](#)

[Global Parameters: Workflow](#)

## Global Parameters: Jobs

### Password Reset LDAP Validation

This parameter enables password validation on the record before executing the Password Reset LDAP script. If enabled and the record in the selected vault contains an invalid password, the script will not execute, neither on demand or scheduled, and an appropriate Response message will appear in the Job History report as an Error.

The available options are:

- **System:** The password validation will occur on all Password Reset LDAP script executions regardless of where the record is located.
- **Personal Vault** (default value): The password validation will only occur on Password Reset LDAP scripts that are executed from within a Personal Vault.
- **None:** Password validation will not occur on Password Reset LDAP script executions.

### Periodic Jobs Execution When Checkout

This parameter defines the execution logic of periodic jobs when the record is checked out.

The following options are available:

- **Proceed** - Periodic jobs will be executed even if the record is checked out. This is the default setting.
- **Cancel** - Periodic jobs will be cancelled at the time of scheduled execution if the record is checked out. This option allows the record to remain intact during the time it is checked out such as password values. The option relies on the necessary jobs being scheduled during the *Check In* process.
- **Defer** - Periodic jobs will be deferred to the request expiration time if the record is checked out. This option allows the record to remain intact during the time it is checked out deferring jobs until the request has expired and the record is checked in.

## Rerun Failed Job Interval

When this parameter is non-zero, the system will reschedule failed periodic, monthly or weekly jobs several times with the specified interval during the specified time window or until the job will succeed.

Note that the non-zero time interval should be smaller than the rerun failed job time window.

Time format:

Space or a colon-separated list of tokens, each token is a number+time unit.

Allowed units are:

- d** - days,
- h** - hours,
- m** - minutes,
- s** - seconds.

If no time unit is specified then the value is considered to be in milliseconds. Negative values or zero allowed.

Example:

1. 1d 12h - 1 day and 12 hours
2. 45m - 45 minutes
3. 0d or 0h or 0m or 0 - zero

## Rerun Failed Job Window

When this parameter is non-zero, the system will reschedule failed periodic, monthly or weekly jobs several times during the specified time window or until the job will succeed.

Time format:

Space or a colon-separated list of tokens, each token is a number+time unit.

Allowed units are:

- d** - days,
- h** - hours,
- m** - minutes,

s - seconds.

If no time unit is specified then the value is considered to be in milliseconds. Negative values or zero allowed.

Example:

1. 1d 12h - 1 day and 12 hours
2. 45m - 45 minutes
3. 0d or 0h or 0m or 0 - zero

## SSH Connector Type

This parameter allows to switch between default (Jsch Connector) and extended (SSHD Connector) provider to execute all SSH and Interactive SSH jobs in the system.

SSHD Connector provider includes extended cryptography algorithms to support job execution on a different set of devices.

To override this parameter for individual records, use record level field *SSHConnectorType* (Display name: SSH Connector Type, Choice values: Jsch Connector, SSHD Connector).

## Other Global Parameters

[Global Parameters: Access](#)

[Global Parameters: Browser Extension](#)

[Global Parameters: Discovery](#)

[Global Parameters: Drivers](#)

[Global Parameters: Jobs](#)

[Global Parameters: Preference](#)

[Global Parameters: Proxy](#)

[Global Parameters: Sessions](#)

[Global Parameters: Storage](#)

[Global Parameters: Workflow](#)

## Global Parameters: Preference

### Access Sessions Events

When disabled, PAM limits visibility of this information/report to auditors and system administrators only.

### Days for License Expiration Warning

This setting defines the number of days prior to the expiration of your license when a warning message will be triggered.

## Display License Expiration Warning to Administrators

This parameter controls whether the license warning message is displayed to all users or only to administrators. If disabled, the message is displayed to all users. If enabled, the message will be displayed only to administrators.

## Debug Mode

This parameter enables Debug Mode for the whole application or for the current user if enabled in the User Preferences.

The parameters trigger the output of the additional information to the system logs to help the vendor to troubleshoot certain cases.

## Display Full Administrator Menu for Auditors

When enabled Auditors are granted view-only access to additional subsection within the Administration section of the user interface.

## Display Full Path For Objects In Reports

This parameter controls the visibility of full object paths in reports.

When enabled, full path to the object is shown.

When disabled, only the object name is shown.

## Email Override

This user preference allows users to override email for system notifications with an email address on one of the domains enabled by the system administrators.

System administrators should define the comma-separated list of allowed domains in the global parameter Email Override to enable email override for specified domains.

## Initial Query Type

The default value for the Search Center query type on the records list screen

## Language

Defines the language that will be used when logged into the System.

## Search Scope

Defines the record search scope for the browser extension. Possible values are the following:

- **Everything** - Displays all records found for the currently open WEB Portal URL
- **Exclude Personal Vaults** - Displays all records found for the currently open WEB Portal URL excluding records found in the Personal Vaults of other users for system administrators and auditors. The option is useful to narrow down search results for the system administrators and auditors.

## Session Clipboard Hotkeys

This parameter enables **Ctrl-C/Ctrl-V** (Command-C/Command-V) hotkey combination when copying and pasting text from and to in-browser sessions.

Before enabling this option consider clipboard events logged by the system when event logging is enabled for clipboard operations unrelated to the active sessions.

Note: This feature is not supported in Firefox web browser.

## Session Heartbeat Interval

Session heartbeat interval is a session timeout feedback policy.

The session heartbeat interval is defined by three values in seconds separated by slash character like in the following example: *2/15/30*

- The first value is the number of seconds to display the warning sign about session disconnection.
- The second value is the number of seconds to initiate reconnect for an already connected active session.
- The third value is the number of seconds to initiate reconnect for not yet connected session.

## Session RDP Font Smoothing

If enabled, the text will be rendered with smooth edges.

Text over RDP is rendered with rough edges by default, as this reduces the number of colors used by text, and thus reduces the bandwidth required for the connection.

## Session RDP Resize Method

Resize method for RDP sessions.

Possible values are:

- **Fixed** - RDP Session will be opened in a fixed size;
- **Reconnect** - RDP Session will reconnect each time with the client browser resize.

## Session RDP Screen Size

Screen size for RDP sessions in the form **{width}x{height}**.

When the value is empty or **MAX** or **CURRENT** the size will be initially set to the current window size and will not resize with the browser during the session.

Note that this parameter applies only when Session RDP Resize Method is set to Fixed

## Session RDP Server Layout

This parameter defines the keyboard layout of the RDP server for RDP sessions.

RDP protocol uses identifiers based on the key location on the keyboard (such as the second left key in the top row). To translate between a key meaning and an RDP key event, the system should know the keyboard layout of the RDP server given by this parameter.

## Session Start Mode

This parameter specifies whether a session should start in a full-screen mode, in a regular window or in a browser tab.

## Skin

Defines the application color scheme.

## Starting View

Defines the starting view a user will see after logging in to the application.

## Window Close Confirmation

Enabling this parameter will request a user to confirm closing an application tab or a window.

Refresh the browser after changing this preference to apply new setting.

## Other Global Parameters

[Global Parameters: Access](#)

[Global Parameters: Browser Extension](#)

[Global Parameters: Discovery](#)

[Global Parameters: Drivers](#)

[Global Parameters: Jobs](#)

[Global Parameters: Preference](#)

[Global Parameters: Proxy](#)

[Global Parameters: Sessions](#)

[Global Parameters: Storage](#)

[Global Parameters: Workflow](#)

## Global Parameters: Proxy

### HTTP Proxy [Deprecated]

This parameter enables an HTTP Proxy server that allows high-trust login to WEB applications and WEB Sites.

Note that the System server should be restarted to initialize the HTTP Proxy server.

### HTTP Proxy Connect Timeout

Timeout for connecting to the upstream server on a new connection, in seconds. If set to 0 then the parameter defaults to 40 seconds.

Restart the service after updating this parameter.

## HTTP Proxy Domains

WEB Domains to be handled by HTTP Proxy for high-trust login.

## HTTP Proxy Idle Connection Timeout

Timeout after which to disconnect idle connections, in seconds. If set to 0 then the parameter defaults to 70 seconds.

Restart the service after updating this parameter.

## HTTP Proxy Port

Port for HTTP Proxy server.

## HTTP User Placeholder

This parameter defines a placeholder to type into the User field of a WEB application or a WEB site to be resolved by the HTTP Proxy server to enable high-trust login.

## HTTP Password Placeholder

This parameter defines a placeholder to type into the Password field of a WEB application or a WEB site to be resolved by the HTTP Proxy server to enable high-trust login.

## Proxy Key Password

Private key password for RDP, SQL, HTTP and Universal proxies to secure communication link between native clients and the proxy.

Initial value for this parameter is randomly generated together with the keys and certificates during the system initialization. When the keys are replaced the system administrator can use the password defined by this parameter or update the password using this parameter.

The keys are located in the folder `$PAM_HOME/content/keys` and should be replicated between nodes in the high availability deployments. RDP, SQL and Universal Proxy key pair are stored in the files *keystore\_rdp.p12* (private key) and *certificate\_rdp.cer* (public key). HTTP Proxy key pair is stored in the files *keystore.p12* (private key) and *certificate.cer* (public key).

## RDP Proxy

This parameter enables an RDP Proxy server that allows high-trust login to Windows servers or desktop computers using native clients such as MS RDP (mstsc), RDCMan, mRemoteNG, mobile remote desktop clients, etc.

Note that the System server should be restarted to initialize the RDP Proxy server.



To connect to RDP server through RDP Proxy, specify RDP Proxy host and port in the client application as a destination server and user#record as a user where the user is a system user and the record is either Record ID or search criteria identifying the single record. In this case, the session will be established with the host and credentials on the record.

## RDP Proxy Idle Timeout

Disconnect open RDP proxy session if it is idle for the specified number of seconds.

If set to 0 then it will never disconnect idle sessions.

## RDP Proxy Ciphers Deny List

This parameter disables security ciphers by regular expression pattern. Multiple patterns must be split by coma.

Examples:

**.\*\_SHA** deny all ciphers with ending \_SHA (SHA1) hashing algorithm.

**TLS\_RSA.\*,.\*\_SHA** deny all RSA algorithms and those with SHA1 hashing.

RDP Proxy Client Ciphers and RDP Proxy Server Ciphers are written to `$PAM_HOME/web/logs/pam.log` during application startup.

## RDP Proxy Idle Timeout

Disconnect open RDP proxy session if it is idle for specified number of seconds. If set to 0 then it will never disconnect idle sessions.

## RDP Proxy Port

This parameter defines the access port for the RDP Proxy server to serve high trust login for native clients

Note that the System server should be restarted to initialize the RDP Proxy server with a new port.

## RDP Proxy Protocol Level

This parameter controls the RDP Proxy protocol level used for both - client to proxy and proxy to remote server authentication.

- **nla stands for Network Level Authentication.** Using nla requires TLS encryption and performs authentication steps before starting the remote desktop sessions.
- **ext stands for Extended NLA.** This protocol is almost the same as NLA and in addition, requires "Early User Authorization Result" sent from the server immediately after authentication is performed.

## SSH Proxy

This parameter enables an SSH Proxy server that allows high-trust login to SSH servers (such as Unix or network devices) using native clients such as Unix Shell, Putty, Secure CRT, etc.

Note that the System server should be restarted to initialize the SSH Proxy server.

## SSH Proxy Allowed Channels

This parameter controls what channels/subsystems allowed to use by client software when connecting through SSH Proxy server.

Supported channels are:

- **shell** - Allows shell connection.
- **exec** - Allows remote command execution including scp transfer.
- **sftp** - Allows file transfer using SFTP protocol.
- **tunnel** - Allows SSH tunnels over SSH Proxy.

Settings could be overridden on record level using custom filed named *SshChannels*. There are two scenarios to override channel settings:

1. List channels allowed for current record. This will allow only shell and exec channels to open: *shell, exec*
2. Use system defaults but add or remove specific channel. This will use setting from system parameter but allow sftp and deny tunnel channels: *+sftp,-tunnel*

## SSH Proxy Banner

This parameter defines the banner displayed to SSH Proxy clients.

Use \n character for new line separator.

Note that update of this parameter requires a restart of SSH Proxy service.

## SSH Proxy Ciphers

Cipher algorithms are used by ssh proxy server for data encryption. The algorithm list should be comma-separated.

Available algorithms: aes128-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, aes256-cbc. Available vulnerable algorithms: arcfour128, arcfour256, blowfish-cbc, 3des-cbc.

Default settings exclude known weak algorithms.

## SSH Proxy Idle Timeout

Disconnect open ssh proxy session if it is idle for the specified number of seconds.

If set to 0 then it will never disconnect idle sessions.

## SSH Proxy Keep Alive Count

A number of keep-alive messages without a response from the client. After limit exceeds disconnect stale session.

If set to 0 never send such messages.

## SSH Proxy Keep Alive Interval

Send keep-alive messages every specified amount of seconds.

If set to 0 never send such messages.

## SSH Proxy Key Exchange Algorithms

Key Exchange Algorithms used by ssh proxy server to securely exchange encryption keys with the connected client. The algorithm list should be comma-separated.

Available algorithms: ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256, diffie-hellman-group18-sha512, diffie-hellman-group17-sha512, diffie-hellman-group16-sha512, diffie-hellman-group15-sha512, diffie-hellman-group14-sha256, diffie-hellman-group-exchange-sha256. Available vulnerable algorithms: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1

Default settings exclude known weak algorithms.

## SSH Proxy Macs

Message Authentication Code algorithms used by ssh proxy server for integrity data protection.

The algorithm list should be comma-separated.

Available algorithms: hmac-sha2-512-etm@openssh.com, hmac-sha2-512, hmac-sha2-256-etm@openssh.com, hmac-sha2-256, hmac-sha1-etm@openssh.com, hmac-sha1. Available vulnerable algorithms: hmac-md5, hmac-md5-96, hmac-sha1-96

Default settings exclude known weak algorithms.

## SSH Proxy Port

This parameter defines the access port for SSH Proxy server to serve high trust login for native clients.

Defines custom port for universal proxy service (default: 2017).

System parameter: **xtam.proxy.universal=enabled|disabled**

Note that the PAM server should be restarted to initialize the SSH Proxy server with a new port.

## SSH Proxy Public Key Expiration (in days)

SSH Proxy Public Key expiration in days.

Leave this parameter blank to disable SSH Proxy Public Key expiration.

## Throttle SSH Proxy Automation Connections

This parameter defines artificial delay in milliseconds for SSH Proxy to apply before every new connection performed by a user with Automation global role. The parameter might be defined as a fixed value or as a range (for example 500-1000) in which case the system will select a random delay in milliseconds inside the range.

This parameter is used to throttle performance of automation clients that frequently open multiple connections through SSH Proxy to reduce the load on other system components.

## Universal Proxy HTTP Forwarding

This parameter enables HTTP traffic forwarding mode for Universal Proxy to local or remote host.

Enables Native Session Manager and HTTP Proxy port forwarding.

System parameter: **xtam.proxy.universal.forward.http=enabled | disabled**

## Universal Proxy HTTP Forwarding Host

This parameter holds **host:port** value of upstream server for HTTP traffic forwarding mode.

Defines Native Session Manager and HTTP Proxy port forwarding host (default: 127.0.0.1:8081).

System parameter: **xtam.proxy.universal.forward.http.host=host:port**

## Universal Proxy HTTP Forwarding Use SSL

This parameter enables SSL support when connecting to upstream server for HTTP traffic forwarding mode.

Enables SSL communication with WEB Session Manager.

System parameter: **xtam.proxy.universal.forward.sm.ssl=enabled | disabled**

## Universal Proxy Session Manager Forwarding

This parameter enables Session Manager traffic forwarding mode for Universal Proxy to local or remote host.

Enables WEB Session Manager port forwarding.

System parameter: **xtam.proxy.universal.forward.sm=enabled | disabled**

## Universal Proxy Session Manager Forwarding Host

This parameter holds **host:port** value of upstream server for Session Manager traffic forwarding mode.

Defines WEB Session Manager port forwarding host (default: 127.0.0.1:4822).

System parameter: **xtam.proxy.universal.forward.sm.host=host:port**

## Universal Proxy Session Manager Forwarding Use SSL

This parameter enables SSL support when connecting to upstream server for Session Manager traffic forwarding mode.

Enables SSL communication with WEB Session Manager.

System parameter: **xtam.proxy.universal.forward.sm.ssl=enabled | disabled**

Note that for WEB Session Manager forwarding remote node keystore should contain certificate of the remote WEB Session Manager. In addition to this, master nodes should contain certificates of the remote universal proxy instead of the remote WEB Session Manager. Remote WEB Session manager in this scenario could be completely hidden behind the firewall because only remote universal proxy will connect to remote WEB Session manager on the same node.

## Other Global Parameters

[Global Parameters: Access](#)

[Global Parameters: Browser Extension](#)

[Global Parameters: Discovery](#)

[Global Parameters: Drivers](#)

[Global Parameters: Jobs](#)

[Global Parameters: Preference](#)

[Global Parameters: Proxy](#)

[Global Parameters: Sessions](#)

[Global Parameters: Storage](#)

[Global Parameters: Workflow](#)

## Global Parameters: Sessions

### AS400 Screen Size

Screen size for AS400 sessions in the form **{lines}x{columns}**.

### Exclusive Session

This parameter controls the option to create multiple simultaneous sessions for the same record.

### Password Detection Entropy

This parameter is used to enable [Session Event Masking](#) where detected passwords are masked in [Session Event Reports](#). The higher the value in this parameter, the more complex the recorded KeySequence event must be for it to be detected as a password. A recommended starting point for testing this feature is 30. Enter a 0 value (zero) to disable [Session Event Masking](#).

### Personal Vault Event Recording

This parameter enforces event recording for records located in personal vaults.

Use Default setting to defer recording enforcement to record permissions with the record owner creating sessions with no recordings. Use Enforced setting to enforce recording for all users for all records in personal vaults.

### Personal Vault Session Recording

This parameter enforces session recording for records located in personal vaults.

Use Default setting to defer recording enforcement to record permissions with the record owner creating sessions with no recordings. Use Enforced setting to enforce recording for all users for all records in personal vaults.

## Resize Tolerance

Session Window Resize Tolerance parameter.

Session window resizes tolerance limits for RDP sessions parameter is given in the form **{width}x{height}** (for example, 3x65) to define the change of browser screen in pixels that would trigger resize of the session screen.

The primary purpose of this parameter is to avoid screen resize for RDP sessions in case temporary browser status bars such as the Download status bar appear inside the browser view area.

## Session Clipboard Transfer

Enables clipboard transfer for in-browser sessions.

## Session Connect And Record Message

The banner message presented to a user when accessing WEB session with recording enabled.

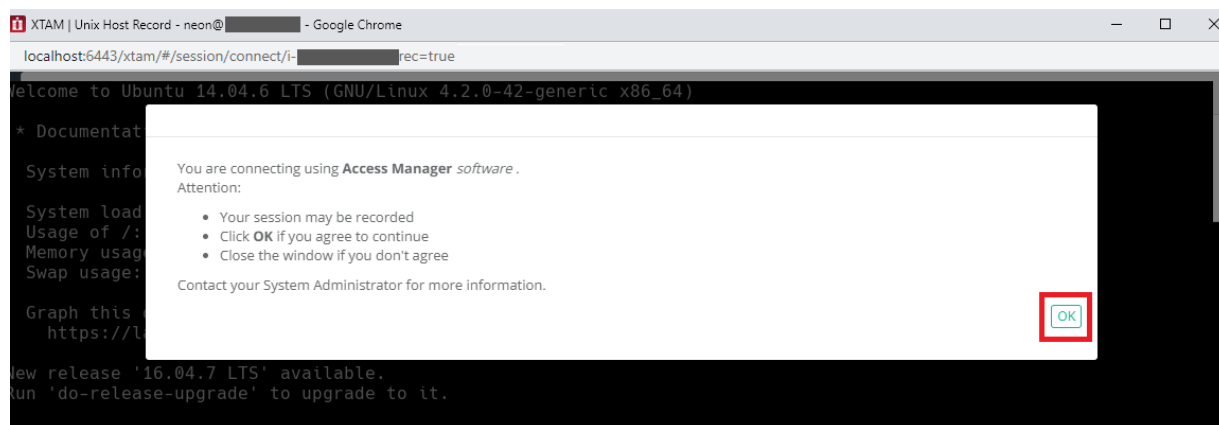
Note that it is possible to use HTML formatting in this message.

Example:

*You are connecting using **Access Manager** software .* *Attention:*

- Your session may be recorded*
- Click **OK** if you agree to continue*
- Close the window if you don't agree*

*Contact your System Administrator for more information.*



## Session Connect Message

The banner message presented to a user when accessing WEB session without recording enabled.

Note that it is possible to use HTML formatting in this message as Session Connect And Record Messages.

## Session Expiration Warning Threshold

This global parameter defines the time threshold before session expiration at which a PAM user receives an on-screen warning.

This setting defines the number of minutes prior to session expiration when the user receive a notification warning them about the upcoming timeout.

## Session File Transfer

Enables file browsing and file transfer for in-browser sessions.

## Session Idle Activity Timeout

Disconnect the open session if it has no activity for the specified number of seconds.

If set to 0 then it will not disconnect sessions with no activity.

## Session Idle Timeout

Disconnect open WEB Session if it is idle for specified number of seconds.

If set to 0 then it will never disconnect idle sessions.

This parameter is deprecated in two parameters: **Web Session Idle Timeout** and **SSH Proxy Idle Timeout**.

## Session Recording Metadata

This parameter defines the option to embed session metadata and session events into the video generated from the session video recording.

- Disabled (default value) disables embedding session metadata and session events into the converted video.
- Embedded enables the pixel-level embedding of session metadata and session events into the converted video.

Stream creates Closed Captions stream of session metadata and session events in the converted video.

Note that the AVI format does not support Closed Captions.

## Session Recording Rendering Bitrate

This parameter defines the bitrate of rendered video generated from session recording per second.

The higher the bitrate, the sharper the video image is.

However, high bit rates slow down the process of conversion and add extra load to the servers.

Default value is 2000000 bit/s.

The bitrates below are recommended high session video rendering resolution:

- 1920x1080 - 8000000 bit/s;
- 1024x768 - 5000000 bit/s;
- 640x480 - 2000000 bit/s.

## Session Recording Rendering Resolution

This parameter defines the resolution of rendered video generated from session recording in pixels.

The higher the resolution is the larger the rendered video becomes.

However, high resolutions slow down the process of conversion and add extra load to the servers.

Default value is **640x480**.

## Session Request Enforcement

Defines how the system will handle remote sessions that are still active when the user's requested time period or range has expired.

Terminate (default value) will terminate all active sessions when their requested time period or range has expired.

Continue will allow active sessions to continue beyond their requested time period or range.

## Session WebSockets

Enables WebSockets protocol for in-browser sessions.

## Support Relayed Sessions

This parameter enables web session connectivity using the Remote Relay Node option.

## URI Handler RDP

This parameter defines a template for browser URI handler to launch a native RDP client on Windows and Linux platforms using WEB GUI to connect through system RDP Proxy.

The URI Handler template might reference the following placeholders for the system to fill for each specific record:

- **{USER}** for currently logged in user
- **{RECORD}** for the selected Record ID
- **{HOST}** for RDP Proxy Host
- **{PORT}** for the RDP Proxy port

Following is a typical example of URI Handler:

- `rdp://{USER}#{RECORD}@{HOST}:{PORT}`

Note that the system takes advantage of both native application and browser URI handler already deployed on the client computer only allowing customization of URI handler pattern. Also, note that browsers on Mac OS include pre-installed URI Handlers that are used to launch native clients from the browser.

## URI Handler SSH

This parameter defines a template for browser URI handler to launch a native SSH client on Windows and Linux platforms using WEB GUI to connect through system SSH Proxy.

The URI Handler template might reference the following placeholders for the system to fill for each specific record:

- **{USER}** for currently logged in user
- **{RECORD}** for the selected Record ID



- **{HOST}** for SSH Proxy Host
- **{PORT}** for the SSH Proxy port

Following is a typical example of URI Handler:

- `ssh://{USER}#{RECORD}@{HOST}:{PORT}`

Note that the system takes advantage of both native application and browser URI handler already deployed on the client computer only allowing customization of URI handler pattern. Also, note that browsers on Mac OS include pre-installed URI Handlers that are used to launch native clients from the browser.

## Use Proximity Groups to Resolve Relays

Resolve relay nodes available for the particular record using Proximity Groups configuration.

## Web Session Idle Timeout

Logout from the application if it is idle for the specified number of seconds.

If set to 0 then it will never log out when idle.

## Other Global Parameters

[Global Parameters: Access](#)

[Global Parameters: Browser Extension](#)

[Global Parameters: Discovery](#)

[Global Parameters: Drivers](#)

[Global Parameters: Jobs](#)

[Global Parameters: Preference](#)

[Global Parameters: Proxy](#)

[Global Parameters: Sessions](#)

[Global Parameters: Storage](#)

[Global Parameters: Workflow](#)

## Global Parameters: Storage

### Archived Objects Retention

Archived objects retention in days. The system will delete archived objects from the database. Use 0 to disable archived objects retention.

### Audit Logs Retention

Audit logs retention in days. The system will export old audit log entries daily and delete them from the database.

Use 0 to disable audit logs archiving.

## Content Location

A storage location for session recordings in case the content storage is set to File System.

Note that in the case of multiple WEB Front Ends the storage location should be shared between the WEB front ends.

`$PAM_HOME` variable refers to the installation location of the software.

## Content Storage

A storage type for session recordings.

## Encrypt Content

This parameter enables or disables encryption of session recordings and logged transferred files.

## Export Location

A storage location for database export files.

Note that in the case of multiple WEB Front Ends the storage location should be shared between the WEB front ends.

`$PAM_HOME` variable refers to the installation location of the software.

## Export Schedule

The time between automatic exports in minutes. Zero if automatic export is disabled

## Export Time Window

The time window for allowed automated scheduled export.

Time window setting is an expression in cron format defining the time window for the system export.

When this parameter is defined the export will be scheduled only during the specified time window.

Use time window cron expression builder to construct required expression or type the cron expression directly to the parameter.

Examples of time window expression:

1. **\* \* 1-7 ? \* SUN,SAT \*** - between 1am and 7am, on every Sunday and Saturday
2. **\* \* 0,1,2,3,12,22,23 ? \* MON,TUE,WED \*** - during 0am, 1am, 2am, 3am, 12pm, 22pm and 23pm, on every Monday, Tuesday and Wednesday

## Personal Vault

This parameter enables or disables the personal vault feature for all system users.

## Personal Vault Role

This parameter defines user permission level for their own Personal Vault.

- The Owner role allows users to manage content in the personal vault and share it with other users.
- The Manager role allows users to manage content in the personal vault without sharing.

The role is applied when provisioning a new Personal Vault.

After changing this parameter, existing vaults will retain their current role.

## Report Folder

This parameter defines the path to Report Folder where admins can type path on the file system where to store these reports.

Path might contain placeholder like in the example of Content Location or Temporary Location: `$PAM_HOME/content/reports`.

## Report Title Prefix

This parameter defines the prefix before title in exported or scheduled reports.

This prefix will be part of the file name and in the first row of the generated report.

## Session Recording Retention

Session recording retention in days. The system will delete the session recording after the specified number of days.

Use 0 to disable session recording deletion.

## Session Transfers Retention

File transfers stored from session events retention in days.

The system will delete stored file transfers after the specified number of days.

Use 0 to disable session file transfers deletion.

## System Export Retention

System export retention in days.

The system will delete the system export after the specified number of days.

Use 0 to disable system export deletion.

## System Log Session Events

This parameter controls the option to system log session events such as key sequences or file transfers including streaming session events to SIEM systems.

## System Logs Retention

System logs retention in days.

The system will delete WEB container system logs after a specified number of days.

Use 0 to disable system logs deletion.

## Temp Folder Retention

Temporary files retention in days.

Deletes temporary files from `$PAM_HOME/web/temp/`.

Deletes temporary files from location specified in the Temporary Location parameter.

Default recommended value is 7 days

Use 0 to disable temporary files deletion.

`$PAM_HOME` variable refers to the installation location of the software.

## Temporary Location

Storage location for temporary files.

Note that the `$PAM_HOME` variable refers to the installation location of the software.

## Other Global Parameters

[Global Parameters: Access](#)

[Global Parameters: Browser Extension](#)

[Global Parameters: Discovery](#)

[Global Parameters: Drivers](#)

[Global Parameters: Jobs](#)

[Global Parameters: Preference](#)

[Global Parameters: Proxy](#)

[Global Parameters: Sessions](#)

[Global Parameters: Storage](#)

[Global Parameters: Workflow](#)

## Global Parameters: Workflow

### Approve by Mail

This parameter enables the option to approve access requests by replying **Ok**, **Yes** or **Approved** to the request notification email.

Any other message in the email reply will be considered the reason for the request rejection.

Note that mail server configuration should include an IMAP port and folder for the server to scan mailbox for the approval emails.

### Approve by Mail Enforce JWT

This parameter enables token authentication for the request approval emails sent by approvers responding to approval requests notifications. Enforcing token authentication for emails improves security of email-based

approve process by reducing the risk of forging an approver's email.

When token authentication is enabled, the system injects a secure signed token into the approval notification email. The token embeds information about the user, workflow, requested object and time. When processing the response from the approver, the system then checks the token signature and matches data encoded into the token with the actual workflow, user and environment information.

Note that the system disables verification part of the authentication in case request notification template does not include token placeholder or one of the master node sending notification is not new enough to support token authentication.

## Approve by Mail Filter

This parameter defines the email subject filter for the Approve-by-Email process to select emails from the IMAP request approval integration folder.

Leave this parameter blank for the Approve-by-Email process to handle all emails from the IMAP folder.

## Approve by Mail Keywords

This parameter defines a set of keywords an approver can use to approve access requests by replying to the email notification in addition to default **Ok, Yes, Approve** and **Approved keywords**.

All other responses to the email notification will reject the access request.

## Default Requested Time

Defines the default number of minutes in the requested time for access request.

## Minimum Requested Time

Defines the minimum number of minutes is requested time for access request.

Leave this field blank if you don't want to apply this option.

## Maximum Requested Time

Defines the maximum number of minutes in requested time for access request.

Leave this field blank if you don't want to apply this option.

## Minimum Reason Length

Defines the minimum number of symbols in a reason for access request.

Leave this field blank if you don't want to apply this option.

## Reason Selection Helper

This parameter enables and disables access request reason selection helper with type-ahead prompt while entering request reason and selection list of **top 10 most used reasons** in the past.

## Holidays

Defines the days that the System will use as a reference for Holidays.

Dates should be entered as M/D and multiple dates should be separated with a comma.

## Weekend

Defines the days that the System will use as a reference for Weekends.

Days should be entered as text and multiple days should be separated with a comma.

## Work Hours

Defines the time range(s) that the System will use as a reference for Work Hours (relative to the System server time).

Time range(s) outside of those specified will be used as a reference for After Hours.

For example, if 8:30-17:30 is entered (HH:MM-HH:MM), Work Hours is referenced as 8:30 AM to 5:30 PM whereas After Hours is referenced as 5:30 PM to 8:30 AM.

## Other Global Parameters

[Global Parameters: Access](#)

[Global Parameters: Browser Extension](#)

[Global Parameters: Discovery](#)

[Global Parameters: Drivers](#)

[Global Parameters: Jobs](#)

[Global Parameters: Preference](#)

[Global Parameters: Proxy](#)

[Global Parameters: Sessions](#)

[Global Parameters: Storage](#)

[Global Parameters: Workflow](#)

## Records

### Records

A record, sometimes referred to as a secret, is an asset stored within PAM that contains sensitive information that is shared between users, whose access and use is audited.

Records are built from Record Types that define the type of asset that is being managed.

Records can be organized by Containers (folder or vaults) that allows for easier management using inheritance and reporting.

### Create a New Record

From within your desired container, click the **Add Record** button and select the *Record Type* to use from the dropdown menu list.

The chosen Record Type will contain all the relevant fields for the creation of your new Record.

If you cannot decide which to choose or one that fits your requirements is not present, talk with your System Administrator about creating a [Custom Record Type](#).

NOTE: The ability to create new records is provided by the permissions that have been granted to your account. If you do not have the **Add Record** button, then you lack the permission required to create new records. Talk with your PAM System Administrator for more information.

## Create New Record Page

On the new Record page, you will be presented with a list of fields to populate. These fields are generated based on the current configuration of the Record Type.

Populate all the fields as you require and click the **Save** or **Save and Return** button to complete the record creation.


Both the *Name* and *Description* fields will be visible and searchable from the Records List page, so it is recommended to use relevant, non-sensitive values.






## Viewing a Record

To view any record, you simply need to locate it within one of your accessible views (*All Records*, *Shared With Me*, *Favorites* or *Search* results) and either click on the **Record Name** or chose the option **View** from the record's Action menu (...).

If a record is linked, then the path of each linked instance of this record will appear as clickable hyperlinks below its description in the Record List view.

When viewing a record, the following information and options may be available based on the level of permission that you have been granted to this record and the operations that have been enabled on it:

<b>Breadcrumb Path</b>	Displays the full path location of this object. If the object has multiple parents, then it will have a breadcrumb path for each linked parent.
<b>Go to Parent</b>	Navigates back to the parent container. If multiple parents, select the parent to navigate back. The record's breadcrumb will also display the path of each parent container that you may also click on to navigate to a different location.
<b>Connect</b>	Creates a <a href="#">secure remote session</a> to this managed asset or endpoint.
<b>Execute</b>	Executes the <a href="#">selected task</a> that has been configured with an on-demand policy event.
<b>Unlock/Lock</b> 	Unlocks the secured fields enabling you to <i>Show</i> or <i>Copy to Clipboard</i> the secured value. After unlock, this button becomes a <i>Lock</i> option to return the value to its locked and masked state.
<b>Audit Log</b>	Displays the audit events specific to this record including <i>Timestamps</i> , <i>Users</i> , <i>IP Addresses</i> and <i>Events</i> .
<b>Change History</b>	Displays the <i>history of changes</i> that have been made to the values of this record.

<b>Sessions</b>	Displays all the secure remote sessions, both Active and Completed, that have been established with this record. Also provides access to <i>Session Video Recordings, Events, Join, Terminate</i> and <i>Recording Export or Download</i> options.
<b>Job History</b>	Displays all the <i>Jobs</i> or <i>Tasks</i> that have been executed with this record, including details, timestamps and users.
<b>Grant</b>	Provides the option to Grant Access to this record using an existing Workflow Template and Binding.
<b>Manage</b>	Provides a menu of options to manage this record including <i>Command Control Policies, Formula, Permissions, Tasks, Workflows</i> and <i>Archive</i> state.
<b>Edit</b>	Switches the record into Edit mode so that the record values can be modified.
<b>Subscribe to Alerts</b> 	Allows the user to subscribe to alerts for this record.
<b>Add/Remove Favorite</b>  / 	Adds or Removes this record from the user's Favorites list.
<b>Anonymous Link</b> 	Generate an anonymous link associated to this record.
<b>Request &lt;Name&gt;</b> 	If you are bound by a workflow template, your <i>Connect, Execute</i> or <i>Edit</i> buttons will be shown with a Request label. You must first request and gain approval before you can access these options.

## Split View

To comply with specific security policies, maintain regulatory compliance and enforce segregation of duty, it may become a business requirement to ensure that no single user has access to the entire secret or password string within a record.

Some refer to this functionality as the “Two-person rule” because it requires one user to retrieve the first part of a password and a second user to retrieve the remainder, thus requiring two people to reconstruct the full password string.

When this Split View feature is enabled, the *Unlock* option will either reveal the first part of the record's password or the second part, based on the system's configuration.

This prevents a single user from ever being able to *Unlock* the complete password for a record.

If you see only half of the password when you click **Unlock**, then your System Administrator has enabled this feature.

Speak with your System Administrator for assistance if you need to retrieve the other half of the password.

Password

5R+Td.:6U7%{|\*\*\*\*\*







## Editing a Record

When you wish to make changes to an existing record's values, you first need to switch the record to *Edit Mode*.

You can switch to *Edit Mode* by either first viewing the record and then clicking the record's **Edit** button or you can select the **Edit** option from the Records List page by opening the record's Action menu (...).

All changes made to the record values will be captured to the record's *Change History*, including timestamp, user and changed values.

Additionally, an Edit event will be logged to the record's *Audit Log*.

When you are finished with the modifications, click either the **Save** or **Save and Return** button to save your changes.

## Sharing a Record

Records can be shared with other users that have access to the system. To share a record with another user(s) or group, click the **Share** button for this record on the Record List page or select the **Permissions** option located in the record's Action menu (...).

Additionally, if you are already viewing the record you wish to share, click the Manage > Permissions option to open its sharing or permissions page.

Before you share a record or container, it is recommended to understand its current inheritance.

Records can either have inherited permissions or unique permissions.

NOTE: Permissions are configured *by default to inherit* from the object's parent container. When sharing a record, you will either need to share the parent container so that through inheritance this record is also shared (along with all other child objects in the parent container) or *you can break inheritance* and create unique sharing permissions for an individual record.

Both scenarios are equally supported, but you should consult with your object Owner or PAM System Administrator for guidance and recommendations.

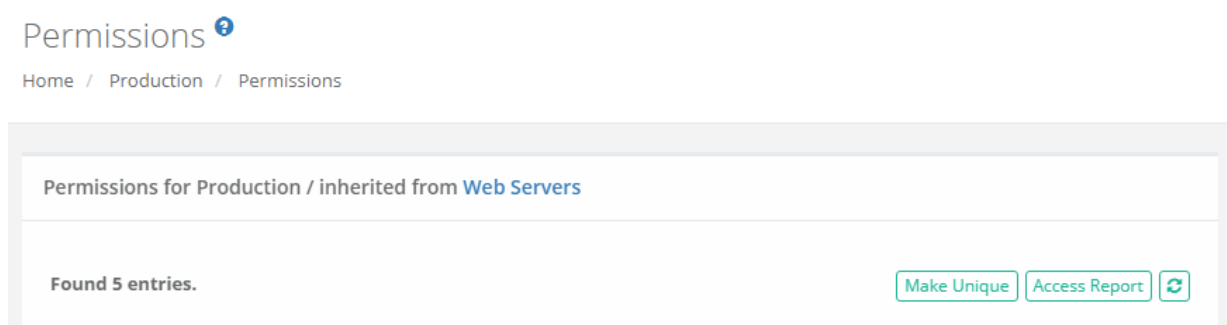
Records with *inherited permissions* (example shown below) means that the permissions associated to this object originate from its parent.

This means if you want to share a record with inherited permissions, then you must share its parent object.

Modifying permissions on a parent object will then affect all other objects that inherit permissions from it as well.

When viewing the permissions of an object with inherited permissions, the button **Make Unique** will be visible and you will see the *inherited from <Parent>* text in the header.

Clicking this **Make Unique** button will break the permission inheritance of this object to its parent and create a unique permission list that can be modified as needed.

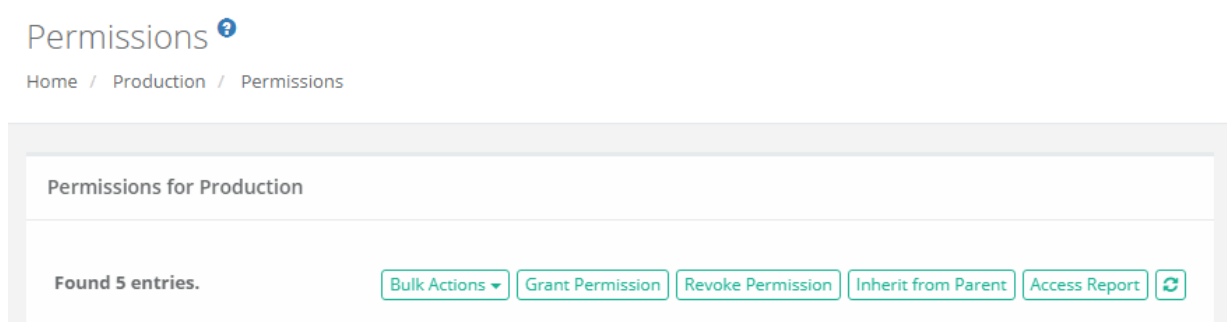


Records with *unique permissions* or broken inheritance (example shown below) means that the permissions associated to this object do not originate from a parent and are unique to this object.

This means if you want to share a record with unique permissions, then you can do so without affecting the permissions of any other object.

When viewing the permissions of an object with unique permissions, the button **Inherit from Parent** will be visible.

Clicking this **Inherit from Parent** button will remove all unique permissions and reestablish inheritance from this object's parent.



## To Share or Grant Permission to the selected object:

1. Access the object's permissions page by using the **Share** button or Manage > Permissions option.
2. Click the **Grant Permissions** button to open the dialog.
3. In the Principal field, enter the user(s) or group(s) that you wish to share with and then click the **Add** button. You may also use the **Search** button to locate your principal.
4. Configure the [object permissions](#) that you wish to grant to the selected principal(s).
5. Finally, click the **Select** button to complete the sharing or granting process.

## To Edit existing permissions to the selected object:

1. Access the object's permissions page by using the Manage > Permissions option.
2. Locate the Principal from the list that you want to edit their permissions and click the **Edit** button in the Actions column.
3. In the Grant Access dialog, confirm the principal is correct and then modify their permissions as required.
4. Finally, click the **Select** button to complete the edit process.

To Revoke existing permissions to the selected object:

1. Access the object's permissions page by using the Manage > Permissions option.
2. Select the Principal that you wish to revoke permissions from the list by checking their box and click the **Revoke Permission** button.
3. Confirm your action to revoke the selected permissions in the confirmation dialog.

For ongoing maintenance and auditing, the **Access Report** button will generate a list of all users, unwound from any group membership, as well as their Permissions to this object.

This report is helpful when determining how a user gained access to an object and with what level of permission.

## Deleting a Record

Records can be deleted only from the Record List view. Locate the record you wish to delete from within its Parent Container, open the record's Action menu and select the **Delete** option.

Confirm your operation in the confirmation dialog by clicking the **Delete** button (or **Cancel** to not delete) to complete the process.

You can delete a container using the same method as described with a record; however, a container that contains child objects cannot be deleted.

You must first delete all child objects before you can delete this parent container.

## Managing a Record

The **Manage** menu options allow for advanced configuration of the record.

By default, these configurations inherit from their parent so in order to make changes you will either need to update the parent or break inheritance to this record and make updates as required (using the **Make Unique** button).

Command Controls	Defines all the <a href="#">command control policies</a> that are associated to this record.
Formula	Defines the <a href="#">password complexity formula</a> that will be used when generating passwords.
Permissions	Defines the users and groups that have <a href="#">permissions</a> to this record.

Tasks	Defines all the <a href="#">tasks</a> that are associated to this record.
Workflows	Defines all the <a href="#">workflow bindings</a> that are associated to this record.

## Archive/Restore Records

A record that has been switched to the Archive state is one where some of the functionality has been limited (**Tasks**, **Connection** and **Editing**) but the record itself remains in its current location with its current configuration and logs.

For details, please read our [Object Archiving](#) article.

To place a record in an Archived state, choose the **Archive** option located in the **Manage** menu. Records in an archived state will appear visually different from non-archived records.

To restore a record from an Archived state, choose the **Restore** option located in the **Manage** menu.

## Working with Multiple Records (Bulk Actions)

The **Bulk Actions** menu allows you to perform a single action against all your selected records. To use the Bulk Actions menu, first select one or more records using each one's checkbox and then open the Bulk Actions menu and chose your intended operation.

Depending on your selection, the operation may generate a form that needs to be populated, it may generate a confirmation dialog before executing the operation, or the action may automatically be executed.

Your permissions are verified against each record before the operation itself is executed.

For example, if you select two records, one record that you have permissions to delete and a second which you do not, and choose the Bulk Actions > Delete option, the system will verify your permissions and only delete the one record for which you have permissions to delete.

At the conclusion of any Bulk Action, a status report will be generated to show the results for each selected record.

## Clipboard Actions (Copy, Cut, Paste, Link)

You can rearrange or reorganize both your Records and Folders (Vaults cannot be used with Clipboard actions) using standard clipboard actions like **Copy**, **Cut**, **Paste** and **Link**.

These clipboard actions can be performed with a single record or folder or can be done in bulk using the **Bulk Actions** menu options.

Copy	Use Copy to add the selected object(s) to your session's clipboard to be copied (duplicated to a new location).
Cut	Use Cut to add the selected object(s) to your session's clipboard to be moved to a new location (deleted from the current location).

Paste	<p>Use Paste to paste your clipboard object(s) to this current parent container. Paste will create a duplicate copy of the original object(s) or it will move (cut) the original object(s) to this new location.</p> <p>Objects created using <i>Paste</i> will inherit permissions from its new parent; <u>any unique permissions will be lost.</u></p>
Link	<p>Use Link to create a linked object of the original in this new location. Linked records allow you to have the same object appear in multiple locations. Deleting a linked record will only delete the selected instance, leaving the remaining linked records in place. Deleting the last link will trigger deletion of the object.</p> <p>Objects created using <i>Link</i> will retain the inherited permissions from their original parent or their unique permissions as configured.</p>

TIP: You must have permissions to the object in both the original and new locations to successfully complete clipboard actions.

Note: There is the difference between **Copy/Paste** and **Cut/Paste**:

- **Cut** action **moves** the object to a new location (it is deleted from the current location).
- **Copy** action just **copies** the object (it is duplicated to a new location).
- **Copy/Paste** - the object won't inherit any properties from the previous one.
- If PAM User performing **Copy/Paste** actions, it is creating a new object,
- If PAM User performing **Cut/Paste** actions, it is moving the same objects, but these are moved to a different location.

## Finding Objects

All non-Personal Vault records and containers are stored in the same All Records or Root Folder within Access Manager.

Depending on which is most convenient for you, locating specific records can be done easily with any of the following methods:

- You can navigate through the container hierarchy to find your record by *Name* or *Description*.
- You can use the *Search records...* bar to find your record by Name, Description or other indexed field values. You may also save your custom search query to your [Searches menu](#) for later access by using the **Add/Remove Favorites** button.
- You can add your most frequently used records or containers to your Favorites list to easily organize them in your left navigation menu.

## Anonymous Links

Work with Anonymous Access or Guest Links in Privileged Access Management(PAM) is easy.

Generating Anonymous Links within Privileged Access Management allows a user (“author”) to securely share messages or record details with others without requiring them to sign-in to Privileged Access Management making it possible to share information with guests.

Anonymous Link URLs are generated with a unique, random 32 character ID string and can be opened by anyone who has the link until the link’s expiration policy has been met.

Once this expiration policy is satisfied, the content of the Anonymous Link is permanently destroyed.

Anonymous Link URLs will be generated and accessed like below:

```
https://xtam.company.com/xtam/alink/519c43d4-715b-4fff-a583-3afa1d43296e
```

PAM Anonymous Links provide the following benefits over traditional secret sharing through insecure channels like email or instant messaging applications:

- Immediate, time and/or access based expiration policies available to the author.
- Permanent destruction of message upon reaching its expiration policy.
- Dynamic record details that provide up to date values on a read-only HTML page.
- Audit events to track creation, access and expiration of anonymous links.

And of course, please keep these points in mind when determining whether or not to allow Anonymous Links within your PAM deployment:

- By its design, an Anonymous Link and its message content can be accessed and viewed by anyone who has the link. This means that the message author may intend to send it to only one specific recipient, but this recipient could then forward it along to others. Links are not assigned to specific users or groups as they are built to support guests (users without sign-in authentication).
- Administrators cannot view, expire or delete any links or messages that have been sent. They can review the Audit Log to determine who generated the message, but they have no control over the link, its message or configuration once it is generated.
- PAM will need to be available to anyone who wishes to access an anonymous link. Please keep in mind any firewall restrictions or security considerations that may need to be made to allow for external access to PAM. Although recipients are not required to login to PAM, PAM will still need to be externally accessible from the recipient’s location.
- Since Access Manager logins are not required, the **Opened Anonymous Link** audit event will attempt to capture the recipient’s IP Address only. If the recipient happens to be an Access Manager user and is already authenticated in their browser, then it will also capture their username.
- The content of the Anonymous Link will be destroyed and cannot be retrieved after its expiration. Afterwards, navigating to the link will cause an expiration error message.
- Anonymous Links generated from PAM records are used to share record details which will include sensitive information like passwords. Unlock audit events are generated when record links are opened, so Tasks may be triggered from these activities.

## Link for Records

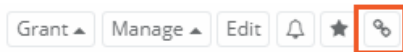
Generating an Anonymous Link for PAM Records.

When generating an anonymous link for a specific PAM record, a link will be generated that will contain the current text values of the record (current as of the time the link is opened) in HTML form; it will not be granting access to the record itself.

1. Login to PAM as a user with Manager or Owner permissions to the record. Alternatively, global System Administrators can generate links as well.

Note: If the link author's Record Control permission level is removed or reduced below Manager or they are blocked by an active workflow, then the contents of the record will not be displayed when the link is opened. Instead the body of the message will read "The author of the anonymous link does not have permissions to the shared item" or "This anonymous link is blocked by an active workflow" until their original permissions have been restored or the workflow has been approved.

2. Open or view the record that you want to generate a link for.
3. Click the **Anonymous Link** button:



Note, if this button is not present than you either do not have the required permission (Record Control: Manager or Owner), you are currently blocked by an active workflow or this feature has been disabled by the System Administrator.

4. In the **Create Anonymous Link** form, fill out all the required fields as desired:
  - **Message:** Enter a message that will be displayed in the body of the link when accessed. The message can be up to 1024 characters long.
  - **Expiration in Minutes:** Enter a numerical value defined in minutes for the amount of time that the message should be available. The expiration time begins when the link is generated, not when it is first accessed, if ever. The maximum allowed time is 4320 minutes (3 days).
  - **Number of Times to Open:** Enter a numerical value that defines the total number of times that the link can be accessed before it is expired. This value must be between 1 and a maximum open value of 5.

5. When the above values are entered, click the **Generate** button to generate your anonymous link URL.

Create Anonymous Link

Production Server

Message

Hey Peter, here is the information that you need to fix the site.

Expiration in Minutes

15

Number of Times to Open

2

Link to Share

https://xtam.company.com/xtam/alink/12554bea-03cf-47e7-b0df-b528a8d306fc

Close

Generate

6. Copy the full URL from the read-only **Link to Share** field to send it to your recipient(s).
7. You may now click the **Close** button to exit the Create Anonymous Link form or adjust the values and click **Generate** again to generate a new link to share.

Once the URL is generated and displayed, the link is active. If you made a mistake, navigate to the **Anonymous Links** section of your Profile, select this link and click the **Expire** button. This action will immediately expire your link (destroying its content) so you can generate a new link.

To review the activity associated to your anonymous links, navigate to Management > My Profile > Anonymous Links.

On this page, you will find all your non-expired links and their configuration. From here, you can confirm their expiration time, understand how many times it has been accessed, find the link’s unique URL or immediately expire any active link(s).

User Profile

Home / My Profile

Profile

Subscriptions

Anonymous Links

Preferences

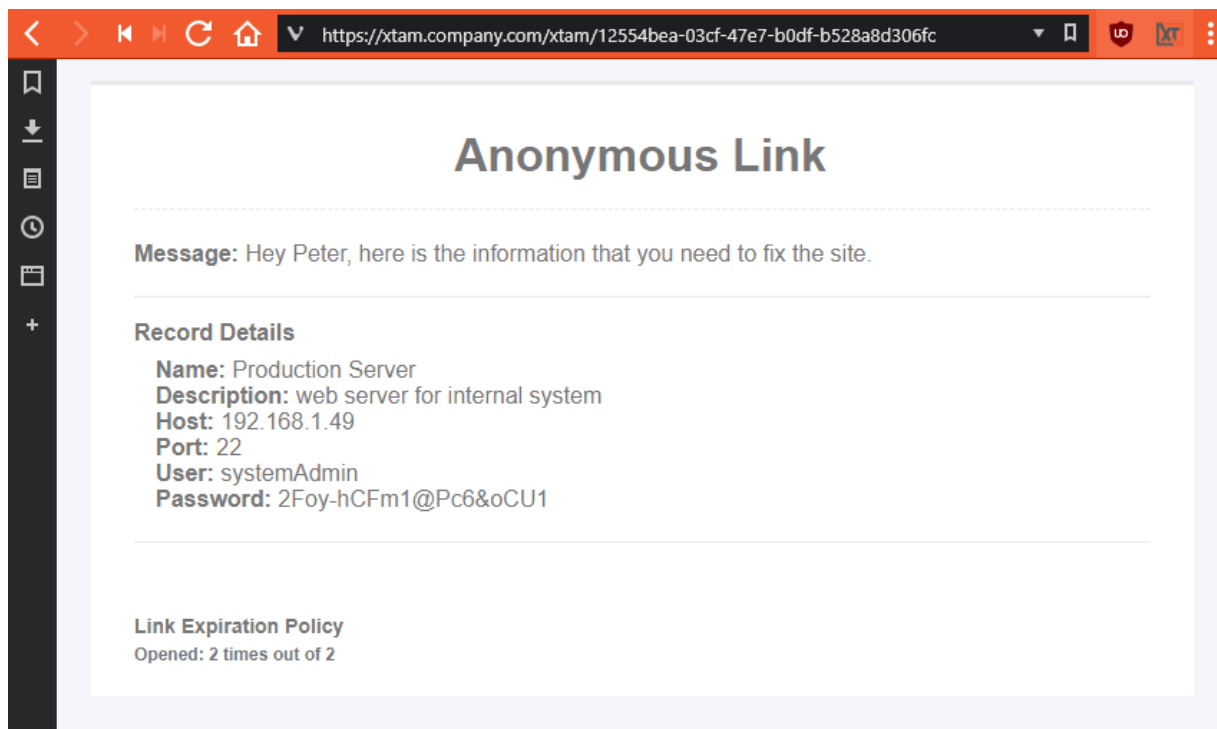
Found 1 links.

CreateExpire

Object	Created	Expiration in Minutes	Number of Times to Open	Opened	Link to Share	Actions
	06/06/2019 13:27	15	2	0	https://xtam.company.com/xtam/alink/12544bea-03cf-47e7-b0df-b528a8d306fc	

Expired links are permanently destroyed and will not be visible.





Anonymous Record Link Content including the Record's Details

## Link with a Generic Message

Generating an Anonymous Link with a Generic Message.

When generating an anonymous link with only a generic message (no association to a specific record), a link will be generated that will contain your generic message in HTML form; it will not be granting access or displaying any information related to an record.

1. Login to PAM with any user. Generic anonymous links that have no association with any records can be created by any authenticated System user.
2. Navigate to Management > My Profile > Anonymous Links and click the **Create** button.

Note: If the Anonymous Links section is not visible, then this feature has been disabled by your System Administrator.

3. In the Create Anonymous Link form, fill out all the required fields as desired:
  - **Message:** Enter a message that will be displayed in the body of the link when accessed. The message can be up to *1024 characters long*.
  - **Expiration in Minutes:** Enter a numerical value defined in minutes for the amount of time that the message should be available. The expiration time begins when the link is generated, not when it is first accessed, if ever. *The maximum allowed time is 4320 minutes (3 days)*.
  - **Number of Times to Open:** Enter a numerical value that defines the total number of times that the link can be accessed before it is expired. *This value must be between 1 and a maximum open value of 5.*
4. When the above values are entered, click the **Generate** button to generate your anonymous link URL.

## Create Anonymous Link

Message

Hi Peter. The default password for your new login is SOiUtO5eAeek78jY

Expiration in Minutes


30

Number of Times to Open

1

Link to Share

https://xtam.company.com/xtam/alink/1cbb0c02-1c91-4262-bd42-ae27b077d0a4



Close

Generate

5. Copy the full URL from the read-only **Link to Share** field to send it to your recipient(s).
6. You may now click the **Close** button to exit the Create Anonymous Link form or adjust the values and click **Generate** again to generate a new link to share.

Once the URL is generated and displayed, the link is active. If you made a mistake, navigate to the Anonymous Links section of your System Profile, select this link and click the **Expire** button. This action will immediately expire your link (destroying its content) so you can generate a new link.

After each new link is generated, it will appear in the Anonymous Link table on this same page.

On this page, you will find all your non-expired links and their configuration.

From here, you can confirm their expiration time, understand how many times it has been accessed, find the link's unique URL or immediately expire any active link(s).

### User Profile

Home / My Profile

Profile

Subscriptions

Anonymous Links

Preferences

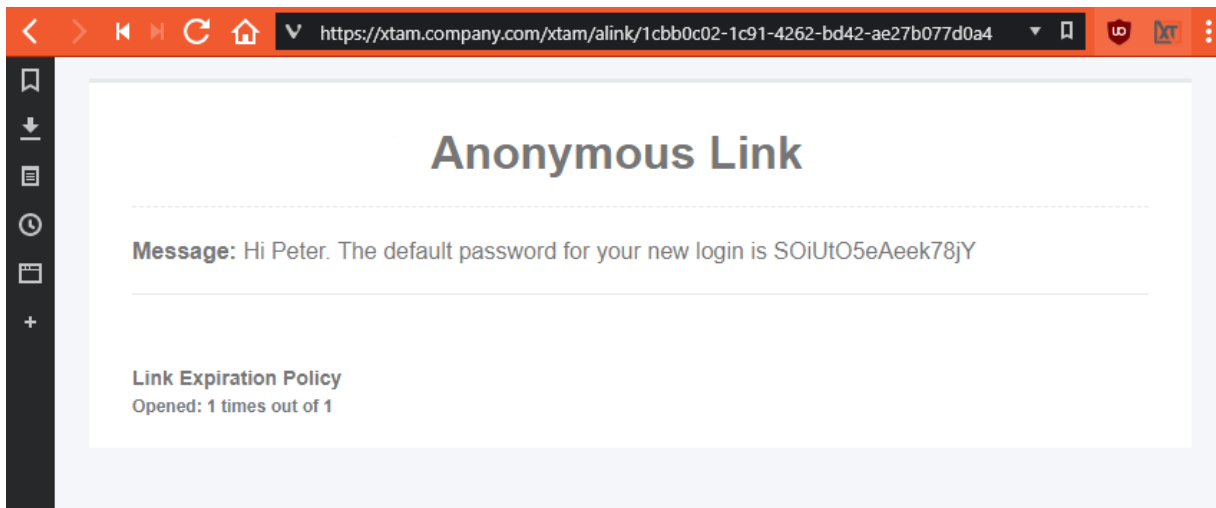
Found 1 links.

Create

Expire

Object	Created	Expiration in Minutes	Number of Times to Open	Opened	Link to Share	Actions
<input type="checkbox"/>	06/06/2019 14:03	30	1	0	https://xtam.company.com/xtam/alink/1cbb0c02-1c91-4262-bd42-ae27b077d0a4	<div></div>

Expired links are permanently destroyed and will not be visible.



Anonymous Generic Link Content that only includes the Author's Message

## Disable the Link

Disabling the Anonymous Link Feature.

System Administrators can choose to enable or disable the use of Anonymous Links in Privileged Access Management.

Please note that if the Anonymous Links feature is disabled, all currently active links will remain accessible until their expiration policy has been satisfied. Disabling anonymous link does not automatically expire active links.

Login to the System with a System Administrator account.

1. Navigate to Administration > Settings > Parameters and locate the Anonymous Links parameter.
2. Select one of the following values:
  - **Enabled:** Enables Anonymous Links to be generated from Access Manager records and generic messages.
  - **Generic:** Enables Anonymous Links to be generated from generic messages. Disables the ability to generate Anonymous Links from Access Manager records.
  - **Disabled:** Disables all Anonymous Link generation in Access Manager.
3. Click the **Save** button to complete your configuration change.

## Design of the Link

Customizing the Design of the Anonymous Link Content.

The visual design of the Anonymous Link content was meant to match the look of the Access Manager system; however if you wish to make changes, this section will describe the process.

You will need to make changes to the System installation, so please work with your Administrators to gain access to the PAM server with the required permissions.

System does not need to be offline nor does it require a restart in order to modify this layout.

Future system updates will not override any custom changes you make to the layout.

1. Login to PAM host server with an account that has permission to modify the `$PAM_HOME` directory. You will be copying and modifying one (1) `.css` file.
2. Navigate to `$PAM_HOME/web/webapps/pam/templates` and copy the file **anonymousLink.css**.
3. Paste this `anonymousLink.css` file to `$PAM_HOME/content/templates`. If the `/templates` directory does not exist, please create it first and then paste the file into this location.
4. Customize **anonymousLink.css** file as desired (it is a standard web style sheet) and save the file when complete. Consult with your Web Designer for assistance when working with the `.css` file.
5. Open (or refresh) any valid Anonymous Link URL to review your changes.

## Expired or Restricted Link

Expired or Restricted Link Content Examples.

These messages will appear if the content in the link cannot be displayed.

Note that the actual text displayed for each of these conditions can be modified by updating the `anonymousLink.css` file as described in the prior section of this article.

When a link expires, the following message will appear when it is opened.

### Anonymous Link

The link you are attempting to view has either expired or is no longer available. Please contact the message sender if you need to view it again.

When a link's author no longer has permission to access the record from which the link was generated, the following message will appear when it is opened.

### Anonymous Link

The author of the anonymous link does not have permissions to the shared item.

When a link's author is blocked by a workflow, the following message will appear when it is opened.

### Anonymous Link

This anonymous link is blocked by an active workflow.

# Archiving Records

Records in Privileged Access Management can be set to an **Archive** state in order to disable use of some of the functionality while remaining in-place. The following article describes what an archived record is and how to archive and restore records.

A record that has been switched to the Archive state is one where some of the functionality has been limited but the record itself remains in its current location with its current configuration.



An example is where you have an underlying managed endpoint that you have shutdown, removed and decommissioned but you wish to keep the record in-place (rather than deleting it) so access to its audit log, historical reports and last password state can still be accessed but not continue executing tasks or establishing remote sessions.

Another case for the use of the Archive state is one where it acts as a first stage recycle bin.

Before deleting the record, a user can switch to the Archive state to limit the record's use and gauge the response from their user base.

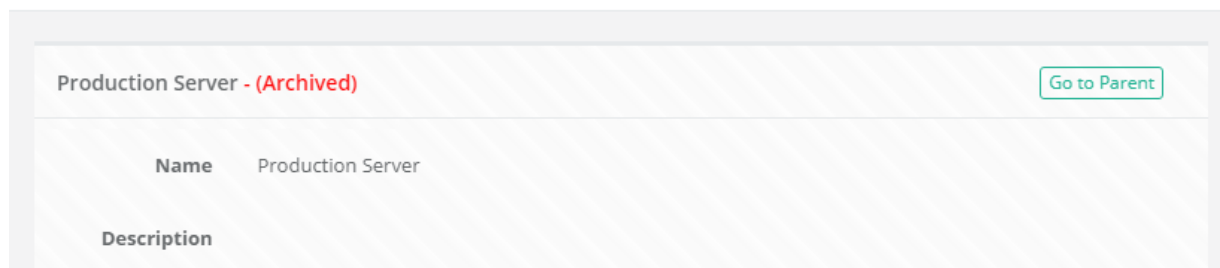
If no one asks about it (or complains) for a set period of time, then it may be safe to go ahead and delete the record or even keep it archived indefinitely.

When a record is archived, the following functionality is altered or limited:

- The standard green record icon () is replaced with a grey record icon () to easily distinguish them.
- When viewing, the record will have a subtle diagonally striped background and **– (Archived)** will be appended to the name to easily distinguish them.

## Record View

Root Folder / 2 AWS / **Production Server**

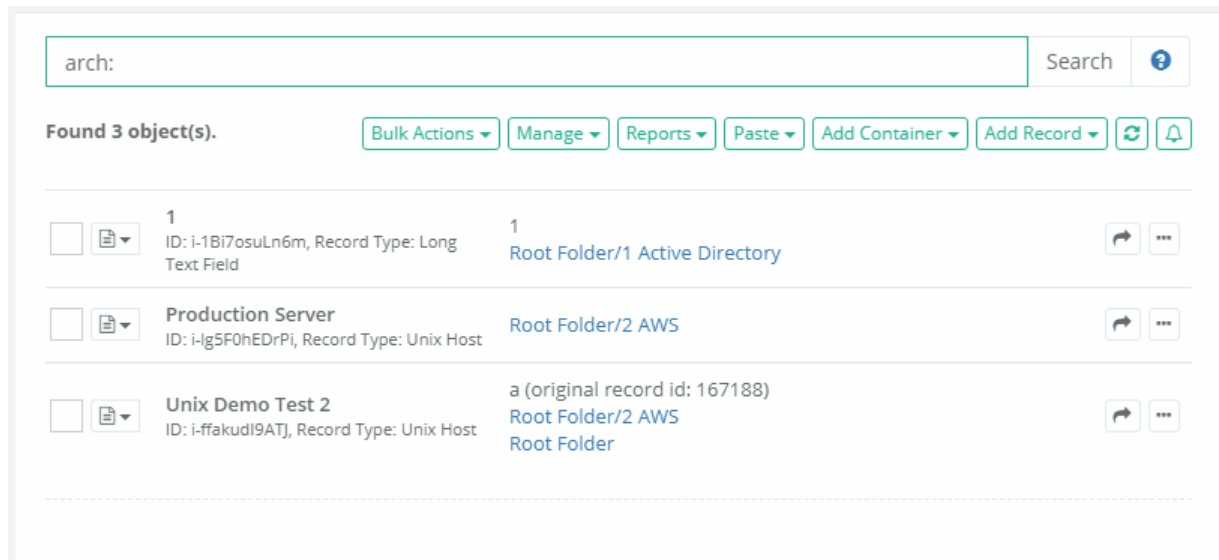


- All associated Tasks will be placed into a suspended state meaning they will not be executed while archived. If or when the record is restored, Tasks will be moved back to their previous state and will resume as configured.
- The option and ability to **Execute** tasks, through any means, will be disabled (permissions are not modified).
- The option and ability to **Connect**, through any means, will be disabled (permissions are not modified).
- The option and ability to **Edit** the record, through any means, will be disabled (permissions are not modified).

## Functionality of an Archived record

When a record is archived, the following functionality is still available:

- An archived record can still be opened or viewed.
- An archived record can still be cut, copied, pasted and deleted.
- The *Audit Log*, *Change History*, *Session History* and *Job History* reports are still accessible.
- Passwords and Secured Fields can be unlocked.
- *Workflows*, *Permissions*, *Formulas*, *Tasks* and *Command Control* configurations are still accessible and can be modified.
- Workflow requests can still be submitted and approved or rejected.
- Audit Events are still generated, including the Archive and Restore events themselves.
- Archived records can still appear in all reports.
- Archived records can still appear in search results. You can use the search query **arch:** to specifically search for archived records.



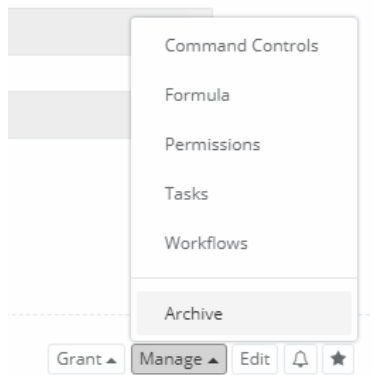
- Alerts and Notifications are still processed and sent.
- Favorite and Unfavorite options are still accessible.

## Archive or Restore record

How can you Archive or Restore an PAM record?

To archive a record:

1. Login to the System with a user that has Manager or Owner permissions to the record or an Privileged Access Management System Administrator. Only Manager, Owner or System Administrator can archive or restore a record.
2. Open or View the non-archived record.
3. Navigate to Manage > Archive.

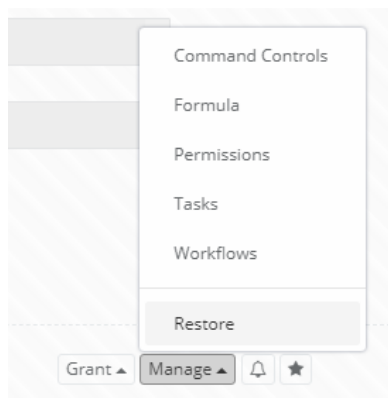


4. Confirm your action by clicking the **OK** button in the dialog.

This record is now archived.

To restore a record:

1. Login to the System with a user that has Manager or Owner permissions to the record or an Access Manager System Administrator. Only Manager, Owner or System Administrator can archive or restore a record.
2. Open or View the archived record.
3. Navigate to Manage > Restore.



4. Confirm your action by clicking the **OK** button in the dialog.

This record is now restored.

## Mass archive or multiple records restore

It is also possible to mass archive or restore multiple records at the same time using Record List Bulk Operations.



To activate the mass archive or restore option:

1. Select several records on the record list.
2. After that, select the menu item *Bulk Actions / Archive or Restore*.

Found 77 object(s).

Bulk Actions ▾
 Manage ▾
 Reports ▾
 Paste ▾
 Add Container ▾
 Add Record ▾
 ↺
 🔔

Show objects per page: 50 ▾

<input checked="" type="checkbox"/>		<b>code signing</b> ID: i-fkKBXPcirOx, Record Type: Certificate	⚙️ 👁️ ↻ ⋮
<input type="checkbox"/>		<b>record</b> ID: i-hLW8UhU4ymY, Record Type: Secured File	⚙️ 👁️ ↻ ⋮
<input checked="" type="checkbox"/>		<b>Secured File</b> ID: i-k2uw891Krk1, Record Type: Secured File	⚙️ 👁️ ↻ ⋮
<input checked="" type="checkbox"/>		<b>Secured File small</b> ID: i-5sNfxNrc1pA, Record Type: Secured File	⚙️ 👁️ ↻ ⋮
<input checked="" type="checkbox"/>		<b>Session Connect Host</b> ID: i-1a3DQMRNxf3, Record Type: Windows Host	▶️ ⚙️ 👁️ ↻ ⋮
<input type="checkbox"/>		<b>Session Connect Login</b> ID: i-9echvkV7SUI, Record Type: Windows Host	▶️ ⚙️ 👁️ ↻ ⋮
<input type="checkbox"/>		<b>SQL server for App</b> ID: i-20AU05S7Ac, Record Type: Windows Host	▶️ ⚙️ 👁️ ↻ ⋮
<input type="checkbox"/>		<b>SSH Tunnel</b> ID: i-7qnsdi8i4sU, Record Type: Unix Host	▶️ ⚙️ 👁️ ↻ ⋮
<input type="checkbox"/>		<b>Telnet</b> ID: i-hQVEfuk9NVW, Record Type: Telnet Host	▶️ ⚙️ 👁️ ↻ ⋮
<input type="checkbox"/>		<b>test_ephemeral</b> ID: i-13LScpOrqTS, Record Type: Windows Host Ephemeral Account [34.219.23.136]	▶️ ⚙️ 👁️ ↻ ⋮

Request Access  
 Request Unlock  
 Request Execute  
 Execute  
 Share  
 Inherit Permissions  
 Inherit Workflows  
 Update  
 Unselect All  
 Copy  
 Copy Folders  
 Cut  
 Delete  
**Archive**

3. Confirm the operation.

**Warning!**

**Please confirm mass record archiving.**

OK

Cancel

4. After the operation is completed, confirm the result in the operation log that appears on the screen.

## Tracking Archived Objects

To track records that have been Archived or records that have disappeared, there are 2 searches that will show these records:

Archived Records

- Browse to Searches > **Archived Records**
- For each record that you want to restore, click the ellipses (...) and select the **Restore** option

Orphaned Objects

- Browse to Searches > Archived Records
- From the Query drop-down on the left, select **Orphaned Objects**



- Click **Search**
  - Find the object that you wish to recover
  - Click the ellipses (...) and select **Copy**
  - Browse to the location that you want this record to appear
- Use the option Paste > Link option

## Record List

Root Folder

•


Orphaned Objects ▾

Search for Orphaned Objects that do not belong to any folder...

✕

+

Search



Found no records.

Bulk Actions ▾


Manage ▾


Reports ▾


Paste ▾

Add Container ▾

Add Record ▾







## Generating Strong Passwords

Privileged Access Management provides an option to generate a new, strong password for any password field included with a record.

The password will be generated randomly based on the Formula policy that is currently associated to this record.

### To generate a random password

1. Create a new Record or view an existing record that includes the default *Password* field.
2. Click the **Edit** button for this record.
3. To the right of the *Password* field, click the **Key** button (Privileged Access Management **Generate Password** Button) to generate a random password. The password will automatically be added to the password field. You can click the **Unlock** button (Privileged Access Management Generate Password Unlock Button) to view this new password.

Password

YNjlyZV5UmRd#{2j)615^%YG2nsz93{=YRa(n9X6wHxg3\_h



Save Save and Return Cancel

4. When satisfied with the password, click the **Save** or **Save and Return** button to complete the operation. The password will not be saved to the record until you click one of the **Save** buttons.
- If you **Cancel** out of the Edit page, then the original password in this Record will not be updated.

To customize the [password complexity requirements](#), either modify the Formula associated to this record or the [Formula](#) assigned to the Record Type (if Formula inheritance is enabled).

Privileged Access Management contains an [easy random password generator screen](#) accessible from any part of the WEB application.

# Object Export (Export to CSV)

The record list Export option allows a System Administrator to export objects (vaults, folders or records) to a CSV file that can later be used as an [Import](#) into the same or a different PAM instance or location. Some common uses for this type of object level CSV Export / Import are:

- Moving objects to a different PAM deployment such as Production to Staging / Test, regional deployment, or other examples.
- Copying containers with child records between locations of the same PAM deployment. This is a good use case for geo-distributed departments or individual clients in an MSP-type deployment.
- Migrating or consolidating multiple PAM objects into one instance or splitting a single instance into several regional or client-based setups.
- Making an export of a customer's vault by a managed service provider (MSP) which can later be used for importing into an independent PAM server in their network.
- Creating hierarchy templates for multiple regional locations of MSP customers to use as a base for repeatable onboarding.
- Moving data between personal vaults in the events of onboarding or offboarding of employees or move generic data out of a personal vault to shared vaults.
- Making a copy of data from shared vaults to a developer's personal vault for development and testing of PAM API integration scenarios.

The intent of this Export feature is to provide a [System Administrator](#) an option to export objects to a CSV file that can then be used to import to PAM. Each object's values like Host, User, Password and others are encrypted by the user provided password so that the file itself does not contain these sensitive values in clear text.

To import this exported CSV file, the user will be required to provide the identical password that was used to encrypt the values during export. Failure to provide a password or providing the incorrect password will prevent the Import from being processed.

## Considerations for CSV Object Export

Before you begin, please read the following considerations to determine if your requirements will be met by this feature.

1. Historical log data about the exported object(s) including, but not limited to, audit log events, change history, job history, session history and object metadata (ID, created by/date, modified by/date) are not exported. Imported objects are created as new objects in the destination location.
2. Linked objects will be created as new, non-linked objects after import.
3. Permission and [Workflow](#) configurations on the included object(s) are not exported.
4. Custom Record Type definitions are not exported. If a custom Record Type or Field is used by objects in the export, they must exist by the same name in the target instance prior to import for a successful result. The internal name of a field is used in the CSV file, not its Display Name.
5. Be aware of exported records that include [Reference Records](#). The export file will contain the name of the [Reference Records](#) as a value, but it may not include the actual [Reference Records](#) depending on the

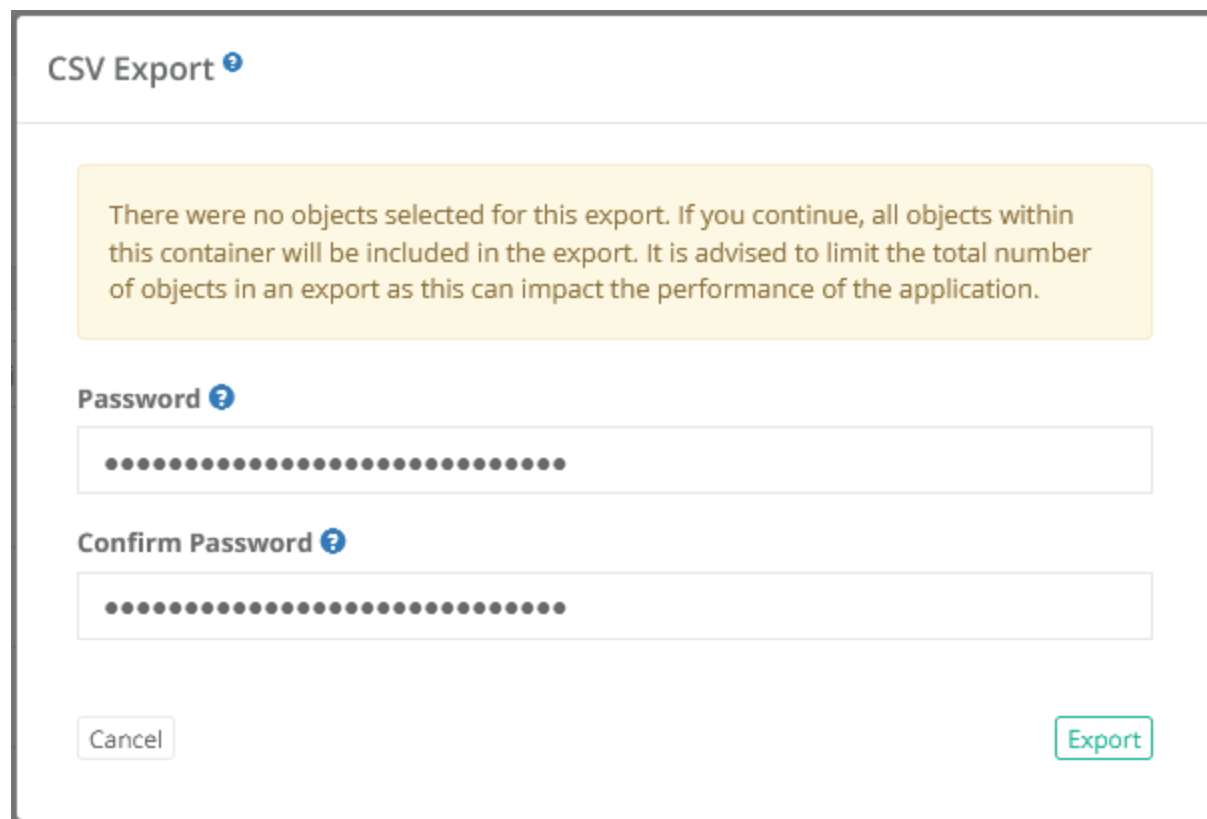
user's selection. Be sure to check the Import results to ensure the configured [Reference Records](#) was set properly.

Depending on the number of objects included in the Export, this operation can take several minutes or longer to complete. Please consider performing this operation during off-peak or low-peak times if you need to export > 1000 objects.

## To Export a Parent Container to a CSV file:

1. Login to PAM with a System Administrator account. *Only a System Administrator may create a CSV Export.*
2. Navigate into the parent container, Vault or Folder, that you wish to Export.
3. Without selecting any objects, from this container's Manage menu, choose the **Export** option.
4. When prompted, **enter a password** that will be used for encryption. Type it a second time to **confirm your password**.

Secure this export password in a safe location and do not share it with others unless required. If lost, you will not be able to recover this password from PAM nor the exported CSV file.



The screenshot shows a 'CSV Export' dialog box. At the top, it says 'CSV Export' with a help icon. Below this is a yellow warning box with the text: 'There were no objects selected for this export. If you continue, all objects within this container will be included in the export. It is advised to limit the total number of objects in an export as this can impact the performance of the application.' Below the warning box are two password input fields. The first is labeled 'Password' with a help icon, and the second is labeled 'Confirm Password' with a help icon. Both fields contain a series of dots representing masked characters. At the bottom left is a 'Cancel' button, and at the bottom right is an 'Export' button.

5. Click the **Export** button to begin the export process of all the objects located within this container.
6. When the Export is complete, the CSV file will be downloaded from your web browser. The CSV file will

contain the parent folder from which the export was processed and all objects contained within this parent.

If a workflow binding has been applied to your account, then you must Request Export and be approved prior to having the option to perform an Export. The [Workflow](#) approval will only be applied to the container, and its child objects, from which the request was submitted. For example, if the Request Export was submitted on the folder named Production Servers, once approved, this user may then export the objects contained only within this folder for as long as the workflow approval remains active.

## To Export Selective Objects to a CSV file:

1. Login to PAM with a System Administrator account. *Only a System Administrator may create a CSV Export.*
2. Navigate into the parent container, Vault or Folder, that you wish to Export.
3. From within this container, **select** the objects to export by clicking the checkbox next to each object to include.

Please note that if you select a folder, this will include all child objects in this folder including any subfolders.

4. After you selected all the objects to include, from this container's Manage menu, choose the **Export** option.
5. When prompted, **enter a password** that will be used for encryption. Type it a second time to **confirm your password**.

Secure this export password in a safe location and do not share it with others unless required. If lost, you will not be able to recover this password from PAM nor the exported CSV file.



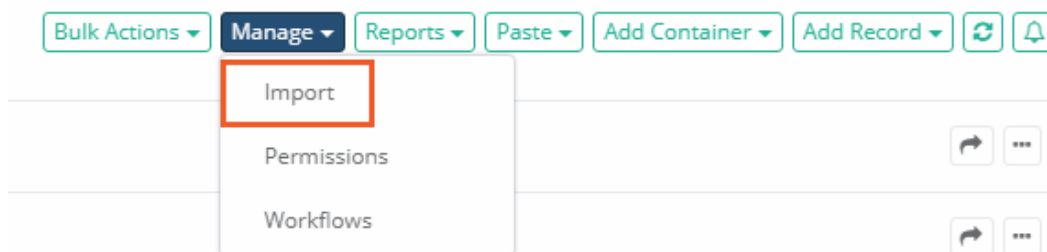
6. Click the **Export** button to begin the export process of all the objects located within this container.
7. When the Export is complete, the CSV file will be downloaded from your web browser. The CSV file will only contain the selected objects.

If a workflow binding has been applied to your account, then you must Request Export and be approved prior to having the option to perform an Export. The [Workflow](#) approval will only be applied to the container, and its child objects, from which the request was submitted. For example, if the Request Export was submitted on the folder named Production Servers, once approved, this user may then export the objects contained only within this folder for as long as the workflow approval remains active.

## Importing Records from Third Party Systems

The Import option available in Imprivata Privileged Access Management (PAM) allows any permitted user (Editor, Owner or System Administrator) to import their existing records and connections from several popular sources, including CSV, Remote Desktop Connection Manager and PuTTY.

During the import process, the folders and records contained within your files will be created in PAM using their commonly shared parameters like name, description, host and port.



This will assist in getting users to more quickly adopt Access Manager as the interface will look like an experience in which they are familiar.

The following Import options are currently supported:

1. [Import from a CSV File](#) (can be used for mRemote and other connection manager “Export to CSV” options)
2. [Import from a Remote Desktop Connection Manager save file](#) (.rdg)
3. [Import from an exported PuTTY file](#) (.reg)
4. [Import from an exported KeePass version 2 file](#) (.xml). More [here](#).

If you would like to discuss other import options, please contact our Support Team <https://support.imprivata.com/communitylogin>.

There is also an [Import Overwrite](#) option to configure the software to support existing records of the same name.

## CSV file

### To import from CSV file:

1. Create your own CSV file using this [attached file](#) as an example. Please take particular notice of the CSV headers as those are required in order for the Import to process.

The headers in the CSV upload file must match an existing field name available in your chosen Record Type. For example, if you want to upload a value to a field named *Service*, then this field *Service* must already exist as part of your selected Record Type and you must include **Service** in the CSV header as a column.

2. Login to PAM and either create a new folder or navigate to an existing folder that will serve as your root import location. *NOTE: If you do not create or use a folder, then all objects will be imported to the Root Folder.*

Note: vault can be imported on Root folder level only. Vault cannot be imported to another folder or vault.

To import objects with difficult structures such as `folder/folder/record` or `vault/folder/record`, parent objects should be separated using `" / "`.

To import a file you should write path to the record like this: `file:Disk:\path\to\file` for example, `file:D:\CSVImport-CertFiles\certificate.cer`.

3. Click **Import** to begin the process.
4. Click the **Select File** button and load your `.csv` file.
5. Click **Import** to begin the process.
6. When it is complete, a log will be generated to show the status of each folder and record. Please review this log to ensure all objects were created successfully.
7. Return to the import location to begin using your new records.

## RDC Manager save file

### To import from Remote Desktop Connection Manager save file:

1. Open Remote Desktop Connection Manager and save your session as a **.rdg** file.
2. Login to PAM and either create a new folder or navigate to an existing folder that will serve as your import location. *NOTE: If you do not create or use a folder, then all objects will be imported to the Root Folder.*
3. Click import to begin the process.
4. Click the **Select File** button and load your **.rdg** file.
5. Click **Import** to begin the process.
6. When it is complete, a log will be generated to show the status of each folder and record. Please review this log to ensure all objects were created successfully.
7. Return to the import location to begin using your new records.

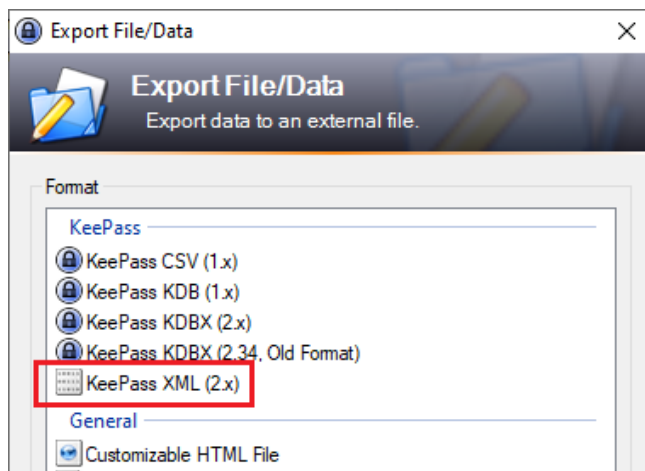
## PuTTY export file

### To import from PuTTY export file:

1. Save your PuTTY session to a **.reg** file.
2. Login to PAM and either create a new folder or navigate to an existing folder that will serve as your import location. *NOTE: If you do not create or use a folder, then all objects will be imported to the Root Folder.*
3. Click import to begin the process.
4. Click the **Select File** button and load your **.reg** file.
5. Click **Import** to begin the process.
6. When it is complete, a log will be generated to show the status of each folder and record. Please review this log to ensure all objects were created successfully.
7. Return to the import location to begin using your new records.

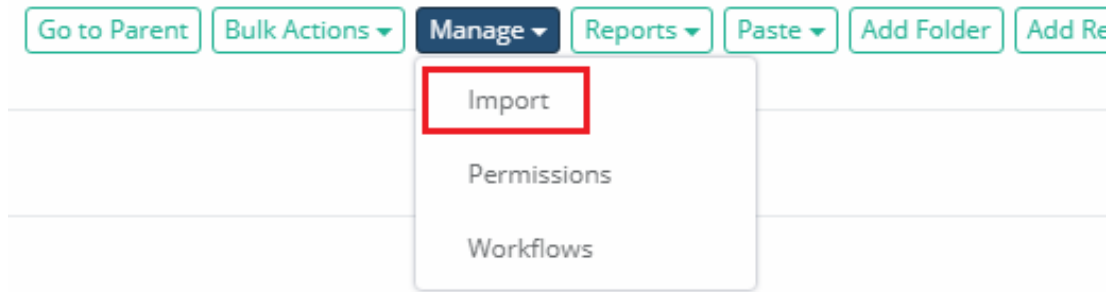
## Import a KeePass v2 Export

1. Create your KeePass version 2 export using its native Export option. When exporting, you may either export the entire *Database* or a selected *Group*, use the format **KeePass XML (2.x)**.



2. After the export has been generated, login to PAM with either a System Administrator account or Owner to the folder that will be used for Import.

3. Navigate into the System folder (or vault) that will be the import location and select the Manage > Import option from this folder's toolbar.



4. Click **Select File** to then choose your KeePass .xml export file for import.
5. Finally, click the **Import** button to begin the process.

Please note that exported Remote Desktop Connection Manager and PuTTY sessions use encryption for passwords, certificates and keys. Due to the possibility of someone using PAM as a means of decryption, these fields will not be included with our Import process and as a result, any record that contains one of these fields will need to be edited to include their value before it can be used in PAM.

## Import Overwrite Behavior

When importing records, you must also select the overwrite option that best supports your requirements. Each option outlines how PAM will process existing records during import.

For the purpose of **Import Overwrite**, *existing records* are defined by having an exact Record Name match in the same location as an object from the import file. The available options are:

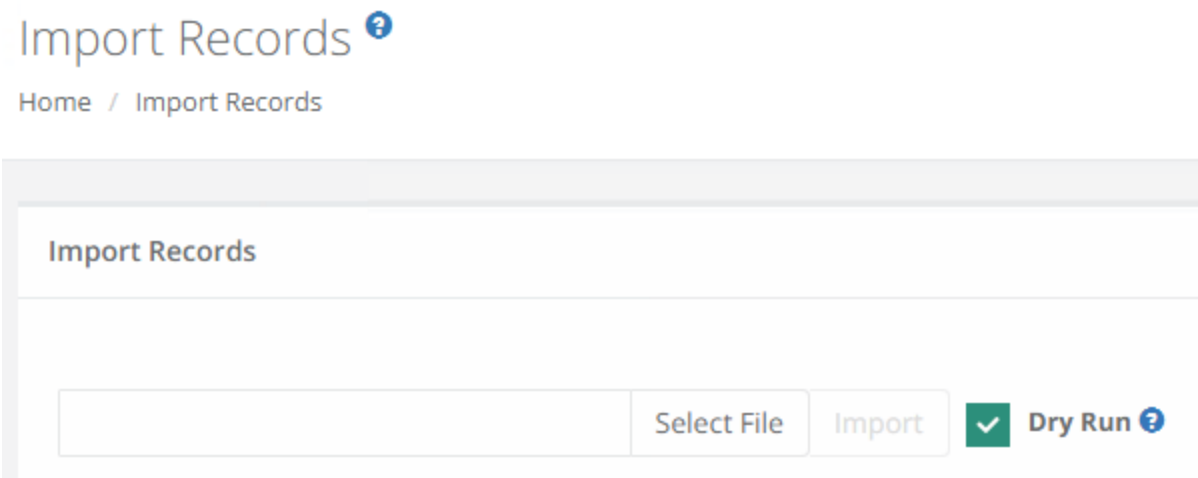
1. Create  
The Create option does not check for existing records when importing new records. This is the fastest option; however, this option might create duplicate records when importing to an existing record hierarchy.
2. Skip (slower)  
The Skip option detects existing records during the import process and skips them from import while only importing new, non-existing records. Skip is slower than the Create option in detecting existing records; however, it might provide better overall performance in cases when most of the records in the import file already exist in this location.
3. Update (slowest)  
The Update option detects existing records during the import process and updates the first found match for each existing record with the values from the import file generating a record update event. This import option also creates new records when matching existing records are not found. This option is the slowest one for the import process.

## Dry Run for CSV, KeePass, RDG and PuTTY files

For Import of the objects from CSV, KeePass, PuTTY or Remote Desktop Connection Manager files to your Records you can use Dry Run.



The option runs the Import process and reports issues as the regular import process without actually creating objects in the system.

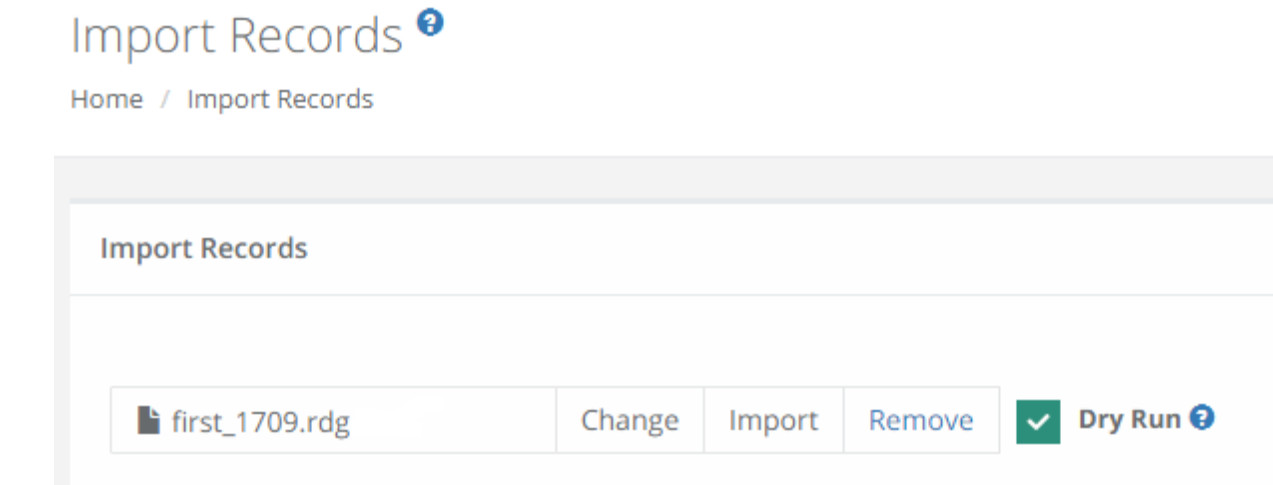


To be sure your objects have no errors, we recommend you to use Dry Run.

Dry Run does not consider any of the Import Overwrite options for its evaluation. It only evaluates the values of each object from the import file.

**To Dry Run your objects:**

- 1. Go to Records > Manage > Import.
- 2. Add the object to the field, and touch the check-box with the Dry Run.



- 3. Press the **Import** button.
- 4. Now you can see the Status of the objects.

Import Records			
Import complete. Please review the results below or return back to your import folder to continue.			
<a href="#">Return Back to Folder</a>			
Name	Type	Status	Message
Timesheet system	Record	OK	
{Secret=, Type=Unix Host, Description=PBX phone server, User=ITAdmin, ReferenceId=, Parent=WEB, Reference=, Port=1532, Host=192.168.1.88, Url=, Name=PBX, Password=*****}	Folder	ERROR	The parent object "WEB" was not found. Please update your file and try again.
IT	Folder	OK	

Note: the objects with errors can be imported as well.

if the objects for Import are OK:

Import Records			
Import complete. Please review the results below or return back to your import folder to continue.			
<a href="#">Return Back to Folder</a>			
Name	Type	Status	Message
server	Record	OK	
ms	Record	OK	
1	Record	OK	
1	Record	OK	
1	Record	OK	

Note: if you choose *Dry Run* option, PAM creates no objects in the file system. To Import these objects you need to choose the object and press the **Import** button.

*Dry Run* is unchecked by default.

# Import from KeePass

Import KeePass v2 Entries into the Identity Vault.

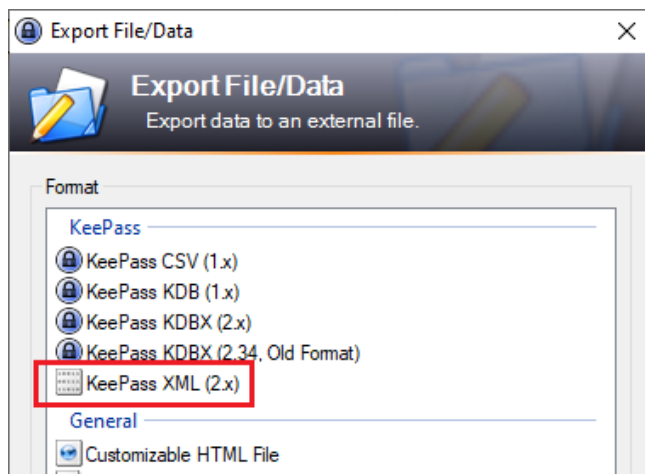
KeePass Password Safe is very popular free client side password management tool which is efficient in managing personal accounts and passwords in a secure way; however, it does not scale well for multi-user or corporate use.

If you are planning the transition from KeePass to Access Manager, then our built-in utility provides an easy method to preserve entries, group hierarchy and smart detection of entry types.

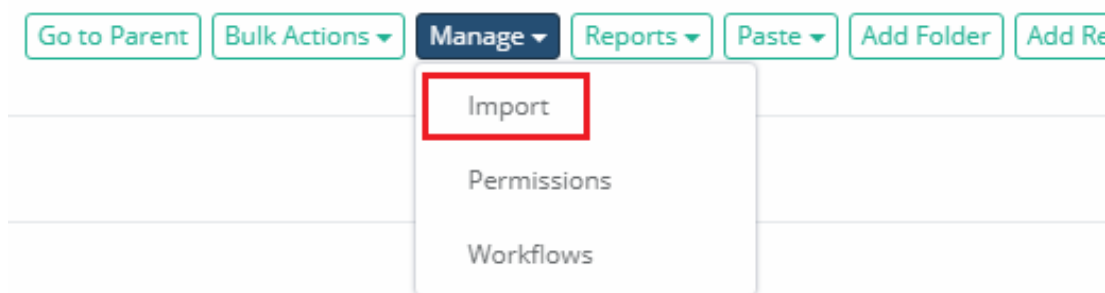
For Import of the objects from CSV, KeePass, PuTTY or Remote Desktop Connection Manager files to your Records you can use [Dry Run](#).

To Import a KeePass v2 Export into Access Manager:

1. Create your KeePass version 2 export using its native Export option. When exporting, you may either export the entire *Database* or a selected *Group*, use the format **KeePass XML (2.x)**.



2. After the export has been generated, login to Access Manager with either a System Administrator account or Owner to the folder that will be used for Import.
3. Navigate into the System folder (or vault) that will be the import location and select the Manage > **Import** option from this folder's toolbar.



4. Click **Select File** to then choose your KeePass `.xml` export file for import.
5. Finally, click the **Import** button to begin the process.

After the import is complete, review the results to ensure all objects were imported successfully.

The KeePass Import Utility includes the following mapping guidelines:

- KeePass Groups are created as System Folders, including its root Database.
- KeePass Group and Entry Notes are created as System Folder or Record Description.
- KeePass Entry URL is created as System Record Host or URL. If the KeePass URL is blank, then the Title will be used instead.
- KeePass Entries located in a Group named Windows are created as System Records using the Windows Host record type. \*
- KeePass Entries located in a Group named Unix, Linux or Network are created as System Records using the Unix Host record type. \*
- KeePass Entries located in any other named Group are created as System Records using the WEB Portal record type. \*
- KeePass Entry References, History, String Fields, Attachments or any other properties not mentioned above are unsupported.
- KeePass Entries located in a Group named Unix, Linux or Network and have a password and a file, are created as System Record using Unix Host with a Protected Key record type.
- KeePass Entries located in a Group named Unix, Linux or Network and have the password field empty but have a file are created as System Record using Unix Host with a Protected Key record type.
- KeePass Entries have only a file attached are created as System Record with a Certificate record type.

If a KeePass entry has a blank User Name and blank URL, then the System Record will be created using the Secret record type.

You can change the Record Type after the import is complete by selecting your Records and using the option Bulk Actions > Update.

[< Back to Importing Records from Third Party Systems](#)

## Record Field Options and Types

When [creating or extending Record Types](#), you are provided the option to add new Record Fields.

These record fields are what users will have the option to populate when creating new Records in PAM.

Edit Field:

Save Cancel

Field Type	<div>String</div>
Name	<div></div>
Display Name	<div></div>
Hidden	<div><input type="checkbox"/></div>
Secured	<div><input type="checkbox"/></div>
Indexed	<div><input type="checkbox"/></div>
Order	<div></div>
Helper	<div></div>
Default Value	<div></div>

The following is a list of available options when creating or modifying Record Type Fields.

**Field Type:** Defines the type of value that can be entered into this field.

**Name:** This will be the internal name of the field (no spaces allowed). It must be unique and it's recommended to use an alphanumeric string.

**Display Name:** This will be the name of the field that user's will see in the Record. It's recommended to keep it short, but descriptive.

**Hidden:** Checking this box will make this field hidden. PAM will hide this field from the record's View and only those with *Record Control: Editor* or higher will be able to see or modify it when editing the record.

**Secured:** Checking this box will make this field secured. PAM will conceal the value entered into the field and require *Record Control: Unlock* or higher for the user to see it. A common example for using a secured field is for Passwords.

**Indexed:** Checking this box will make this field's value searchable. Any user with at least *Record Control: Viewer* or higher will be able to use the PAM search bar to locate this record using this value in their search query.

To maintain the security around secured values, **Secured** fields will not be indexed.

**Order:** Defines the ordering of how fields appear in the Record view. Fields with a lower order appear before fields with a higher order.

**Helper:** The Helper value can be used to display descriptive text into the field to provide assistance to the user as to which value is expected in this field. It is similar to a tooltip, but it appears directly in the field.

**Default Vault:** The value set in the Default Value field will be the preset value when new records are created or for existing records that contain an empty value. The use of a Default Value is not available for all Field Types.

## Field Types

### Checkbox

- Used to provide a checkbox boolean option.
  - The default state will be unchecked.

Checkbox



### Choice

- Used to provide an option that is presented with multiple choices in a dropdown menu.
  - Choice options should be entered as a single line separated with a comma.

Choice

Choice1  
Choice2  
Choice3

### Date

- Used to provide an option that is presented with multiple choices in a dropdown menu.
  - This will generate a date selector that also provides an option for time, displayed as hours and minutes.

Date

2018-02-03  15 : 30

### File

- Used to provide an option where a user can upload and attach a file to the record.

File

Select file

### Number

- Used to provide an option where a user is limited to entering only numeric values. Supports up to 9 values.

Number

123456789

### String

- Used to provide an option where a user can enter a single line of text.

String

user@domain.com

### Text

- Used to provide an option where a user can enter multiple lines of text.

Text

Key: \_.>Cp,s9XsUX# `U6myBpC}Xo  
Key: s?aOYAj|##-5Q.8G6gc\$2LCic  
Key: a%b|Fnaxg5eMmpuKaq1uQ6

## Reference Record

A reference record is a record that is used in multiple other records so that any parameters (*Host, Port, User, Password, Certificate, Passphrase* or *custom fields*) can be shared.

For example, you could create an Active Directory (AD) account record and rather than re-entering the same user, password, certificate or passphrase into multiple other records, you could simply point to this AD account as a reference and the system will auto-populate and maintain these parameters.

The system will then “reference”, instead of storing a copy, this original record when needing to access the shared credentials.

In addition to making it easier to build out and organize your system, this also makes it much more convenient when rotating passwords.

In the previous example, if this AD account was NOT used as a reference, when the password was changed in any record, the others would stop working because their password is now outdated.

Alternatively when it is configured as a reference, a password reset executed on any would then be updated to all.

## Using of reference record

First, to ensure security, in order for any user to configure a record with a reference, they must have at least *Editor* permission on this new or existing record and at least *Unlock* permission to the reference record.

Once granted the necessary permissions, simply enter or select the record in the Reference Record field and the shared parameters will be added for you (and overwrite any current parameters in these shared fields).

Shared parameters are read only so if you need to modify them then you will need to edit the reference record itself.

SQL Database

Name

Description

Reference Record

---

Type

Host

Port

User

Password

If you would like to remove a reference record and instead assign parameters directly to a record, simply remove the reference from the field, the shared parameters will become *read/write* enabled and then enter your new parameters as needed.

Once complete, click the **Save** button to finish the operation.

SQL Database

Name

Description

Reference Record

---

Type

Host

Port

User

Password

Enter the value **\$null** into a field to prevent it from being referenced in other records.

If questions about architecture and system recommendations for large scale farm deployments remain or issues arise while using PAM, please contact the Support team:

<https://support.imprivata.com/communitylogin>.



# Saving a File to a Record

Privileged Access Management’s *Records* can be used to securely store (encrypted) and share any file types including certificates, keys, archives and documents in its AES-256 bit protected database.

This is extremely useful when needing to share file objects between trusted users while maintaining security and capturing audit events like who downloaded the file and when.

To begin, you may use an existing *Record Type* that contains a secure File field or you may create your own custom Record Type.

For the purpose of this exercise, we are going to create our own custom type.

- 1. Login to the System as a System Administrator and then navigate to Administration > Record Types.
- 2. Click the **New Record Type** button to start creating your own custom type.

## Record Types

Home / Record Types

Record Types List

Found 9 record types.

Refresh

New Record Type

Record Type	Parent Record Type	Session Manager	Action
<input type="checkbox"/> Secret			<div>Edit</div>
<input type="checkbox"/> Active Directory			<div>Edit</div>

- 3. Enter a unique **Name** and (optionally) a **Description**. Leave the **Session Manager** option empty because this record will be used to store files, not establish remote sessions. Also leave the **Parent Type** option empty as well as we are not going to inherit any fields from an existing type. Click the **Save** button.

Record Type: Secured File

Found fields.

Save

Name

Secured File

Description

Record to store files

Session Manager

Parent Type

- 4. Your new record type has been created, so it is now time to add our custom fields. Click the **Add Field** button.

5. Enter a unique **Name** (*name is used internally to store the file*) and a **Display Name**. The display name will be shown in the Record so it should be easily understandable by others. Check the **Secured** box, enter 100 for sorting **Order** and finally leave Helper empty. Click **Save** to continue.

Record Type: Secured File 2

Edit Field: securedFile01

[Save](#) [Cancel](#)

Field Type File ▼

Name

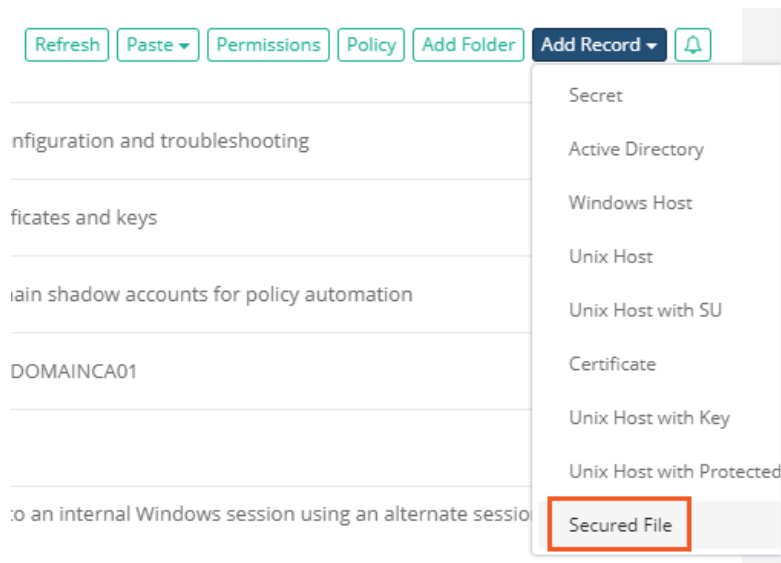
Display Name

Secured ☒

Order

Helper

6. If you would like to add additional custom fields, simply repeat the process above based on your requirements. When satisfied with your new custom Record Types and its fields, continue on to the next step.
7. Navigate to Records > All Records.
8. Click the **Add Record** button to open the drop down menu and then select your new Record Type.



9. Enter a **Name** for this new Record and optionally a **Description**. Below these two default fields, will be the custom fields we created earlier. In our example, there are two secured File fields.
10. To work with *File* fields, simply click the **Choose File** button and open a file selector dialog. Locate and add your file to this field. Repeat this process as often as necessary to add or replace a file associated to the field.

## Our Network Logins

<b>Name</b>	Our Network Logins
<b>Description</b>	An Excel file containing all our network and service logins and passwords. DO NOT SHARE WITH NON-IT EMPLOYEES!
<b>Type</b>	Secured File
<b>Secured File (01)</b>	<input type="button" value="Choose File"/> NetworkLogins.xlsx
<b>Secured File (02)</b>	<input type="button" value="Choose File"/> NetworkLo...mote.xlsx

- When complete, click **Save and Return** to save the record and return back to the All Records view.
- You have now created a Record that stores your encrypted file in the PAM system. At this point you can View the record to observe how it will appear to other users, you may **Edit** the record to change the file (s) or modify its **Permissions** to share it with others.
- To download the file from PAM's secured Record, click the **Unlock** button to the right of the field and then click on the file's name. A confirmation box will appear, so click **OK** to begin the download.

## Our Network Logins

<b>Name</b>	Our Network Logins
<b>Description</b>	An Excel file containing all our network and service logins and passwords. DO NOT SHARE WITH NON-IT EMPLOYEES!
<b>Secured File (01)</b>	NetworkLogins.xlsx <input type="button" value="Unlock"/>
<b>Secured File (02)</b>	NetworkLogins - Remote.xlsx <input type="button" value="Unlock"/>

If you followed through with this exercise, navigate over to the system's Audit Log now (Administration > Audit).

This is the area of the system where all events are captured and available for review. In this log you should see the results of our previous actions of creating the Record Type, Creating the Record, Unlocking the file and finally Downloading the file from the system.

Found 499 audit log records.

Time: Last Week ▼

Category: Any ▼

Level: Any ▼

Event: Any ▼

[Refresh](#)Show  entriesSearch: [Copy](#)[CSV](#)[Excel](#)[PDF](#)[Print](#)

Showing 1 to 50 of 499 entries

Time	User	Object	Category	Level	Event	Message
08/02/2017 11:21:13	Chris Kolodziejcki (chrisk)	<a href="#">Our Network Logins</a>	Data	INFO	Download	NetworkLogins.xlsx
08/02/2017 11:21:02	Chris Kolodziejcki (chrisk)	<a href="#">Our Network Logins</a>	Data	INFO	Unlock	
08/02/2017 11:20:39	Chris Kolodziejcki (chrisk)	<a href="#">Our Network Logins</a>	Data	INFO	Create	
08/02/2017 11:19:50	Chris Kolodziejcki (chrisk)		Data	INFO	Record Type Add Field	Record Type: Secured File, Field: securedFile02
08/02/2017 11:19:22	Chris Kolodziejcki (chrisk)		Data	INFO	Record Type Add Field	Record Type: Secured File, Field: securedFile01
08/02/2017 11:18:50	Chris Kolodziejcki (chrisk)		Data	INFO	Create Record Type	Record Type: Secured File

## Split View and Secret Co-ownership

To comply with specific security policies, maintain regulatory compliance and enforce segregation of duty, it may become a business requirement to ensure that no single user has access to the entire secret, password or parameter within a record.

Some refer to this functionality as the “Two-person rule” because it requires one user to retrieve the first part of a password and a second (or more) user to retrieve the remainder, thus requiring two people to construct the full password.

In Privileged Access Management, we call this “Split View” and when enabled, the *Unlock* option will either reveal the first part of the record’s password or the second part based on your configuration.

This prevents a single PAM user from ever being able to *Unlock* the complete password for a record.

Password

5R+Td.:6U7%{|\*\*\*\*\*



Password


\*\*\*\*\*|e\$vseLMpqq[2



## Configure

To configure Split View:

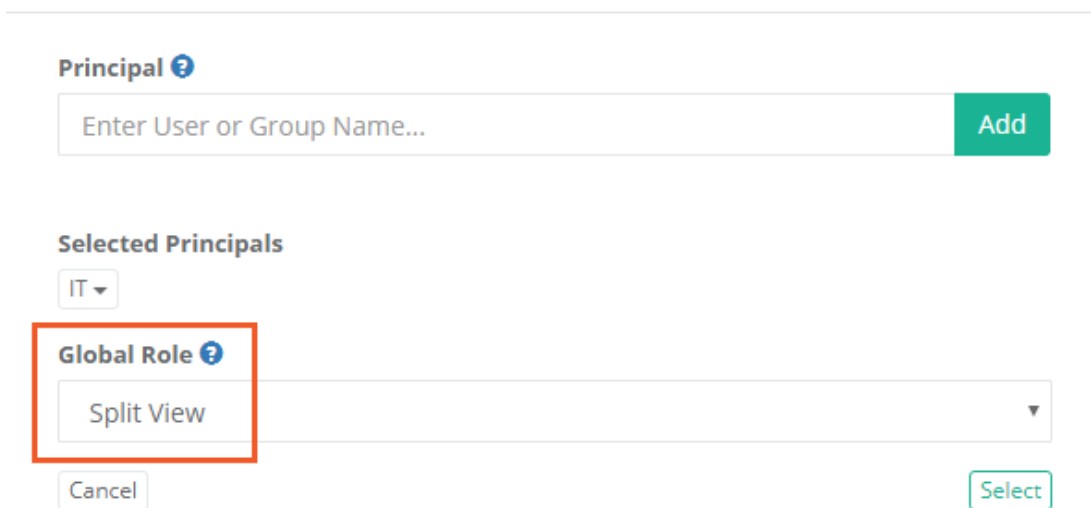
1. Login to the System as a System Administrator.
2. Navigate to Administration > Settings > Parameters.
3. Locate the option **Split View Role** and select one of the available options.



Split View Role First Part [?] Save

- a. **Disabled**: When selected, the Split View functionality is disabled.
  - b. **First Part**: When selected, the users assigned the Global Role Split View will reveal only the first part of the value when using the *Unlock* option.
  - c. **Last Part**: When selected, the users assigned the Global Role Split View will reveal only the last part of the value when using the *Unlock* option.
4. Click the **Save** button for this option.
  5. Navigate to Administration > Global Roles.
  6. Click the Add button, add a Principal(s) and assign the Global Role *Split View*.
  7. Click **Select** button to complete this role assignment.

## Grant Access



Principal ?

Enter User or Group Name... Add

Selected Principals

IT

Global Role ?

Split View

Cancel Select

Note that the user(s) or group(s) assigned this role will reveal either the first or last part of the value in the unlocked field. All other PAM users not assigned this role will reveal the remaining part of the value.

8. Split View is now enabled.

## Test

### To test Split View:

1. Login to the System as a user with the Global Role *Split View*.
2. Open a record with a *Password* field and click the **Unlock** button.

3. The password will be revealed as shown below.

Password

5R+Td.:6U7%{|\*\*\*\*\*



Please note that the partial password is displayed by splitting the full value into two equal parts, defining the split with a pipe (|) character, with the remaining concealed password displayed as asterisks (\*\*). The pipe character appears in both halves of the split and is not part of the password itself.

4. Logout and then login to the System as a user without the Global Role *Split View*.
5. Open the same record and click the **Unlock** button.
6. The other portion of the password will now be revealed to this user.

Password

\*\*\*\*\*|e\$vseLMpqq[2



7. For comparison, here is the full, non-split, password used in this example.

Note the use of the pipe (|) is only to define the split and is not an actual character in the password.

Password

5R+Td.:6U7%{e\$vseLMpqq[2



## Consideration

### For Consideration when Enabling Split View:

1. The Split View functionality is only applied to a record's *Unlock* option.  
Editors, Owners and System Administrators will be able to view the full, non-split password in both the Edit and Change History views of the record.
2. When Split View is enabled, it is applied to all System users with at least the *Unlock* permission to a record.

## Creating a SSH session record

1. InPrivileged Access Management, create a new record using one of the available Unix types. This includes **Unix Host** (user and password auth), **Unix Host with Key** (user and ssh key auth), **Unix Host with Protected Key** (user, ssh key and passphrase auth), **Unix Host with SU** (user and password with switch user) or any custom record type for utilizes the *SSH protocol*.
2. Populate all the fields with your endpoint's connection details.
3. Click the **Save and Return** button.

Your record is now saved and under management in Privileged Access Management.

All access to this record will be captured in the audit log, including Active and Completed sessions as well as keystrokes.

[Permissions](#) and [workflows](#) can also be applied to your users or groups ensuring only authorized personnel can access to the record.

Forbidden sequences and meta-commands (ctrl-c, ctrl-d, etc) for users are regulated by the System Administrators and run under [Command Control](#) policies.

Your CISO, Auditors and Security team are now smiling.

[<Using your SSH session record in a native SSH Client](#)

## Containers

### Containers (Folders and Vaults)

Two forms of containers exist within the system, Folders and Vaults. Both options serve as containers that can hold child objects and inherit their configuration down to these child objects.

For a complete list of differences between these containers, please see our article [PAM Containers: Folders vs Vaults](#).

### Create a New Container

From within your desired parent container, click the **Add Container** button and select the *container type* to use from the dropdown menu list.

Enter both a **Name** (required) and **Description** (optional).

Neither the Name nor Description must be unique but for ease of use we recommend creating at least a unique description, if not both.

TIP: Vault containers can only be created in the **All Records** or **Root Folder** container. If you are currently within a vault or folder, then only the *Add Folder* option will be present to create a sub-folder. Vaults cannot be created inside containers.

### Opening or Editing a Container

A container can be opened from the Record List page by either clicking on the container's Name or selecting the **Open** option located in its dropdown menu.

A container can only be edited from the Record List page by selecting the **Edit** option located in its dropdown menu.

The *Edit* page will allow you to modify both the *Name* and *Description* of this container.

### Sharing a Container

Containers can be shared with other users that have access to the system.

To share a container with another user(s) or group, click the **Share** button for this container on the Record List page or select the **Permissions** option located in the container's top menu (Manage > Permissions).

Before you can share a folder, it is recommended to understand its current inheritance. Containers can either have inherited permissions or unique permissions. Vaults are always created with unique permissions, but they can be reset to inherit from their parent (i.e. All Records or Root Folder).

NOTE: Permissions are configured by default to inherit from the object’s parent container. When sharing a container, you will either need to share the parent container so that through inheritance this container is also shared (along with all other child objects) or you can break inheritance and create unique sharing permissions for an individual container. Both scenarios are equally supported, but you should consult with your object Owner or PAM System Administrator for guidance and recommendations.

Containers with *inherited permissions* (example shown below) means that the permissions associated to this object originate from its parent. This means if you want to share a container with inherited permissions, then you must share its parent object. Modifying permissions on a parent object will then affect all other objects that inherit permissions from it as well. When viewing the permissions of an object with inherited permissions, the button **Make Unique** will be visible. Clicking this **Make Unique** button will break the permission inheritance of this object to its parent and create a unique permission list that can be modified as needed.

Permissions ⓘ

Root Folder / IT Records / Permissions

Permissions for IT Records / inherited from Root Folder

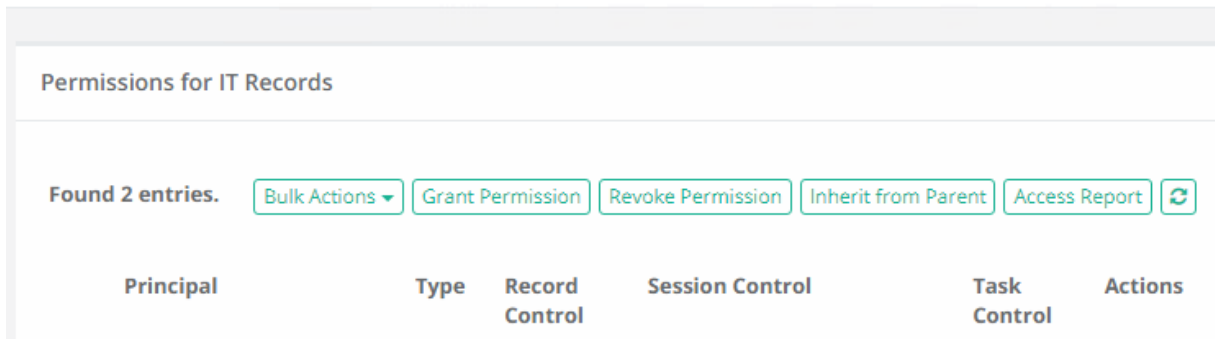
Found 2 entries.

Make Unique Access Report ↺

Principal	Type	Record Control	Session Control	Task Control	Actions
-----------	------	----------------	-----------------	--------------	---------

Containers with *unique permissions* or broken inheritance (example shown below) means that the permissions associated to this object do not originate from a parent and are unique to only this object. This means if you want to share a container with unique permissions, then you can do so without affecting the permissions of its parent. When viewing the permissions of an object with unique permissions, the button **Inherit from Parent** will be visible. Clicking this **Inherit from Parent** button will remove all unique permissions and reestablish inheritance from this object’s parent.





## To Share or Grant Permission to the selected object:

1. Access the object's permissions page by using the **Share** button or Manage > **Permissions** option.
2. Click the **Grant Permissions** button to open the dialog.
3. In the Principal field, enter the user(s) or group(s) that you wish to share with and then click the **Add** button. You may also use the **Search** button to locate your principal.
4. Configure the [object permissions](#) that you wish to grant to the selected principal(s).
5. Finally, click the **Select** button to complete the sharing or granting process.

## To Edit existing permissions to the selected object:

1. Access the object's permissions page by using the Manage > Permissions option.
2. Locate the Principal from the list that you want to edit their permissions and click the **Edit** button in the Actions column.
3. In the *Grant Access* dialog, confirm the principal is correct and then modify their permissions as required.
4. Finally, click the **Select** button to complete the edit process.

To Revoke existing permissions to the selected object:

1. Access the object's permissions page by using the Manage > Permissions option.
2. Select the Principal that you wish to revoke permissions from the list by checking their box and click the **Revoke Permission** button.
3. Confirm your action to revoke the selected permissions in the confirmation dialog.

For ongoing maintenance and auditing, the **Access Report** button will generate a list of all users, unwound from any group membership, as well as their Permissions to this object. This report is helpful when determining how a user gained access to an object and with what level of permission.

# Deleting a Container

A container can be deleted from the *Record List* page by selecting the **Delete** option located in its dropdown menu.

Please note that a container that contains child objects cannot be deleted. You must first delete all child objects before you can delete this parent container.

# Managing a Container

The **Manage** menu options allow for advanced configuration of the container.  
By default, the *Permissions* and *Workflows* configurations inherit from their parent so in order to make changes you will either need to update the parent or break inheritance to this container and make updates as required (**Make Unique** button).

Import	Defines your import location. Your import will create objects in this originating container.
Permissions	Defines the users and groups that have access to this container.
Workflows	Defines all the workflow bindings that are associated to this container.
Local Users	Create and Manage local users that are specific to this container.
Local Groups	Create and Manage local groups that are specific to this container.
Tokens	Create and Manage API tokens that are generated specific to this container.

Before making changes to the manage options of your container, please ensure you are in and working with the container you wish to update.  
The name of the container you are managing will be displayed in the *Record List* breadcrumbs.

## Container Scoped Objects

Containers (Vaults or Folders) can have objects created that are specific to this container only.  
This allows for local users, groups and API tokens to be created and managed not only by System Administrators but also by the *Container Owners* as well.  
These container scoped objects can only be used within the container that they are created and are useful for scenarios where the System Administrator wishes to delegate the management of users, groups and API tokens to the container owners themselves.

When considering the use of *Container Scoped Objects*, please note the following guidelines:

- These objects can be created and managed by any users with the **Record Control: Owner** permission to any folder or vault, with the exception of Root Folder and any folders located in a user's Personal Vault.
- Container Scoped Principals (principals are Users or Groups) can only be used within the container in which they were created. For example:
  - A container scoped user created in Folder A cannot be used in Folder B, unless both folders exist as subfolders of the same first-level parent.
  - A container scoped group created in Folder A can include global principals or principals from this same folder or parent only. It cannot include container scoped users from another first-level container.
- Container Scoped API Tokens can only be generated for Container Scoped Users available within this designated container, including any subfolders.
- Container Scoped Principals cannot be granted the [Global Roles](#) System Administrator or Auditor.
- Container Scoped Principals cannot be granted any [Global Permissions](#).
- Container Scoped Principals cannot be a member of any [Global Local Groups](#).

For Container Owners, all subfolder container scoped principals and API tokens can be managed from the parent folder.

For System Administrators, all subfolder container scoped principals and API tokens can be managed from the parent folder or they can manage the same objects from the Administration area of the product for global reporting or management.

## Container Scoped Local Users

Create and manage local user accounts that can only be used within this container itself.

These user accounts can be used to share objects or generate API tokens that are only valid in this container.

Creating a container scoped local user does not automatically grant them access to any objects.

Once created, permissions will still need to be granted to them as usual or they will need to be added to the appropriate container scoped groups as needed.

## Container Scoped Local Groups

Create and manage local groups that can only be used within this container itself.

These groups can be used to share objects that are only valid to this container.

## Container Scoped API Tokens

Create and manage API tokens that are assigned for use to container scoped users and can only be used within this container itself.

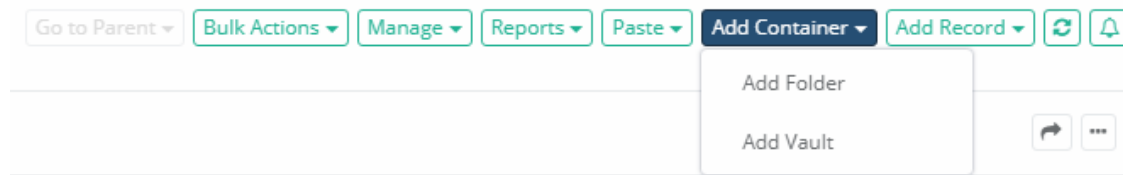
## Difference between Container Types

Privileged Access Management provides containers to make the organization, sharing and management of many records more easy.

For example, all managed records, endpoints or accounts that are specific to your IT department can be saved in a container named IT Dept.

Or if you are a MSP or MSSP managing multiple customers, then you can save and secure all of your customer's records in their own customer named container.

These containers can be created in the form of either a *Folder* or a *Vault*.



While both Folder and Vault containers provide a similar look, they do offer distinct uses as this article will describe.

Please read through the list of differences to help determine if your needs better fit with the use of a Folder, a Vault or a combination of both in PAM.

- Vaults can only be created in PAM root folder. You may create a (sub-)Folder in a Vault, but you cannot create a Vault within a Folder.
- Vaults cannot be created inside containers.
- Vaults can only be created and deleted by System Administrators.
- Vaults have a different color and icon compared to Folders so they can be more easily identifiable.
- Vaults are created with unique permissions. When a new Vault is created, it will include the permissions assigned to PAM Root Folder at the time of creation, but it will not be set to Inherit modifications made to these permissions.
- Vaults and Folders can be used as [Proximity Group](#) Selectors: both options are available now while previously it was limited to Vaults only. Proximity Groups allow for remote session managers to be deployed to isolated networks so records within these Vaults and Folders will have their traffic routed to the specified network without opening standard ports which can be then be found and used by threats.

Group:

Group Name

Must contain value

Selector

Default

▼

Servers

Default

IP-Range

Host Mask

Vault Based

Folder Based

Composite

- For more information about these Remote Session Managers and their architecture, please see our blog titled [Deployment Architecture to Scale Session Manager](#).
- Cross-vault shadow account usage is not allowed. This means if you have a task running on a record in Vault A, this task will fail when configured with a [Shadow Account](#) record from Vault B.
- Cross-vault dynamic credentials search usage is not allowed. This means if you have dynamic credentials for a specific user finding a record from another vault then the user will fail to Connect with the audit log message Failure to activate dynamic credential to find a record from the same vault using criteria:  
**CRITERIA.**

You can disable this blocker by adding the following line to your `$PAM_`  
`HOME/web/conf/catalina.properties` file and then restarting the pam management service:

**`xtam.shadow.crossvault.disable=true`**

## Sharing Records or Containers

When two or more users need access to a record or folder in Privileged Access Management (PAM), the Owner of this object must share access to it, meaning its permissions must be modified.

When the permissions are modified and shared with a user (or group), then the Owner also needs to specify which level of control this user (or group) should have on the object.

Before we show you how to share, let's review the basic Permission model in PAM.

Sharing and [Permissions](#) consists of a few key concepts; [Users or Groups \(Principals\)](#), [Record Control](#), [Session Control](#), [Task Control](#), [Inheritance](#) and [Global Roles](#).

For an up-to-date list of permissions, please review [Privileged Access Management Permissions](#).

- [Users or Groups \(Principals\)](#): These may be local users or groups, or Active Directory users or groups.
- [Record Control](#): These are the defined set of permissions that will be granted to the user or group. This includes but is not limited to view, edit and delete operations on this object.
- [Session Control](#): If the record contains a host connection, then this will determine if the users or group can establish a secure session to this host.
- [Task Control](#): If the record contains a task, then this will determine if the user or group can execute, review or manage these tasks.
- [Inheritance](#): Inheritance is used throughout PAM to more quickly establish a parent/child relationship between objects. If a parent object has a specific set of permissions and a child inherits from it, then that child object will have identical permissions. If a child has unique permissions (not inherited), then the parent and child may have a different set of permissions associated to them. This concept is important when determining how you want to structure your sharing and permission model for [Records](#) and [Folders](#).
- [Global Roles](#): These are the user or group of users that will be granted limited or full system wide access to PAM.

[To Share or Grant Permissions a Record or Folder](#)

[To Unshare or Revoke Permissions to a Record or Folder](#)

[To Edit a User or Group's Permission to a Record or Folder](#)

[To Inherit Permission to a Record or Folder from its Parent](#)

## Editing Permissions

1. Login to PAM with an account that has Owner permissions to the Record or Folder you want to unshare with others.
2. **Open** the Folder or **View** the Record that you wish to Edit and click the **Permissions** button.
3. Locate the User or Group whose permissions you wish to Edit and click the **Edit** button to the right.

### Permissions for Shadow Accounts

Found 3 records.

[Refresh](#)

[Grant Permission](#)

[Revoke Permission](#)

[Inherit from Parent](#)

Principal	Type	Role	Session	Actions
<input type="checkbox"/> Chris Kolodziejewski (chrisk)	User	Owner	Connect	<a href="#">Edit</a>
<input type="checkbox"/> IT User 01 (it01)	User	Editor	None	<a href="#">Edit</a>
<input type="checkbox"/> Peter Senescu (psenescu)	User	Owner	None	<a href="#">Edit</a>

4. In the *Permission* dialog that appears, make the necessary changes and click **Select** to complete the operation.
5. The object's permission will refresh and immediately reflect the modification(s) just made.

[To Share or Grant Permissions a Record or Folder](#)

[To Unshare or Revoke Permissions to a Record or Folder](#)

[To Inherit Permission to a Record or Folder from its Parent](#)

## Inheriting Permission

1. Login to PAM with an account that has Owner permissions to the Record or Folder you want to unshare with others.
2. **Open** the Folder or **View** the Record that you wish to Edit and click the **Permissions** button.
3. Click the **Inherit from Parent** button.

### Permissions for Shadow Accounts

Found 3 records.

Refresh

Grant Permission

Revoke Permission

Inherit from Parent

Principal	Type	Role	Session	Actions
<input type="checkbox"/> Chris Kolodziejski (chrisk)	User	Owner	Connect	<input type="button" value="Edit"/>
<input type="checkbox"/> IT User 01 (it01)	User	Editor	None	<input type="button" value="Edit"/>
<input type="checkbox"/> Peter Senescu (psenescu)	User	Owner	None	<input type="button" value="Edit"/>

4. Read and then confirm that you understand this operation by clicking **OK**.
5. The object's permission will refresh and immediately display that it is now inheriting from its parent. All previously unique permissions and sharing on this object were revoked and those of its parent have been granted via inheritance.

[To Share or Grant Permissions a Record or Folder](#)

[To Unshare or Revoke Permissions to a Record or Folder](#)

[To Edit a User or Group's Permission to a Record or Folder](#)

## Creating Permissions

1. Login to PAM with an account that has Owner permissions to the Record or Folder you want to share with others.
2. **Open** the Folder or **View** the Record that you wish to share and click the **Permissions** button. A view detailing the current permissions associated to this object will display.

The Inheritance concept described above will become visible immediately when looking at an object's permissions.

If this object inherits from its parent, the Title will state that it inherits permissions and specify the parent from which it does.

- If this object inherits permissions from its parent, the Title will state it inherits and the parent from which it does. You will also see a button labeled **Make Unique**.

#### Permissions for ACME Domain Shadow Account / inherited from [Shadow Accounts](#)

Found 2 records.

Refresh

Make Unique

Principal	Type	Role	Session	Actions
<input type="checkbox"/> Chris Kolodziejcki (chrisk)	User	Owner	Connect	<a href="#">Edit</a>
<input type="checkbox"/> Peter Senescu (psenescu)	User	Owner	None	<a href="#">Edit</a>

- If this object does not inherit (unique permissions), then it will not state this in the Title. You will also see three buttons; **Grant Permissions**, **Revoke Permissions** and **Inherit from Parent**.

#### Permissions for Shadow Accounts

Found 2 records.

Refresh

Grant Permission

Revoke Permission

Inherit from Parent

Principal	Type	Role	Session	Actions
<input type="checkbox"/> Chris Kolodziejcki (chrisk)	User	Owner	Connect	<a href="#">Edit</a>
<input type="checkbox"/> Peter Senescu (psenescu)	User	Owner	None	<a href="#">Edit</a>

If you want to share this object but it inherits from its parent, then you will need to modify the parent's permissions. Once modified, the parent's permissions will be automatically made available on this child object via inheritance.

If you want to share this object but don't want to modify the parent, then you will need to make this object's permissions unique and then Grant Permissions directly to it. In this scenario, both the parent and child will have different permissions which allows for greater control over sharing; however, it also makes the management of these objects more difficult.

3. For the sake of this example, let's assume the object has unique permissions or is the Root Folder. Click the **Grant Permission** button located in the toolbar.
4. Enter the user or group name in the Principal field and click **Add**. This principal will now be listed below the field.



- Now select the **Role** and **Session Control** level from the drop down menu that will be granted to this principal.

### Grant Access

#### Principal

Add

#### Selected Principals

#### Role

#### Session Control

CancelSelect

- Click **Select** to complete the operation.
- The Grant Permission dialog will close and the object's permission will now reflect the modification(s) just made.

[To Unshare or Revoke Permissions to a Record or Folder](#)

[To Edit a User or Group's Permission to a Record or Folder](#)

[To Inherit Permission to a Record or Folder from its Parent](#)

## Revoking Permissions

### To Unshare or Revoke Permissions to a Record or Folder:

- Login to PAM with an account that has *Owner* permissions to the Record or Folder you want to unshare with others.
- Open** the Folder or **View** the Record that you wish to unshare and click the **Permissions** button.
- Locate and select the Users or Groups whose permissions you wish to revoke and check the box next to their entry.
- Click the **Revoke Permission** button.

Found 3 records.

Refresh

Grant Permission

Revoke Permission

Inherit from Parent

Principal	Type	Role	Session	Actions
<input type="checkbox"/> Chris Kolodziejski (chrisk)	User	Owner	Connect	<button>Edit</button>
<input checked="" type="checkbox"/> IT User 01 (it01)	User	Editor	None	<button>Edit</button>
<input type="checkbox"/> Peter Senescu (psenescu)	User	Owner	None	<button>Edit</button>

5. The object's permission will refresh and immediately reflect the modification(s) just made. The selected User or Group no longer has access to this object.

[To Share or Grant Permissions a Record or Folder](#)

[To Edit a User or Group's Permission to a Record or Folder](#)

[To Inherit Permission to a Record or Folder from its Parent](#)

## Record Types

### Record Types

Record Types are the foundation of all records stored in the system. Through extensive use of inheritance, fields, tasks, formulas, and command control policies, configurations can be automatically applied or updated to all records that are built from their record type unless these objects have their record inheritance broken.

A Folder record type can be used to add custom fields to containers; vaults and folders.

These custom fields can be used to add metadata to containers that will be visible in the Record List view and can be used for enhanced Folder search.

Unlike other record types, this Folder record type can only be used to add new fields to a container.

## Working with Record Types

Record Types changes can only be performed by users with the System Administrator role. To manage all system Record Types, navigate to Administration > Record Types.

**TIP:** Access Manager comes "out of the box" with many prebuilt Record Types. While it is possible to edit or delete any of these types, we recommend that you create new record types rather than editing or deleting these default Types.

### Creating Record Types

On the Record Type administration page click the **New Record Type** button to create a new type. Create your new record type by populating the fields as explained below

Name	Enter a name for this record type as it will appear in the Add Record dropdown menu. It must be unique and should be short, yet descriptive enough for your users to understand its intent when selecting it from the <b>Add Record</b> dropdown menu.
Description	Enter a description. The record type description will only be visible in the <b>Record Type</b> administration page view.
Session Manager	Select the session manager to associate with this type. Session Manager determines the protocol to use when creating a remote session using this type. For example, for a record type that will be used with Windows endpoints, you would select the RDP option. Leaving this selection blank will result in the <b>Connect</b> option being unavailable in the records.
Parent Type	If inheritance from an existing record type is desired, then select the parent type from the dropdown menu. If inheritance is not desired, then leave this selection blank.
Hidden	Check this box if you want to not have this record type appear in the <b>Add Record</b> dropdown menu.
Personal Vault	Check this box if you want to make this record type available to be used in <b>Personal Vaults</b> .
Vaults	Unhidden record types can be assigned to a non-personal vault(s) where it may only be used. A record type assigned to a Vault(s) may only be used within those selected vaults preventing its ability to be created, pasted, imported, or linked to another vault where this type is not available. <b>Unhidden</b> record types without any defined Vault selections will be available in all non-personal vaults.

NOTE: To create your Folder record type, click the **New Record Type** button and enter exactly Folder into the Name field. This special Folder record type will be created with limited options and can only be used to create new custom fields specifically for container metadata.

Click the **Save** button to save your new record type.

When the record type has been created, you can now configure its additional properties as explained below.

## Fields

Defines the fields that will be visible on all records that use this record type. Additional fields can be added to record types using the **Add Field** button.

Field Type	Select the type of field from the dropdown menu.
Name	Enter an internal name for this field. Must be unique, alpha-numeric characters only and must begin with an alpha character.

Display Name	Enter a display name for this field. This will be the field name that users see when Creating, Viewing or Editing records, so make it short, yet descriptive.
Secured	Check this box if you want the field to be secured. Secured fields are masked from view, have the Unlock feature, require permission to see the unmasked value and generate additional audit events when <b>Locked</b> and <b>Unlocked</b> .
Indexed	Check this box if you want the field value to be indexed so that it can be found in Search queries. Please note that a Secured field cannot be Indexed and vice versa.
Order	Defines the order of the fields in the record. Lower number appears higher in the record.
Helper	Enter a helper value that will appear in the field to provide guidance when the user is creating a new record.

Click the **Save** button after each new field is configured. Repeat this process to create additional fields.

## Formula

Defines the [password complexity formula](#) that will be inherited to all records that use this record type.

## Tasks

Defines the [tasks](#) that will be inherited to all records that use this record type.

## Commands

Defines the [command control policies](#) that will be inherited to all records that use this record type.

### *Editing Record Types*

Any existing record type can be edited after it is created.

To edit a record type, simply click the **Edit** button to enter the selected record type's **Edit Mode**.

In Edit Mode, changes to the record type's configuration, fields, formula, tasks and command control policies can be made and these updates will be applied to all inherited records.

### *Deleting Record Types*

Any record type that is not being used can be deleted.

A record type that is currently being used by any record in the system cannot be deleted until all the in-use records have been updated to use another type or deleted themselves.

To find all records that use a specific record type, enter the query **type:Record Type Name** in the *Search records...* box on any Records page.

For example, the search query **type:Windows Host** will return a list of all current records in the system that are configured with the record type *Windows Host*.

### *Inheritance*

Record types use inheritance to simplify the management of objects that share or require a common configuration.

For example, all managed Unix systems should have the same password Formula and password rotation Task, while all managed Windows systems will share a different formula and task configuration policy.

By default, all records created from the same record type will inherit the [Formula](#), [Tasks](#) and [Command policies](#) from this record type.

Any changes that need to be made to these policies must be done on the record type level and will therefore also be applied to all other records that are using this record type.

NOTE: While inheritance from record type to record is the default configuration, you can also break inheritance on a record and make the above configuration(s) **unique**. Once the settings are unique to a record, they can be updated as required without affecting the record type configuration or any other records that continue to inherit from the type. Additionally, you can also choose to **Inherit from Parent** within the record's configuration page(s) if you wish to return it back to its inherited state with its record type.

Additionally, a custom child record type can be created so that it inherits from a parent record type. In this scenario, the *child record* type only inherits the fields from its defined *parent* type.

## Default Record Types

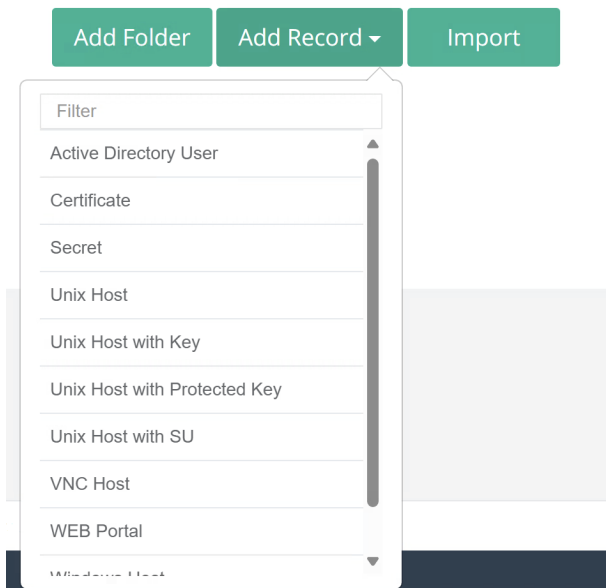
PAM provides a variety of out of the box Record Types to assist in creating, organizing, connecting and establishing inheritance (parent/child relationship) of formulas, strategies and policies within your records and secrets.

The following article will list and define each of the available Records Types in Privileged Access Management.

If you would like to hide Record Types from users, enable the **Hidden** checkbox.

These hidden record types can still be used; however, they will not appear in the **Add Record** dropdown menu.

Record Types can also be configured to allow their use in Personal Vaults. If you would like them to be used in Personal Vaults, check the **Personal Vault** box and if you would not, then uncheck this same box.



Please note that the ability to [create custom record types](#) is only available for System Administrators.

Using Service Administrator's account navigate Administration > *Record Types* and find a list of available records types.

A screenshot of the 'Record Types' page in the Service Administrator interface. The page shows a list of 47 record types. The left sidebar contains navigation links: Service Administrator, Records, Administration (highlighted), Global Permissions, Global Roles, Local Users, Local Groups, Discovery, Scripts, Record Types (highlighted), Tokens, Workflows, Command Control, MFA, Behavior Profiles, Settings, and Updates. The main content area shows the 'Record Types List' with a table of record types. The table has columns: Record Type / Description, Parent Record Type, Session ..., Enabled, Personal ..., Vaults, and Actions. The table lists several record types: AWS Access Keys, WEB Portal, Kubernetes, and Oracle. Each record type has an 'Edit' button next to it. The 'Record Types' link in the sidebar is highlighted with a red box.

There are 47 record types available:

AWSP	Record Type / Description	Parent Record Type	Session Manager	Enabled	Personal Vault	Vaults	Actions
	AWS Access Keys A record with AWS access key id and secret key		AWSP				
HTTP	Record Type / Description	Parent Record Type	Session Manager	Enabled	Personal Vault	Vaults	Actions
	WEB Portal [*deprecated as of 2025] A record with WEB Portal information		HTTP	Y	Y		
Kubernetes	Record Type / Description	Parent Record Type	Session Manager	Enabled	Personal Vault	Vaults	Actions
	Kubernetes A record to connect to Kubernetes console of a container		Kubernetes				
ORAP	Record Type / Description	Parent Record Type	Session Manager	Enabled	Personal Vault	Vaults	Actions
	Oracle A record with Oracle DB information		ORAP				
Other	Record Type / Description	Parent Record Type	Session Manager	Enabled	Personal Vault	Vaults	Actions

	Active Directory User An Active Directory User Record			Y	Y		
	AD Query A record for Active Directory queries to execute tasks on mass for multiple computers stored in Active Directory	Active Directory User Record					
	AWS STS Temporary Access AWS STS Temporary Keys Generator						
	Certificate A record with a certificate, a private or a public key			Y			
	Informix A record with Informix DB information						
	LDAP Server LDAP Server						
	LDAP User LDAP User						



	Microsoft Entra ID A record with Entra ID credentials (formerly Azure Active Directory)						
	MS SQL Server A record with MS SQL Server information						
	MySQL A record with MySQL DB information						
	PostgreSQL PostgreSQL Database						
	Secret A record with a secret sentence			Y	Y		
	Virtual SMS MFA Virtual SMS MFA						
	Virtual TOTP MFA Virtual TOTP Application						
<b>RDP</b>	<b>Record Type / Description</b>	<b>Parent Record Type</b>	<b>Session Manager</b>	<b>Enabled</b>	<b>Personal Vault</b>	<b>Vaults</b>	<b>Actions</b>

	Remote App Host A record with Remote Application Host configuration		RDP				
	Windows Host RDP Windows Host A record with Windows Host Information		RDP				
	Windows Host Ephemeral Account Windows Host Ephemeral Account		RDP				
<b>RemoteApp</b>	<b>Record Type / Description</b>	<b>Parent Record Type</b>	<b>Session Manager</b>	<b>Enabled</b>	<b>Personal Vault</b>	<b>Vaults</b>	<b>Actions</b>
	Google Chrome A record with Google Chrome Remote Application information		RemoteApp				
	Internet Explorer [*deprecated as of 2025] A record with Internet Explorer Remote Application information		RemoteApp				

	MS SQL Studio A record with MS SQL Studio Remote Application information		RemoteApp				
	MySQL Workbench A record with MySQL Workbench Remote Application information		RemoteApp				
	EAM (formerly OneSign) Admin Console A record with EAM (formerly OneSign) Admin Console Remote Application information		RemoteApp				
	EAM (formerly OneSign) Appliance Console A record with EAM (formerly OneSign) Appliance Console Remote Application information		RemoteApp				

	Oracle SQL Developer A record with Oracle SQL Developer Remote Application information		RemoteApp				
	PC5250 A record with PC5250 Terminal Remote Application information		RemoteApp				
	PuTTY A record with PuTTY Remote Application information		RemoteApp				
	Remote Desktop Connection A record with Remote Desktop Connection Remote Application information		RemoteApp				
	Toad Oracle A record with Toad Oracle Remote Application information		RemoteApp				
SSH	<b>Record Type / Description</b>	<b>Parent Record Type</b>	<b>Session Manager</b>	<b>Enabled</b>	<b>Personal Vault</b>	<b>Vaults</b>	<b>Actions</b>

	Cisco A record with Cisco Host information	Unix Host	SSH				
	Juniper A record with Juniper Host information	Unix Host	SSH				
	Linux Host Ephemeral Account Linux Host Ephemeral Account		SSH				
	Linux Host Ephemeral Account with Key Linux host ephemeral account authentication using private key		SSH				
	Palo Alto Networks A record with Palo Alto Networks Host information	Unix Host	SSH				
	Unix Host A record with Unix host information		SSH	Y	Y		

	Unix Host with Key A record with a Unix host accessed with a private key		SSH	Y			
	Unix Host with Private Key Unix Host with Private Key as a Field		SSH				
	Unix Host with Protected Key A record with a Unix host accessed with a protected private key		SSH	Y			
	Unix Host with Reconcile Account Unix Host with reconcile account on record to manage the primary account		SSH				
SSH_EXEC	<b>Record Type / Description</b>	<b>Parent Record Type</b>	<b>Session Manager</b>	<b>Enabled</b>	<b>Personal Vault</b>	<b>Vaults</b>	<b>Actions</b>
	Unix Host Command A record with exec command over ssh support	Unix Host	SSH_EXEC				
SSH_SU	<b>Record Type / Description</b>	<b>Parent Record Type</b>	<b>Session Manager</b>	<b>Enabled</b>	<b>Personal Vault</b>	<b>Vaults</b>	<b>Actions</b>

	Unix Host with SU A record with Unix host information including SU	Unix Host	SSH/SU	Y	Y		
<b>Telnet</b>	<b>Record Type / Description</b>	<b>Parent Record Type</b>	<b>Session Manager</b>	<b>Enabled</b>	<b>Personal Vault</b>	<b>Vaults</b>	<b>Actions</b>
	AS400 A record with AS400 connection information		Telnet				
	Telnet Host A record with Telnet host information		Telnet				
<b>VNC</b>	<b>Record Type / Description</b>	<b>Parent Record Type</b>	<b>Session Manager</b>	<b>Enabled</b>	<b>Personal Vault</b>	<b>Vaults</b>	<b>Actions</b>
	VNC Host A record with VNC host information		VNC	Y			

In the following list, each of the out of the box Record Type section includes:

- **Sample Record Type Name**

- A description of the main use for this type when creating records.
- Can this record type be used for establish remote sessions and/or execute strategies.
- A list of the default fields includes with this record type.
  - Field Name: [field type] Description of the field.
  - Field Name: [field type:secured] Secured field means that its content is masked and can only be unmasked by clicking the Unlock button. For more information about Secured fields and Unlocking, please read this blog post.

## • Active Directory

- Used to store an AD/LDAP account or any account that requires a username and password combination. Ideal use for [reference records](#).
- Cannot be used to establish a remote session, but can be associated with Password Reset tasks.
- **Record Fields**
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.

## • AD Query

- Used for [Active Directory queries](#) to execute tasks on mass for multiple computers stored in Active Directory.
- Cannot be used to establish a remote session, but can be associated with Password Reset and other tasks.
- **Record Fields**
  - User: [string] The user name to be used when executing tasks. A Domain Administrator account is recommended.
  - Password: [string:secured] The password associated to the user in this record.
  - AD Query: [string] The Active Directory query that will be executed of which the results will be used as Host(s) for each task execution.

## • AS400

- Used to establish a SSH connection to an AS400 host for access that requires a username and password.
- Can be used to establish a remote session and be associated with Password Reset tasks.
- **Record Fields**
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - Port: [number] The port number required for this connection.
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.

## • Certificate

- Used to store a certificate file so that it can be shared between users and teams while maintaining a “source of truth” with auditing events.
- Cannot be used to establish a remote session.
- **Record Fields**
  - Cert: [file:secured] The certificate file to be stored and used in this record.



## Cisco

- Used to establish a connection to a [Cisco](#) device for SSH access that requires a username and password. This can optionally be configured to automatically switch to Enable mode using the supplied password.
- Can be used to establish a remote session and be associated with Password Reset and custom tasks.
- **Record Fields**
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - Port: [number] The port number required for this connection.
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.
  - Enable Password: [string:secured] (optional) The password that will be automatically entered in order to switch to Enable mode.
  - Enable Level: [string:secured] (optional) The Enable level, blank defaults to level 15.

## Google Chrome

- Used with Google Chrome Remote Application information in order to launch the Google Chrome Web Browser [native remote application](#) and provide URL and login parameters to a web site.
- Can only be used to establish a remote session using the native application.
- **Record Fields**
  - URL: [string] The URL to be used to launch the web site.
  - User: [string] The user name to be used when logging in to the web site in the native remote application.
  - Password: [string:secured] The password associated to the user in this record.

## Informix

- Used to establish a connection to a Informix database. Useful to executing strategies (scripts) against the connected database and to reset database passwords.
- Cannot be used to establish a remote session, but can be associated with Password Reset and custom tasks.
- **Record Fields**
  - Connection: [string] The connection string to be used with this record. Use this formatting when entering this value: jdbc:informix-sqli://<HOST>:<PORT>/<DATABASE>:INFORMIXSERVER=<SERVER>; For example: jdbc:informix-sqli://123.45.67.89:1526/testDB:INFORMIXSERVER=myserver;
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.

## Internet Explorer [Deprecated]

- Used with Internet Explorer Remote Application information in order to launch the Internet Explorer Web Browser [native remote application](#) and provide URL and login parameters to a web site.
- Can only be used to establish a remote session using the native application.
- **Record Fields**
  - URL: [string] The URL to be used to launch the web site.
  - User: [string] The user name to be used when logging in to the web site in the native remote application.
  - Password: [string:secured] The password associated to the user in this record.

## Juniper

- Used to establish a connection to a [Juniper](#) device for SSH access that requires a username and password.
- Can be used to establish a remote session and be associated with Password Reset and custom tasks.
- **Record Fields**
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - Port: [number] The port number required for this connection.
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.

## MS SQL Server

- Used to establish a connection to a Microsoft SQL database. Useful to executing strategies (scripts) against the connected database and to reset database passwords like 'sa'.
- Cannot be used to establish a remote session, but can be associated with Password Reset and custom tasks.
- **Record Fields**
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - Port: [number] The port number required for this connection.
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.

## MS SQL Studio

- Used with MS SQL Studio Remote Application information in order to launch the MS SQL Server Management Studio native remote application and provide connection parameters.
- Can only be used to establish a remote session using the native application.

- **Record Fields**
  - Host: [string] The server name to be used when logging in to the native remote application.
  - User: [string] The user name to be used when logging in to the native remote application.
  - Password: [string:secured] The password associated to the user in this record.

## MySQL Workbench

- Used with MySQL Workbench Remote Application information in order to launch the MySQL Workbench native remote application and provide connection parameters.
  - Can only be used to establish a remote session using the native application.
- **Record Fields**
  - Stored Connection: [string] The name of the MySQL Workbench Stored Connection that should be used for connection. Please note that a Stored Connection in MySQL Workbench is required and needs to be accessible by the user account specified in the Remote App Host record.
  - Password: [string:secured] The password associated to the account saved in the selected Stored Connection.

## Oracle

- Used to establish a connection to an Oracle database. Useful to executing strategies (scripts) against the connected database and to reset database passwords.
  - Cannot be used to establish a remote session, but can be associated with Password Reset and custom tasks.
- **Record Fields**
  - Host: [string] The connection string needed to connect to the database. This may require port number, SID and other such values.
  - User: [string] The user name to be used when establishing the connection.
  - Password: [string:secured] The password associated to the user in this record.

## PostgreSQL

- Used to establish a connection to an PostgreSQL database. Useful to executing strategies (scripts) against the connected database and to reset database passwords.
  - Cannot be used to establish a remote session, but can be associated with Password Reset and custom tasks.
- **Record Fields**
  - Host (Connection String): [string] The connection string needed to connect to the database given by host:port/database, host/database, host[:port]/database or full JDBC connection string jdbc.postgresql://host[:port]/database
  - User: [string] The user name to be used when establishing the connection.
  - Password: [string:secured] The password associated to the user in this record.

## • Palo Alto Networks

- Used to establish a connection to a Palo Alto Networks device for SSH access that requires a username and password.
- Can be used to establish a remote session and be associated with Password Reset and custom tasks.
- **Record Fields**
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - Port: [number] The port number required for this connection.
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.

## • PC5250

- Used with PC5250 Terminal Remote Application information in order to launch the PC5250 Terminal native remote application and provide connection parameters.
- Can only be used to establish a remote session using the native application.
- **Record Fields**
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - Port: [number] The port number required for this connection.
  - User: [string] The user name to be used to authenticate in the remote application.
  - Password: [string:secured] The password associated to the user in this record.

## • PuTTY

- Used with PuTTY Remote Application information in order to launch the PuTTY native remote application and provide connection parameters.
- Can only be used to establish a remote session using the native application.
- **Record Fields**
  - Host: [string] The host name to be used when logging in to the native remote application.
  - Port: [number] The port number to be used when logging in to the native remote application.
  - User: [string] The user name to be used when logging in to the native remote application.
  - Password: [string:secured] The password associated to the user in this record.

## • Remote App Host

- Used to establish a connection to the host that has been configured with Windows RemoteApp functionality.
- Can be used to establish a remote session and be associated with Password Reset and custom tasks.
- **Record Fields**

- Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
- Port: [number] The port number required for this connection.
- User: [string] The user name to be used with this record.
- Password: [string:secured] The password associated to the user in this record.
- Filter: [string] Enter the Record Type of the Remote Apps that can be remotely launched using this host. Multiple record types should be separated with a comma.
- Enabled: [checkbox] Check to Enable this server to act as a RemoteApp host or Uncheck to disable.

## Remote Desktop Connection

- Used with Remote Desktop Connection Remote Application information in order to launch the Remote Desktop Connection native remote application and provide connection parameters.
- Can only be used to establish a remote session using the native application.
- **Record Fields**
  - Host: [string] The host name to be used when logging in to the native remote application.
  - Port: [number] The port number to be used when logging in to the native remote application.
  - User: [string] The user name to be used when logging in to the native remote application.
  - Password: [string:secured] The password associated to the user in this record.

## Secret

- Used to store any generic secret that is text based like combinations or credit and account numbers.
- Cannot be used to establish a remote session.
- **Record Fields**
  - Secret: [string:secured] A text based secret that will be stored with the record.

## Telnet

- Used to establish a connection to a host using the Telnet protocol that requires a username and password.
- Can be used to establish a remote session.
- **Record Fields**
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - Port: [number] The port number required for this connection.
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.

## Toad Oracle

- Used with Toad Remote Application information in order to launch the Toad for Oracle native remote application and provide connection parameters.
  - Can only be used to establish a remote session using the native application.
- **Record Fields**
  - Connection String: [string] The connection string needed to connect to the Oracle database. This may require port number, SID and other such values.
  - User: [string] The user name to be used when logging in to the native remote application.
  - Password: [string:secured] The password associated to the user in this record.

## Unix Host

- Used to establish a connection to a Unix host for terminal access that requires a username and password.
  - Can be used to establish a remote session and be associated with Password Reset and custom tasks.
- **Record Fields**
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - Port: [number] The port number required for this connection.
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.

## Unix Host with Key

- Used to establish a connection to a Unix host for terminal access that requires a username and key file. For more information, read our blog post and watch our How To Video.
  - Can be used to establish a remote session and be associated with Password Reset and custom tasks.
- **Record Fields**
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - Port: [number] The port number required for this connection.
  - User: [string] The user name to be used with this record.
  - Cert: [file:secured] The certificate file to be stored and used in this record. If you want to save the body of the key file, then use the Record Type Unix Host with Private Key instead.

## Unix Host with Private Key

- Used to establish a connection to a Unix host for terminal access that requires a username and key file.
  - Can be used to establish a remote session and be associated with Password Reset and custom tasks.
- **Record Fields**

- **Host:** [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
- **Port:** [number] The port number required for this connection.
- **User:** [string] The user name to be used with this record.
- **Private Key:** [text:secured] Paste the body of the private key file into this field. If you want to save the actual key file, then use the Record Type Unix Host with Key instead.

## • Unix Host with Protected Key

- Used to establish a connection to a Unix host for terminal access that requires a username, key file and passphrase.
  - Can be used to establish a remote session and be associated with Password Reset and custom tasks.
- **Record Fields**
  - **Host:** [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - **Port:** [number] The port number required for this connection.
  - **User:** [string] The user name to be used with this record.
  - **Cert:** [file:secured] The certificate file to be stored and used in this record.
  - **Passphrase:** [string:secured] The passphrase required to establish the connection.

## • Unix Host with SU

- Used to establish a connection to a Unix host for terminal access that would, upon connection, automatically SU (switch user) to a second account. For more information, read our blog post and watch our How To Video.
  - Can be used to establish a remote session and be associated with Password Reset and custom tasks.
- **Record Fields**
  - **Host:** [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - **Port:** [number] The port number required for this connection.
  - **User:** [string] The user name to be used with this record.
  - **Password:** [string:secured] The password associated to the user in this record.
  - **SU User:** [string] The switch user to be used with this record.
  - **SU Password:** [string:secured] The password associated to the switch user in this record.

## • VNC Host

- Used to establish a VNC connection to a host computer. Optionally, a password can be added if one is required.
  - Can be used to establish a remote session.
- **Record Fields**

- Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
- Port: [number] The port number required for this connection.
- Password: [string:secured] Optionally, the configured password required to open this VNC session.

## • WEB Portal[Deprecated]

- Used to store any web portal URL and its accompanying username and password. Useful is sharing remote web login credentials with outside team members. Please note this record type is required if using the [Access Manager Browser Extension](#).
- Cannot be used to establish a remote session.
- **Record Fields**
  - Url: [string] The URL to a web page login or signin page.
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.

## Windows Host

- Used to establish a Remote Desktop connection to a Windows computer. For more information, read our blog post and watch our How To Video.
  - Can be used to establish a remote session and be associated with Password Reset and custom tasks.
- **Record Fields**
  - Host: [string] The host name to be used with this record. The name may be an IP address, computer name, FQDN or something else.
  - Port: [number] The port number required for this connection.
  - User: [string] The user name to be used with this record.
  - Password: [string:secured] The password associated to the user in this record.

The *Internet Explorer* and the *Web Portal* record types are deprecated. Consider migrating to other supported record types. These record types are unavailable for new configurations and will be removed in a future release.

## Creating Custom Record Types

Privileged Access Management provides a variety of [out of the box Record Types](#) to assist in creating, organizing, connecting and establishing inheritance (parent/child relationship) within your records and secrets, but we understand that not every configuration of Access Manager is the same nor are its uses.

For this reason, the system supports the ability to create new custom record types so that Privileged Access Management can meet your specific requirements and scenarios.

The following article describes the process of creating your own Record Types.



1. Login to the System using a System Administrator account. Only System Administrators can create new record types.
2. Navigate to Administration > Record Types and click the button **New Record Type**.
3. Enter a **Name** for the new Record Type (*required*) and a **Description** (*optional*).
4. If this Record Type will be used to create remote sessions, then select the protocol that will be used from the **Session Manager** dropdown. If it won't be used for remote sessions, you may leave this selection empty or blank.
5. If you want to inherit fields from an existing **Record Type**, then select that record type from the **Parent Type** dropdown. If you want to make this new record type unique (meaning it will not inherit any fields), then you may leave this selection empty or blank.
6. If you would like to hide this (or any) Record Type from the Add Record dropdown menu, enable or check the **Hidden box**. Please note that hidden Record Types can still be used, this option will simply hide it on these dropdown menus.
7. If you would like to hide this (or any) Record Type from the Add Record dropdown menu in Personal Vaults, disable or uncheck the **Personal Vault** box. Enable or check this box to show and allow this Record Type to be used in Personal Vaults.

Record Type: Contoso

Found fields.

Save

Name

Contoso

Description

Our custom Windows Host record type

Session Manager

RDP

Parent Type

Windows Host

Hidden

☐

8. Click the **Save** button when finished.
9. Once the new base Record Type is saved, you may now add custom Fields to it. Click the **Add Field** button to begin.
10. In the **Field Type** menu, select the type from the dropdown.

For a description of each available field type, please review [this](#) page.

11. Enter a value in the **Name** field. This will be the field's internal name.
12. Enter a value in the **Display Name** field. This will be the field's name in the System interface and the one users will populate. Make sure it is something that will be recognizable and understood by your users.
13. If the field should be secured, meaning it will be concealed by default and have the Unlock option, check the **Secured** box.

14. Enter a numeric value into the **Order** parameter. This will determine the display order of the fields in the System interface.
15. Optionally, you may enter placeholder text into the **Helper** field that will be displayed in the System interface.

Record Type: Contoso extending [Windows Host](#)

Edit Field: departmentid

[Save](#) [Cancel](#)

Field Type	String ▼
Name	departmentid
Display Name	Department ID
Secured	<input type="checkbox"/>
Order	500
Helper	Enter your department ID here.

16. Click the **Save** button when finished.

Your new record type and a new field have now been created.

You may continue to create additional custom fields for this type or you can navigate to the All Records section and begin testing it.

New Record Types will automatically appear in the Record Type dropdown menu and will be immediately available for use.

[Add Folder](#) [Add Record ▼](#) [Import](#) [🔔](#)

- Active Directory
- AS400
- Azure
- Certificate
- Contoso**

## Available Fields for Additional Functionality

Custom Fields Added to Record Types for Enhanced Functionality.

This article lists all the custom fields that can be added to specific Record Types to enable additional functionality in PAM.

Note that these fields cannot be used with all record types, so please be sure to read the description of each before adding them to your PAM instance.

Please see our [Creating New Fields](#) for information about how to create fields in [PAM record types](#).

## AD Query

- Description: Used to define a standard LDAP query against the host in order to execute tasks against the query results. More information can be found in our [Host Queries for Mass Script Execution](#) article.
- Field Type: **String**
- Name: **ADQuery**
- Display Name: **AD Query**
- Example: **(&(objectclass=computer)(objectcategory=computer)(cn=DEV\*))**

## Agent Forwarding (SSH)

- Description: Can be added to *Unix Host with Key*, *Unix Host with Private Key* or inherited record types to enable connecting to the destination server through one or more bastion hosts using the same set of public and private key pair managed in the system vault.
- Field Type: **Checkbox**
- Name: **AgentForwarding**
- Display Name: **Agent Forwarding**
- Example: **Enabled/Checked** to enable SSH Agent Forwarding on this record.

## Allowed Hosts

- Description: Allowed Hosts field used with the comma-separated list of white-listed hosts or *host:port* combinations. The field white lists Forward [SSH Tunnel](#) destinations for SSH records restricting access outside of the white listed hosts. The field also white lists [HTTP Proxy](#) destination to inject credentials for [SSO](#)-based WEB Portals.
- Field Type: **Text**
- Name: **AllowedHosts**
- Display Name: **Allowed Hosts**

## Allowed Resolved Hosts

- Description: Allowed Resolved Hosts field used with the comma-separated list of white-listed hosts, IPs, or IP-range (from-to or IP/bits) combinations. The field white lists user provided destination when connecting to records defined with empty hosts restricting access to all targets outside of the specified access rules.
- Field Type: **Text**
- Name: **AllowedResolvedHosts**
- Display Name: **Allowed Resolved Hosts**

## Audio

- Description: Default system deployment disables audio for WEB RDP Sessions unless enabled globally using system parameter *xtam.session.web.audio=true*. Record level parameter Audio allows record owners to enable or to disable audio in WEB RDP Sessions for individual records or all records in the record type.
- Field Type: **Choice**
- Name: **Audio**
- Display Name: **Audio**
- Values: **Enabled, Disabled**

## Clipboard Transfer Control

- Description: Used to overwrite the global Session Clipboard Transfer parameter (Administration > Settings > Parameters > Session Clipboard Transfer) on individual records.
- Field Type: **Choice**
- Name: **ClipboardTransfer**
- Display Name: **Clipboard Transfer Control**
- Values: **Use Global, Enabled, Disabled**
- Example: **Use Global or no selection** to use the globally defined configuration for sessions connected with this record, **Enabled** to overwrite the globally defined configuration and allow Clipboard Transfers for sessions connected with this record or **Disabled** to overwrite the globally defined configuration and disallow Clipboard Transfers for sessions connected with this record.

## Command

- Description: Can be added to a SSH based record type to execute a specific command upon login. Used in conjunction with the Command Password field to authenticate the command. More information can be found in our [Automatic Command Execution During SSH Login](#) article.
- Field Type: **String**
- Name: **Command**
- Display Name: **Remote Command**
- Example: **mysql -u admin -p -h 10.0.0.33 Master** to connect using the MySQL client.

## Command Password

- Description: If the Command field above requires a password, enter this password to authorize that command.
- Field Type: **String**
- Name: **CommandPassword**
- Display Name: **Command Password**
- Secured: **Enabled/Checked**
- Example: The password for *-u admin* in the previous Command field.

## Connection

- Description: Used to define a complete connection string for Oracle RDBMS connections.
- Field Type: **String**
- Name: **Connection**
- Display Name: **Connection**
- Example: **host:1521:SID**

## Console

- Description: Used to connect to the RDP console session (Windows Server 2003) in case a record has the Console field set to true (checked)
- Field Type: **Checkbox**
- Name: **Console**
- Display Name: **Console**
- Example: **Enabled/Checked** to connect to the RDP console session.

## Enable Level

- Description: Used to define the *Enable* level when switching to [Cisco's Enable mode](#) after login.
- Field Type: **Number**
- Name: **EnableLevel**
- Display Name: **Enable Level**
- Example: **15**

## Enable Password

- Description: Used to define the *Enable* password when switching to [Cisco's Enable mode](#) after login.
- Field Type: **String**
- Name: **EnablePassword**
- Display Name: **Enable Password**
- Secured: **Enabled/Checked**
- Example: **yourPassword**

## Enabled

- Description: Used to define which Remote Application Host record is enabled for operations.
- Field Type: **Checkbox**
- Name: **Enabled**
- Display Name: **Enabled**
- Example: **Enabled/Checked** to enable for operations, **Disable/Unchecked** to disable for operations.

## Enable WinRM SSL

- Description: Used to enable SSL connection for WinRM script execution on Windows computers.
- Field Type: **Checkbox**
- Name: **EnabledSSL**
- Display Name: **Enabled SSL**
- Example: Checked to enable, Uncheck to disable

## Exclusive Session

- Description: Used to designate certain records for exclusive access instead of enforcing exclusive access globally.
- Field Type: **Choice**
- Name: **ExclusiveSession**
- Display Name: **Exclusive Session**
- Example: **Enabled/Disabled, Use Global**

## File Transfer Control

- Description: Used to overwrite the global Session File Transfer parameter (Administration > Settings > Parameters > Session File Transfer) on individual records.
- Field Type: **Choice**
- Name: **FileTransfer**
- Display Name: **File Transfer Control**
- Values: **Use Global, Enabled, Disabled**
- Example: **Use Global** or no selection to use the globally defined configuration for sessions connected with this record, **Enabled** to overwrite the globally defined configuration and allow File Transfers for sessions connected with this record or **Disabled** to overwrite the globally defined configuration and disallow File Transfers for sessions connected with this record.

## File Transfer Disabled

- Description: Used to disable a request for the file transfer protocol (SFTP) during Unix sessions.
- Field Type: **Checkbox**
- Name: **FileTransferDisabled**
- Display Name: **File Transfer Disabled**
- Example: **Enabled/Checked** to disable request for SFTP.

## Filter

- Description: Used to define a comma-separated list of record types served by the specific Remote Application Host record.
- Field Type: **String**
- Name: **Filter**

- Display Name: **Filter**
- Example: **MySQL Workbench**, **MS SQL Studio** to enable only these record types to operate with this Remote Application Host.

## Font Smoothing

- Description: Used, on a record level, to enable nice font rendering during Windows connections at the expense of the increased network traffic. Font Smoothing can also be enabled on a global or user preference level, but this configuration will take precedence over those settings.
- Field Type: **Choice**
- Name: **FontSmoothing**
- Display Name: **Font Smoothing**
- Values: **enabled**, **disabled**
- Example: **enabled** to force font smoothing, **disabled** to allow for the global or user preference setting to be used.

## Glyph Caching

- Description: In addition to screen regions, RDP maintains caches of frequently used symbols or fonts, collectively known as "*glyphs*." Certain known bugs in RDP implementations can cause performance issues with this enabled (old versions such as Windows Server 2008 is a usual example). Setting this parameter to *Disabled* will disable that glyph caching in the WEB RDP session for this record.
- Field Type: **Choice**
- Name: **GlyphCaching**
- Display Name: **Glyph Caching**
- Values: **Enabled**, **Disabled**

## Host Name DNS

- Description: Used to verify a remote Windows host name match with the host name on the record before executing any script on the remote computer in order to detect mis-configured or attacked name resolution service. Checking the field disables the option to verify host for the specific record.
- Field Type: **Checkbox**
- Name: **HostNameDNS**
- Display Name: **Host Name DNS**
- Example: **Unchecked** to enable, **Checked** to disable.

## Hosts

- Description: Hosts field used with the comma-separated list of white-listed hosts or **host:port** combinations. When the list of allowed hosts is defined for the record, **Connect** action prompts for the host selection to resolve the host to connect with the credentials on record. The option facilitates an account-centric approach to manage domain accounts shared among multiple destination endpoints.
- Field Type: **Text**

- Name: **Hosts**
- Display Name: **Hosts**

## Key Size

- Description: Used to specify the size of the key generated for Unix public key rotation.
- Field Type: **Choice**
- Name: **KeySize**
- Display Name: **Key Size**
- Values: **1024, 2048, 4096, 8192**
- Example: **4096**

## Minimum Password Age

- Description: Used to define Minimum Password Age in days to make the system to shift scheduled date of Password Reset job when it is executed before endpoint system allows to change the password. Note that this field still allows execution of the password set job using shadow account to force rotate the password.
- Field Type: **Number**
- Name: **MinPasswordAge**
- Display Name: **Minimum Password Age**

## Override Session Manager

- Description: Used with the value `orap://session-manager-host:port` to override default session manager detected from the proximity groups configuration. For example, use the value `orap://localhost:4822` to indicate local session manager should be used when connecting to this record using Oracle SQL Proxy protocol but still use default proximity groups configuration for other protocols.
- Field Type: **String**
- Name: **OverrideSessionManager**
- Display Name: **Override Session Manager**
- Values: **`orap://session-manager-host:port`**

## Password Attribute

- Description: Used to a configure custom password attribute to support password reset for non-OpenLDAP compliant user directories. Use this custom field PasswordAttribute in a LDAP Server record type to define the LDAP password attribute relevant to this specific user directory server. More information can be found in our [OpenLDAP Automated Password Reset](#) article.
- Field Type: **String**
- Name: **PasswordAttribute**
- Display Name: **Password Attribute**
- Example: Your non-OpenLDAP password attribute value other than the expected *userPassword*



## Platform

- Description: Used to define the Remote Application Host platform; Windows RDS or TSPlus.
- Field Type: **Choice**
- Name: **Platform**
- Display Name: **Platform**
- Values: **Windows RDS, TSPlus**
- Example: **Windows RDS**

## Prologue

- Description: Used to send a sequence into the remote device at the start of the connection.  
Optionally, use the following placeholders in the Prologue field to pass session metadata to the endpoint servers:
  - {USER}** - User on record
  - {PASSWORD}** - Password on record
  - {LOGIN}** - Current system user accessing the endpoint server through the session
  - {SESSION}** - Artificial Connection ID to correlate with the system Sessions report
  - {VNCPASSWORD}** - VNC password if **{PASSWORD}** is used to unlock screen saver in VNC sessions
- Field Type: **String**
- Name: **Prologue**
- Display Name: **Prologue**
- Example: **dbaccess life** to execute this command to access an Informix database immediately after a successful connection.

## Remote App

- Description: Used to name of the remote application to start on the remote RDS Server.
- Field Type: **String**
- Name: **RemoteApp**
- Display Name: **Remote App**

## Remote App Arguments

- Description: Used to name optional parameters of the remote application provided by Remote field.
- Field Type: **String**
- Name: **RemoteAppArgs**
- Display Name: **Remote App Arguments**

## Remote App Directory

- Description: Used to initial folder to launch remote application provided by RemoteApp field.
- Field Type: **String**

- Name: **RemoteAppDir**
- Display Name: **Remote App Directory**

## Resize On Connect Delay

- Description: Used to disable a screen resize and keeps the initial default screen size.
- Field Type: **String**
- Name: **ResizeOnConnectDelay**
- Display Name: **Resize On Connect Delay**
- Example: **-1** to disable the resize.

## Screen Size

- Description: Used to control the screen size for SSH and Telnet sessions target blocked graphical applications on the remote Unix systems that require fixed screen size for their optimal performance. It defines the target screen resolution and is provided in the format WIDTHxHEIGHT in pixels for sizes larger than 320x200 or in COLSxROWS in characters for the sizes smaller than 320x200.
- Field Type: **String**
- Name: **ScreenSize**
- Display Name: **Screen Size**
- Example: **1024x768** in pixels or **80x24** in characters.

## Self Check Status

- Description: Used to enable the Check Status task to validate the record credentials when the task is configured with a Shadow Account. When enabled, Check Status will validate the record credentials when a Shadow Account is present, but it does require that these record credentials have permission on the host to execute the script.
- Field Type: **Checkbox**
- Name: **SelfCheckStatus**
- Display Name: **Self Check Status**
- Example: **Checked to enable, Uncheck to disable**

## Service

- Description: Service or SID name for Oracle RDBMS connections used in combination with Host and Port to build a connection string. Service parameter not started with / or : is treated as a service. Service parameter may start with / to be treated as a service. Service parameter may start with : to be treated as an SID.
- Field Type: **String**
- Name: **Service**
- Display Name: **Service**
- Example: **xtam**

## Service Port

- Description: This parameter defines a custom port for password reset and job execution for the Windows Remote PowerShell strategy using WinRM protocol by specifying the port number in the record type. Default port value is 5985.
- Field Type: **Number**
- Name: **ServicePort**
- Display Name: **Service Port**
- Example: **1234**

## SFTP

- Description: Defines the protocol type to transfer files to and from the WEB RDP session. The default method to transfer files is to use the RDP Drive Redirection feature of the RDP protocol. With the SFTP field enabled, the WEB RDP session uses SFTP protocol to transfer files. The SFTP file transfer will use the same user and password as defined in the record.

Note that for the SFTP option to work the remote server has to have SFTP server deployed and configured.

- Field Type: **Choice**
- Name: **SFTP**
- Display Name: **SFTP**
- Values: **Enabled, Disabled**

## SSH Channels

- Description: Overrides system wide channels configuration available in SSH Proxy using global parameter SSH Proxy Allowed Channels on the record level.  
Supported channels are:  
**shell** - Allow shell connection  
**exec** - Allow remote command execution including scp transfer  
**sftp** - Allow file transfer using SFTP protocol  
**tunnel** - Allow SSH tunnels over SSH Proxy  
There are two scenarios to override channel settings:
  1. List channels allowed for current record. This will allow only shell and exec channels to open: shell, exec
  2. Use system defaults but add or remove specific channel. This will use setting from system parameter but allow sftp and deny tunnel channels.
- Field Type: **String**
- Name: **SshChannels**
- Display Name: **SSH Channels**
- Example: **+sftp,-tunnel**

## SSH Connector Type

- Description: Used to overwrite global SSH Connector Type parameter to allow to switch between default (Jsch Connector) and extended (SSHD Connector) provider to execute all SSH and Interactive SSH jobs in the system. SSHD Connector provider includes extended cryptography algorithms to support job execution on a different set of devices.
- Field Type: **Choice**
- Name: **SSHConnectorType**
- Display Name: **SSH Connector Type**
- Values: **Jsch Connector, SSHD Connector**

## Telnet Login Prompt Detection Regular Expression

- Description: Used to customize login prompt expected during Telnet authentication. Telnet protocol does not specify authentication procedure. While PAM support many typical authentication procedures, there is an option to customize expected login and password prompts for untypical implementations using UserRegex and PasswordRegex fields.
- Field Type: **String**
- Name: **UserRegex**
- Display Name: **User Regex**
- Example: **(.\*)username\$**

## Telnet Password Prompt Detection Regular Expression

- Description: Used to customize password prompt expected during Telnet authentication. Telnet protocol does not specify authentication procedure. While PAM support many typical authentication procedures, there is an option to customize expected login and password prompts for untypical implementations using UserRegex and PasswordRegex fields.
- Field Type: **String**
- Name: **PasswordRegex**
- Display Name: **Password Regex**
- Example: **(.\*)secret(.\*)**

## Terminal

- Description: This parameter sets the terminal emulator type string that is passed to the SSH server. This parameter is optional and if not specified, "linux" is used as the terminal emulator type by default. Examples of terminal strings include VT52, VT100, VT220, VT320, xterm and ANSI.
- Field Type: **String** or **Choice**
- Name: **Terminal**
- Display Name: **Terminal**
- Values: enter a list of terminal emulator strings that can be selected by record creator or editors.
- Example: **VT100**

## Traffic Interceptor Hints

- Description: Used to define a non-standard port(s) for use with capturing SQL traffic when an PAM SSH Tunnel is being used. The hint is a comma-, space- or semicolon-separated list of protocols and ports that should be recorded.
- Field Type: **String**
- Name: **TrafficInterceptorHints** or **TrafficInterceptorHints**
- Display Name: **Traffic Interceptor Hints** or **Traffic Interceptor Hints**
- Example: **mssql:1444 mysql:3333**

## Transport Security

- Description: Used to select a specific transport security level for RDP connections.
- Field Type: **Choice**
- Name: **TransportSecurity**
- Display Name: **Transport Security**
- Values: **rdp, nla, tls, any**
- Example: Select **tls** from the Transport Security dropdown menu to establish the RDP connection using tls.

## Trust WinRM Server certificate

- Description: Disable check of remote WinRM server certificate when executing PowerShell scripts over secure channel using EnableSSL option
- Field Type: **Checkbox**
- Name: **TrustCertificate**
- Display Name: **Trust Certificate**
- Example: Checked to enable, Uncheck to disable

## Trust WinRM Server host

- Description: Disable check of remote WinRM server host match when executing PowerShell scripts over secure channel using EnableSSL option
- Field Type: **Checkbox**
- Name: **TrustHost**
- Display Name: **Trust Host**
- Example: Checked to enable, Uncheck to disable

## VNC Password

- Description: Used to define a VNC Host password to enable referencing an unlock user password or the OS user from the other record. PAM is able to unlock the user session using the account password on the record to present high trust login to the actual user desktop through the VNC protocol
- Field Type: **String**
- Name: **VNCPassword**

- Display Name: **VNC Password**
- Secured: **Enabled/Checked**
- Example: **yourVNCpassword**

## Windows Theme (RDP in-browser sessions)

- Description: Used to define whether the Windows Theme of the destination server will be enabled during in-browser sessions. Windows Theme is disabled by default for performance considerations.
- Field Type: **Choice**
- Name: **Theming**
- Display Name: **Theming**
- Values: **Disabled, Enabled**
- Example: **Enabled**

## Windows Wallpaper (RDP in-browser sessions)

- Description: Used to define whether the Windows Wallpaper of the destination server will be displayed during in-browser sessions. Windows Wallpaper is disabled by default for performance considerations.
- Field Type: **Choice**
- Name: **Wallpaper**
- Display Name: **Wallpaper**
- Values: **Disabled, Enabled**
- Example: **Enabled**

## Record types Security policy report

The option to export record types' policies as a PDF report for audit review.

The report includes record type parameters (session manager, custom script, inheritance, vault visibility), list of fields, password complexity formula as well as task policies for selected or all configured record types.

The report provides insight into default access security configuration for auditors and system owners to review.

# Permissions Roles and Security

## Permissions

Privileged Access Management provides a robust set of permissions that can be granted to users or groups (Principals) in order to control the level of access they have to objects and areas of the software.

Note that permissions in Privileged Access Management are additive, meaning that a higher level of permission includes all the roles of a lesser, and permissions can be inherited via folders.

Below is a list of available permissions and roles in Privileged Access Management.

## Global Roles

Global Roles provide system wide access to Privileged Access Management.

- **Auditor**
  - The Auditor role grants a limited “*View Only*” role to all folders and records in the system. It grants access to the Audit Log (record and system), Session History (record and system), Job History (record and system) as well as Administration Reports. For additional information, please see [What is the Auditor Role](#).
- **System Administrator**
  - The System Administrator role (the highest level available) grants *full access* to all vaults, folders, records, logs, security, script library, workflows, configuration and reports system wide. It can be used to grant and revoke other principals to this System Administrator role and therefore it should only be given to trusted users.

- **Split View**

- The Split View roles grants access to only the first or last part of a split password when the Split View Role is enabled. The Split View Role is configured in the Parameters section of the Administration page.  
[What is Split View?](#)

- **Service**

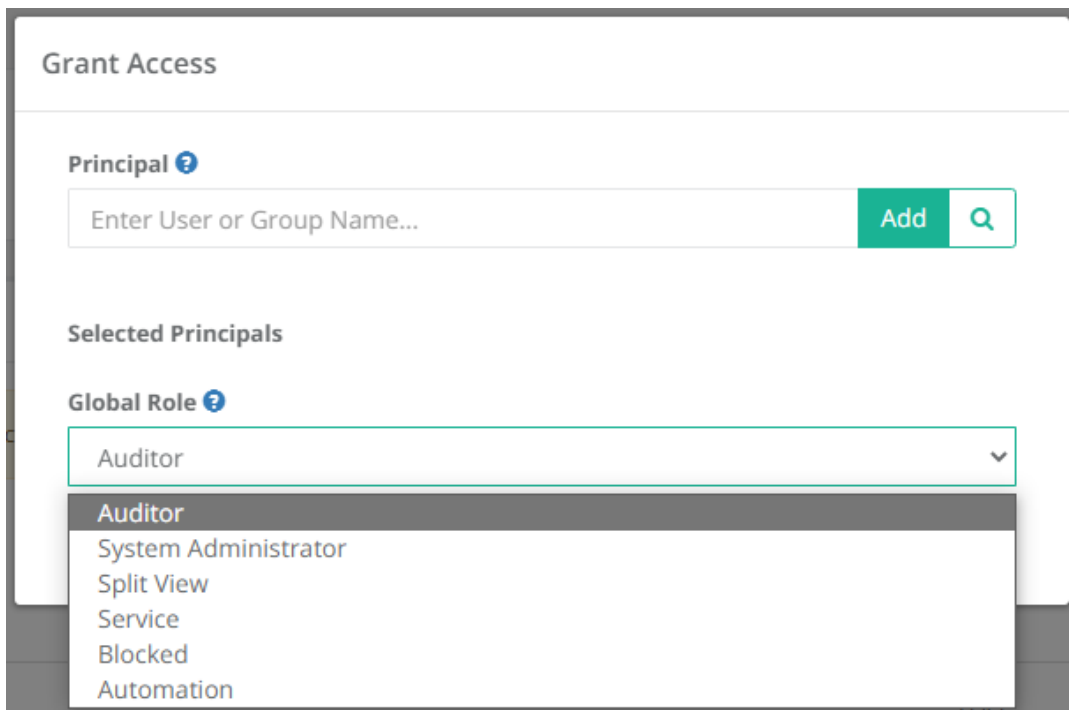
- The Service account is used for a distributed job engine deployment so an Administrator can designate certain records to be executed by specific job engine nodes. Read more about [Distributed Job Engine Deployments](#).

- **Blocked**

- The Blocked role is used to block the user or group members' access to objects in PAM. The blocked user can still login to PAM, but until they are unblocked, they will have no access to any objects or settings. Remove the Blocked role from the principal to restore their access.

- **Automation**

- The Automation account is used to throttle the rate of new connections for scripts to control overall system performance. For additional configuration, read the description and adjust the global parameter *Throttle SSH Proxy Automation Connections* as needed.



The screenshot shows a 'Grant Access' window. At the top, there's a 'Principal' label with a help icon. Below it is a text input field 'Enter User or Group Name...' with an 'Add' button and a search icon. Underneath is a 'Selected Principals' section. The 'Global Role' dropdown is open, showing a list of roles: Auditor, System Administrator, Split View, Service, Blocked, and Automation. The 'Auditor' role is currently selected.

Grant Global Access and Permissions

## Record Control

Record Control provides access to objects (Folders and Records) located in the Records area of System.

- **Viewer**

- The Viewer role grants View Only access to the object.

- **Unlock**

- Viewer plus the ability to Unlock (view) secured fields like Passwords, Secrets and Certificates.



- **Editor**
  - Unlock plus the ability to Edit the object as well as its associated Formula and to view its Session History, Video Recordings and Keystroke and Clipboard Events.
- **Manager**
  - Editor plus the ability to Create or Delete objects (folders and records). Manager cannot create (share) or modify object permissions.
- **Owner**
  - Full Control of the object. This includes creating new objects, modifying or deleting existing objects, sharing access (permissions), workflow configuration, Audit Events, History and Session Termination.

## Session Control

Session Control provides access to connect to Remote Sessions using a record in System.

- **None**
  - The principal may **not** establish a remote session using this record.
- **Connect (Optionally recording without session events)**
  - The principal may establish a remote session using this record and can choose whether their session is video recorded or not. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will not be recorded.
- **Connect (Always recording without session events)**
  - The principal may establish a remote session using this record and their session will always be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will not be recorded.
- **Connect (Optionally recording with session events)**
  - The principal may establish a remote session using this record and can choose whether their session is video recorded or not. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will be recorded.
- **Connect (Always recording with session events)**
  - The principal may establish a remote session using this record and their session will always be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will be recorded.
- **Connect (No Recording with session events)**
  - The principal may establish a remote session using this record and their session will not be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will be recorded.
- **Connect (No Recording without session events)**
  - The principal may establish a remote session using this record and their session will not be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will not be recorded.

## Task Control

Task Control provides access to Tasks associated to Records in System.

- **None**
  - The principal may **not** execute, review or manage tasks.
- **Execute**
  - The principal may execute tasks.

- **Review**
  - The principal may execute or review task results.
- **Manage**
  - The principal may execute or review task results as well as view the task list. To include the ability to *Add/Remove* tasks and edit *Task Policies*, the user should be assigned both *Record Control: Owner* and *Task Control: Manage* permissions.

### Grant Access

**Principal ?**

developers

Add

**Selected Principals**

John Williams ▾

**Record Control ?**

Viewer ▾

**Session Control ?**

Connect (Always Recording) ▾

**Task Control ?**

Review ▾

Cancel

Select

Grant Object Access and Permissions

Permissions for MS SQL Server					
Found 8 records.					
<div>RefreshGrant PermissionRevoke PermissionInherit from Parent</div>					
Principal	Type	Role	Connect	Execute	Actions
<input type="checkbox"/> Jack Baker (baker)	User	Viewer	Connect (Always Recording)	Execute	<div>Edit</div>
<input type="checkbox"/> Chris Kolodziejewski (chrisk)	User	Owner	Connect (Optionally Recording)	Manage	<div>Edit</div>
<input type="checkbox"/> Demo Admin (demo)	User	Owner	Connect (Optionally Recording)	Manage	<div>Edit</div>
<input type="checkbox"/> Developers	Group	Unlock	Connect (Always Recording)	Execute	<div>Edit</div>

## Permission, Roles and Security

The system makes use of extensive permissions, roles and security to maintain control of your records and secrets.

Permissions or access can be granted via inheritance, on individual objects themselves or even globally for all assets.

Granting or sharing access may be done using Users or Groups, labelled throughout Privileged Access Management as *principals*.

### Object Permissions

Objects (folders, vaults and records) permissions provide access to objects located in the system's vault and a user's personal vault.

When granting or sharing permissions to an object, the following roles are available:

#### *Record Control*

Record Control provides the selected principal(s) access to the object.

Viewer	The Viewer roles grants <i>View Only</i> access to the object. If you want a principal to see this object in their Record List or search results, they must have at least this role.
Unlock	Viewer plus the ability to <i>Unlock</i> (view) secured fields like <i>Passwords</i> , <i>Secrets</i> and <i>Certificates</i> .
Editor	<i>Unlock</i> plus the ability to <i>Edit</i> the object as well as its associated Formula and to view its Session History, Video Recordings and Session Events.
Manager	Editor plus the ability to <i>Create</i> or <i>Delete</i> objects (folders and records). Manager cannot create (share) or modify object permissions.
Owner	<i>Full Control</i> of the object. This includes creating new objects, modifying or deleting existing objects, sharing access (permissions), Audit Events, History and Session Termination.

#### *Session Control*

Session Control provides the selected principal(s) access to connect to [Secure Remote Sessions](#) using the record.

None	The principal may not establish a remote session using this record.
Connect (Optionally Recording without Session Events)	The principal may establish a remote session using this record and can choose whether their session is video recorded or not. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will not be recorded.

Connect (Always Recording without Session Events)	The principal may establish a remote session using this record and their session will always be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will not be recorded.
Connect (Optionally Recording with Session Events)	The principal may establish a remote session using this record and can choose whether their session is video recorded or not. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will be recorded.
Connect (Always Recording with Session Events)	The principal may establish a remote session using this record and their session will always be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will be recorded.
Connect (No Recording with Session Events)	The principal may establish a remote session using this record and their session will not be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will be recorded.
Connect (No Recording without Session Events)	The principal may establish a remote session using this record and their session will not be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will not be recorded.

## Task Control

Task Control provides the selected principal(s) access to Tasks associated to the record.

None	The principal may not execute, review or manage tasks or work with them in any manner.
Execute	The principal may execute tasks from the record's <i>Execute</i> menu.
Review	The principal may execute or review task results in the <i>Job History report</i> .
Manage	The principal may execute or review task results as well as view the task list. To include the ability to <i>Add/Remove</i> tasks and edit <i>Task Policies</i> , the user should be assigned both <i>Record Control: Owner</i> and <i>Task Control: Manage</i> permissions.

## Inheritance

Objects use inheritance from their parent container to simplify the management of objects that share or require a common configuration.

For example, all records in the same folder should have the same permissions or workflow bindings applied.

Newly created or pasted records will also inherit this configuration as well.

By default, all records created within the same container will inherit the Password and [Workflow Bindings](#) from the parent container.

Any changes that need to be made to these policies must be done on the parent container and will therefore also be applied to all other records that reside in this same container.

NOTE: While inheritance from parent container to child record is the default configuration, you can also break inheritance on a record and make the above configuration(s) *unique*. Once the settings are unique to a record, they can be updated as required without affecting the container configuration or any other records that continue to inherit from this parent. Additionally, you can also choose to **Inherit from Parent** within the record's configuration page(s) if you wish to return it back to its inherited state with its parent container.

## Global Permissions

*Global Permissions* enables a method to quickly and easily grant users and groups *non-Administrative* permissions to all objects (folders, vaults and records) stored in the system vault.

For example, you may now provide a user with Viewer permissions to all objects, regardless of their current inheritance setting and without having to navigate to each object, by simply granting Global Permission to this principal account.

A few details to note when considering the use of Global Permissions:

- Global Permissions do not override object permissions, meaning if a user is an Owner of an object, Global Permissions cannot be used to reduce their existing permission level.
- Global Permissions are not displayed when viewing the permissions for a specific object; however, they will be displayed when viewing the object's *Access Report*.
- Global Permissions can be assigned to both local System users and external users like Active Directory Users or Groups.
- Global Permissions can only be assigned and managed by System Administrators.

**To grant a principal Global Permissions**, navigate to Administration > Global Permissions and click the **Grant Permission** button. Enter your principal(s), click the **Add** button, select the level of permissions to grant and finally click the **Select** button to complete the process.

**To edit existing Global Permissions**, simply click the **Edit** button for the required principal, make the necessary adjustments and click the **Select** button to finalize the update.

**To remove existing Global Permissions**, check the box next to each principal(s) to select them and then click the **Revoke Permission** button. On the Global Permission page, use the **Access Report** button to generate a list of all user principals that have access to any object throughout the entire system.

## Global Roles

Global Roles provide system wide access using various level of roles, as described below.

### *Auditor*

The Auditor role grants a limited *View Only* role to all containers and records in the system. It grants access to the Audit Log (record and system), Session History (record and system), Job History (record and system) as

well as Administration Reports and read only configuration.

Auditors *cannot* modify the system or records nor can they *unlock*, *execute* or *connect* to any privileged systems or secrets.

## System Administrator

The System Administrator role (the highest level available) grants full access to *all vaults, folders, records, logs, security, script library, workflows, configuration* and *reports* system wide.

It can be used to grant and revoke other principals to this System Administrator role and therefore it should only be given to trusted users.

## Split View

The Split View role grants access to only the first or last part of a split password when the [Split View](#) Role is enabled.

The Split View Role is configured in the Parameters section of the Administration page.

Read more about the [Split View feature](#) in our article.

## Service

The Service account is used for a distributed job engine deployment so an Administrator can designate certain records to be executed by specific job engine nodes. Read more about [Distributed Job Engine Deployments](#) for additional information about this role.

## Blocked

The Blocked role is used to block the user or group members' access to objects in PAM. The blocked user can still login to PAM, but until they are unblocked, they will have no access to any objects or settings. Remove the Blocked role from the principal to restore their access.

## Automation

The Automation account is used to throttle the rate of new connections for scripts to control overall system performance. For additional configuration, read the description and adjust the global parameter *Throttle SSH Proxy Automation Connections* as needed.

# Local Users and Groups

Local users and groups can be created in Access Manager's internal user directory providing a method to quickly create, disable or automatically expire accounts for internal or external resources.

These accounts are independent of any external user directories that you may also integrate with Access Manager (i.e. Active Directory or LDAP).

*Only System Administrators* may create and manage local users and groups on this global level.

## Create a Local User

To create a new local user, navigate to Administration > Local Users and click the **Create** button. Populate the new user form as required.

Login	Enter a unique value that will be used to login to the system.
-------	--

First Name	Enter a first name for this account.
Last Name	Enter a last name for this account.
Mail	Enter an email address for this account.
Expiration	Enter a date and time when this account will be automatically disabled / locked. Leave blank if you do not want to automatically disable / lock this account.
Password	Enter the password for this account. The password must meet the requirements of the <a href="#">Local User Formula</a> .
Repeat Password	Repeat the password for this account.

Click the **Save** button to complete the account creation process.

NOTE: [Local Users](#) can be added to Local Group membership only. Local Users cannot be added to any groups that originate from integrated external user directories like [Active Directory](#).

## Local User Password Formula

The local user password formula allows you to customize the complexity required for setting and resetting local user passwords.

This formula is used for local user passwords only and is separate from all other formulas in the system.

To configure this formula, navigate to Administration > Local Users and click the **Formula** button.

Customize this formula as required and click the **Save** button when complete.

## Managing Local Users

Editing a local user account allows a System Administrator to update the First Name, Last Name, Email, Expiration and Password of any local user account. Click the **Edit** button associated to the Login to edit an account.

Locking a local user prevents this account from logging into the system while Unlocking an account restores the ability to login to the system.

To Lock or Unlock an account, check the box next to the Login(s) and select Bulk Actions > *Lock* or *Unlock* option.

A locked account will display a lock icon (  ) in the *Locked* column.

Deleting a local user removes the account from the system.

Deleted accounts cannot be restored, so we would recommend using the *Lock* option instead of *Delete* if there is a possibility that the account will be needed again in the future.

To delete a local user, click their **Edit** button and then the **Delete** button on their account's edit page.

## Create a Local Group

Local Groups are created and managed within Access Manager's internal user directory and are used to provide group membership capabilities to both Local Users as well as external accounts like Active Directory

Users.

To create a new local group, navigate to Administration > Local Groups and click the **Create** button. Populate the new group form as required.

Name	Enter a unique group name.
Description	Enter a group name description.

Once the group has been created, use the **Add Member** or **Remove Members** buttons to populate the group membership. Alternatively, you can use the **Edit** button to update membership or configuration of existing local groups.

NOTE: [Local Group](#) membership may include both local users and users that originate from your Privileged Access Management integrated [Active Directory](#).

Use the **Delete Group** button to delete the group and use the **Save Group** button to save any changes that have been made to the group.

# Manager Permissions

Privileged Access Management provides a robust set of permissions that can be granted to users or [groups](#) (Principals) in order to control the level of access they have to objects and areas of the software.

Note that permissions in Privileged Access Management are additive, meaning that a higher level of permission includes all the roles of a lesser, and permissions can be [inherited via folders](#).

[Here](#) is a list of available permissions and roles in Privileged Access Management.

# Object Permissions

Objects (folders, vaults and records) permissions provide access to objects located in the system’s vault and a user’s personal vault.

When granting or sharing permissions to an object, the following roles are available.

# Record Control

Record Control provides the selected principal(s) access to the object.

Viewer	The Viewer roles grants <i>View Only</i> access to the object. If you want a principal to see this object in their Record List or search results, they must have at least this role.
Unlock	Viewer plus the ability to <i>Unlock</i> (view) secured fields like Passwords, Secrets and Certificates.
Editor	<i>Unlock</i> plus the ability to <i>Edit</i> the object as well as its associated Formula and to view its Session History, Video Recordings and Session Events.



Manager	Editor plus the ability to <i>Create</i> or <i>Delete</i> objects (folders and records). Manager cannot create (share) or modify object permissions.
Owner	<i>Full Control</i> of the object. This includes creating new objects, modifying or deleting existing objects, sharing access (permissions), Audit Events, History and Session Termination.

## Session Control

Session Control provides the selected principal(s) access to connect to [Secure Remote Sessions](#) using the record.

None	The principal may not establish a remote session using this record.
Connect (Optionally Recording without Session Events)	The principal may establish a remote session using this record and can choose whether their session is video recorded or not. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will not be recorded.
Connect (Always Recording without Session Events)	The principal may establish a remote session using this record and their session will always be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will not be recorded.
Connect (Optionally Recording with Session Events)	The principal may establish a remote session using this record and can choose whether their session is video recorded or not. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will be recorded.
Connect (Always Recording with Session Events)	The principal may establish a remote session using this record and their session will always be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will be recorded.
Connect (No Recording with Session Events)	The principal may establish a remote session using this record and their session will not be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will be recorded.
Connect (No Recording without Session Events)	The principal may establish a remote session using this record and their session will not be video recorded. Session events (keystrokes including SQL traffic over tunnels, clipboard and file transfer) will not be recorded.

## Task Control

Task Control provides the selected principal(s) access to Tasks associated to the record.

None	The principal may not execute, review or manage tasks or work with them in any manner.
Execute	The principal may execute tasks from the record's Execute menu.
Review	The principal may execute or review task results in the Job History report.
Manage	The principal may execute or review task results as well as view the task list. To include the ability to <i>Add/Remove</i> tasks and edit <i>Task Policies</i> , the user should be assigned both <i>Record Control: Owner</i> and <i>Task Control: Manage</i> permissions.

## Inheritance

Objects use inheritance from their parent container to simplify the management of objects that share or require a common configuration.

For example, all records in the same folder should have the same permissions or workflow bindings applied. Newly created or pasted records will also inherit this configuration as well.

By default, all records created within the same container will inherit the Password and Workflow Bindings from the parent container.

Any changes that need to be made to these policies must be done on the parent container and will therefore also be applied to all other records that reside in this same container.

NOTE: While inheritance from parent container to child record is the default configuration, you can also break inheritance on a record and make the above configuration(s) *unique*. Once the settings are unique to a record, they can be updated as required without affecting the container configuration or any other records that continue to inherit from this parent.

Additionally, you can also choose to **Inherit from Parent** within the record's configuration page(s) if you wish to return it back to its inherited state with its parent container.

## Global Permissions

Privileged Access Management provides an additional level of permissions called Global Permissions that is available to quickly and easily grant users and groups non-Administrative permissions to all objects (folders, vaults and records) stored in the Record List.

For example, you may now provide a user with Viewer only permissions to all objects, regardless of their current inheritance setting and without having to navigate to each object, by simply granting Global Permissions to this principal account.

A few details to note when considering the use of Global Permissions.

- Global Permissions do not override object permissions, meaning if a user is an Owner of an object, Global Permissions cannot be used to reduce this existing permission level.
- Global Permissions can be assigned to both local and Active Directory Users or Groups.
- Global Permissions are not displayed when viewing the permissions for a specific object; however they will

be displayed when viewing the object's [Access Report](#).

- Global Permissions can only be assigned and managed by PAM System Administrators.

## Assigning Global Permissions

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Global Permissions.
3. Click the **Grant Permission** button.
4. In the **Principal** field, enter the User or Group Name and then click **Add**.
5. Select the permissions that you wish to globally assign to the selected principals using the available drop-down menu options.
6. When complete, click the **Select** button to assign the global permissions.

The Administration section previously named **Permissions** has been removed. This section was used to assign permissions to the Record List's Root Folder and this can now be managed only from the Manage > **Permissions** option available in the Root Folder's top menu.

## Global Permissions

Global Permissions enables a method to quickly and easily grant users and groups *non-Administrative* permissions to all objects (folders, vaults and records) stored in the system vault.

For example, you may now provide a user with Viewer permissions to all objects, regardless of their current inheritance setting and without having to navigate to each object, by simply granting Global Permission to this principal account.

**To grant a principal Global Permissions**, navigate to Administration > Global Permissions and click the **Grant Permission** button. Enter your principal(s), click the **Add** button, select the level of permissions to grant and finally click the **Select** button to complete the process.

**To edit existing Global Permissions**, simply click the **Edit** button for the required principal, make the necessary adjustments and click the **Select** button to finalize the update.

**To remove existing Global Permissions**, check the box next to each principal(s) to select them and then click the **Revoke Permission** button.

On the Global Permission page, use the **Access Report** button to generate a list of all user principals that have access to any object throughout the entire system.

## Global Roles

Global Roles provide system wide access using various level of roles, as described below.

The image shows a 'Grant Access' window. At the top is the title 'Grant Access'. Below it is a section for 'Principal' with a help icon. There is a text input field labeled 'Enter User or Group Name...' and a green 'Add' button with a magnifying glass icon. Below this is a section for 'Selected Principals'. Underneath is a 'Global Role' section with a help icon. A dropdown menu is open, showing the following options: Auditor (highlighted), System Administrator, Split View, Service, Blocked, and Automation.

## Auditor

The Auditor role grants a limited *View Only* role to all containers and records in the system.

It grants access to the *Audit Log* (record and system), *Session History* (record and system), *Job History* (record and system) as well as Administration Reports and read only configuration.

Auditors cannot modify the system or records nor can they unlock, execute or connect to any privileged systems or secrets.

## System Administrator

The System Administrator role (the highest level available) grants full access to all *vaults, folders, records, logs, security, script library, workflows, configuration* and *reports* system wide.

It can be used to grant and revoke other principals to this System Administrator role and therefore it should only be given to trusted users.

## Split View

The Split View role grants access to only the first or last part of a split password when the Split View Role is enabled.

The Split View Role is configured in the Parameters section of the Administration page.

Read more about the [Split View](#) feature in our article.

# Service

The Service account is used for a distributed job engine deployment so an Administrator can designate certain records to be executed by specific job engine nodes.

Read more about [Distributed Job Engine Deployments](#) for additional information about this role.

# Blocked

The Blocked role is used to block the user or group members’ access to objects in PAM. The blocked user can still login to PAM, but until they are unblocked, they will have no access to any objects or settings. Remove the Blocked role from the principal to restore their access.

# Automation

The Automation account is used to throttle the rate of new connections for scripts to control overall system performance. For additional configuration, read the description and adjust the global parameter *Throttle SSH Proxy Automation Connections* as needed.

# Local Users and Groups

Local users and groups can be created in Privileged Access Management’s internal user directory providing a method to quickly create, disable or automatically expire accounts for internal or external resources.

These accounts are independent of any external user directories that you may also integrate with Privileged Access Management (i.e. Active Directory or LDAP).

Only System Administrators may create and manage local users and groups on this global level.

# Create a Local User

To create a new local user, navigate to Administration > Local Users and click the **Create** button. Populate the new user form as required.

Login	Enter a unique value that will be used to login to the system.
First Name	Enter a first name for this account.
Mail	Enter a last name for this account.
Mail	Enter an email address for this account.
Expiration	Enter a date and time when this account will be automatically <i>disabled/locked</i> . Leave blank if you do not want to automatically <i>disable/lock</i> this account.
Password	Enter the password for this account. The password must meet the requirements of the <a href="#">Local User Formula</a> .
Repeat Password	Repeat the password for this account.

Click the **Save** button to complete the account creation process.

NOTE: Local Users can be added to Local Group membership only. Local Users cannot be added to any groups that originate from integrated external user directories like Active Directory.

## Local User Password Formula

The local user password formula allows you to customize the complexity required for setting and resetting local user passwords. This formula is used for local user passwords only and is separate from all other formulas in the system.

To configure this formula, navigate to Administration > Local Users and click the **Formula** button. Customize this formula as required and click the **Save** button when complete.

## Managing Local Users

Editing a local user account allows a System Administrator to update the First Name, Last Name, Email, Expiration and Password of any local user account.

Click the **Edit** button associated to the Login to edit an account.

Locking a local user prevents this account from logging into the system while Unlocking an account restores the ability to login to the system.

To *Lock* or *Unlock* an account, check the box next to the Login(s) and select Bulk Actions > **Lock** or **Unlock** option.

A locked account will display a lock icon (  ) in the Locked column.

Deleting a local user removes the account from the system.

Deleted accounts cannot be restored, so we would recommend using the *Lock* option instead of *Delete* if there is a possibility that the account will be needed again in the future.

To delete a local user, click their **Edit** button and then the **Delete** button on their account's edit page.

## Create a Local Group

Local Groups are created and managed within Access Manager's internal user directory and are used to provide group membership capabilities to both Local Users as well as external accounts like Active Directory Users.

To create a new local group, navigate to Administration > Local Groups and click the **Create** button. Populate the new group form as required.

<b>Name</b>	Enter a unique group name.
<b>Description</b>	Enter a group name description.

Once the group has been created, use the **Add Member** or **Remove Members** buttons to populate the group membership. Alternatively, you can use the **Edit** button to update membership or configuration of existing local groups.

NOTE: Local Group membership may include both local users and users that originate from your Privileged Access Management integrated [Active Directory](#).

Use the **Delete Group** button to delete the group and use the **Save Group** button to save any changes that have been made to the group.

## Secure IDs

Privileged Access Management provides the option to enable secured IDs to display randomized IDs for managed objects on the user interface.

The optional use of these secured IDs is intended to provide enhanced security and does not reduce the performance, scalability or use of Privileged Access Management.

When enabled, all internal IDs will be displayed or used in both the GUI and API calls using a randomized method to ensure they will no longer be assumed nor guessed to be in a sequential ordering.

Secure IDs will be displayed in all places where the default, sequential IDs were originally.

Before enabling secure IDs, please note the following:

- If a user has bookmarked any record links in their browser, these bookmarks will no longer work after as they are referencing the original ID.
- If you have any scripts or are using the API to call specific functions that contain the original IDs, they will need to be updated to reflect the new secure IDs.
- Using the SSH Proxy feature will require the use of the new secure record IDs or the generic sequential list number for connections.

## Enabling secure IDs

1. Log on to PAM host server with an account that can update files.
2. Open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor.
3. Add the following lines to the end of the file:

```
1 | #Secured IDs
2 | xtam.secured.ids=true
3 | xtam.secured.ids.strict=true
```

4. Save and close this file.
5. Restart the **PamManagement** (Windows) or **pammanger** (Linux) service.

When the service is fully restarted, all the existing IDs throughout Privileged Access Management will have been updated with secured IDs and the original will no longer be accessible.

# Secure ID Examples

XTAM | Record View

XTAM | Record View

XTAM | Discovery Query

+

https://xtam/#/records/record\_view/i-34ie3tUEk0i/type

All Records

Personal Vault

Favorites

< Active Directory >

< PBX System >

< Web Servers >

< Scripts >

< Forms >

< API >

< MSP >

Administration

Reports

Management

Unix Host Session

Go to Parent

Connect...

Execute...

Name

Unix Host Session

Description

unix host session (external) with standard user + pass

Host

10.0.0.26

Port

22

User

unix01

Password

\*\*\*\*\*

Record Type: Unix Host

ID: i-34ie3tUEk0i

Created By: @ 07/11/2017 15:54

Last Modified By: @ 06/27/2018 19:46

Last Action: Connect @ 01/27/2019 23:20

Last Success: Connect @ 01/27/2019 23:20

Job Queue: (click to refresh)

Secure IDs Example: Record View

System Audit Log

Found 30 audit log records.

Time: Last Day

Category: Any

Level: Any

Show 50 entries

Search:

CSV

PDF

Showing 1 to 4 of 4 entries

Time	User	IP	Object	Category	Level	Event	Message
01/30/2019 07:51:22	John Williams (john)		Unix Host Session	Operation	INFO	Session Completed	ID: i-1mBTtEYx9VI Recording
01/30/2019 07:51:19	John Williams (john)		Unix Host Session	Operation	INFO	Session Created	Protocol: SSH ID: i-1mBTtEYx9VI

First Previous 1 Next Last

Secure IDs Example: Audit Log



The screenshot displays the XTAM Record View interface. The browser address bar shows the URL: `https://xtam/#/records/record_view/i-34ie3tUEk0i/type`. The record is titled "Unix Host Session". The details section shows the following information:

- Name:** Unix Host Session
- Description:** unix host session (external) with standard user + pass
- Host:** 10.0.0.26
- Port:** 22
- User:** unix01
- Password:** \*\*\*\*\*

Metadata at the bottom of the record view includes:

- Record Type:** Unix Host
- ID:** i-34ie3tUEk0i
- Created By:** [User] @ 07/11/2017 15:54
- Last Modified By:** [User] @ 06/27/2018 19:46
- Last Action:** Connect @ 01/27/2019 23:20
- Last Success:** Connect @ 01/27/2019 23:20
- Job Queue:** (click to refresh)

Secure IDs Example: Sessions Report

## Auditor Role

What is the Auditor Role in Privileged Access Management and what access does it provide for users?

Beginning with the October 2, 2017 release, Privileged Access Management now includes an additional [Global Role](#) named **"Auditor"**.

This Auditor role allows for a Compliance Officer or Auditor to review and monitor the Privileged Access Management system and its records without having direct permissions to each object or exposing secrets and compromising security.

The screenshot shows the 'Grant Access' window. At the top is the title 'Grant Access'. Below it is the 'Principal' section with a search input field labeled 'Enter User or Group Name...' and an 'Add' button with a magnifying glass icon. Underneath is the 'Selected Principals' section, which contains a dropdown menu showing 'Brian Williams (bwilliams) /Local'. Below that is the 'Global Role' section with a dropdown menu. The dropdown menu is open, showing a list of roles: 'Auditor' (highlighted in blue), 'System Administrator', 'Split View', 'Service', and 'Blocked'.

## "Auditor" can

### A user that has been granted the "Auditor" role:

- Can **View** all records and folders. This includes Name, Description as well as any other record fields (except secured fields).
- Can review **Record Properties** including Type, Created By and Last Modified By parameters.
- Can access the **Audit Log** associated to records as well as the PAM system.
- Can access the **Session History** associated to records as well as the PAM system.
- Can access the **Job History** associated to records as well as the PAM system.
- Can access the **Formulas, Tasks, Permissions and Workflows** of a record or folder.
- Can access the PAM system **Reports**.
- Can access the **Scripts, Tokens, Workflows and Command Control** configurations throughout the PAM system (view only).

## "Auditor" cannot

### A user that has been granted the "Auditor" role:

- Cannot *"Unlock"* or *download* secrets, passwords, certificates or any other object associated to a secured field.
- Cannot *Connect, Join* or *Terminate* active sessions.
- Cannot *review* a record's Change History.
- Cannot *execute* jobs, scripts or password reset tasks.
- Cannot *Create, Edit* or *Delete* a folder or record.
- Cannot *Create, Edit* or *Delete* a workflow, template, binding or grant approval.

- Cannot *modify* Formulas, Tasks, Permissions or Workflows of a record or folder.
- Cannot *reorganize* folders or records using the *Cut*, *Copy* or *Paste* commands.

Please note that if a user or group is assigned the *Auditor role* plus additional permissions to a folder or record, the privileges associated to the folder or record will take precedence over that of the global Auditor role.

## Folder Level Users

Users at the level of the Manage / Local Users folder can be created by a User with the Global Administrator role or by a User with Owner permissions.

Folder Level Users obey the following rules:

- The options are available to folder owners for all folders with the exception of a root folder and any folder in a personal folder.
- All rules are enforced in the GUI and through the server-side AP.
- Folder-level API Tokens could be generated for the folder-level users only. Global tokens could be generated for any users though (even for folder-level ones).
- Owners cannot grant permissions for folder-level principals (users or groups) from other folders. System principals, AD principals or folder-level principals from the same folder could be used for permissions.
- A folder-level principal cannot be granted system admin or system auditor roles.
- Folder-level principals cannot be granted any global permission.
- Folder level groups can include system principals or principals from the same folder as group members but not from other folders.
- Principals and API tokens from subfolders could be managed in the parent folders.
- Folder-level API Tokens could be generated for the folder-level users only. Global tokens could be generated for any users though (even for folder-level ones).
- Owner are available to manage item workflow bindings allowing system administrators to delegate workflow management to vault and folder owners.

## Preventing Users Access to PAM or its Objects (Deny Login and Block Access)

PAM offers several options for a System Administrator to control a user's (or group) access to the software or the objects managed within it. Depending on the circumstances needed, here are methods that can be employed to manage access to PAM.

### Deny Login of a User or Group

When a user or group is denied login to PAM, they are unable to successfully authenticate into PAM.

This prevents a **Deny Login** user from authenticating into PAM by any means including the PAM web console, remote web sessions, proxy sessions and API access.

The **Deny Login** feature can also be useful if you are configuring PAM access to only specific users or groups.

This is done by applying the Deny Login option as the *Default* state for all users and then allowing for exceptions to these users or groups for which you wish to allow PAM authentication.

# Deny Login Required Configuration

The following procedure is required to enable the Deny Login option.

Before you begin, please review, and perform the steps outlined in this section.

1. Login to PAM with a System Administrator account and confirm the Federated Sign-in Module version by navigating to Management > About. On this **About** page, find the parameter **Authentication** and confirm the version is 5.2.8.20221013 or later (Authentication: CAS 5.2.8.20221013). If the displayed Authentication version is earlier or does not display a version number, then you must first update this component using this guide before continuing: [Updating the Federated Sign-in Module](#).
2. Login to the PAM host server and open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor. Elevated permissions may be needed to change or save this file.
3. In this file, use search to confirm or update so that the following parameter is commented out (put a # character before the line). This parameter may appear several times in this file, and each should be commented out:

```
1 | cas.authn.mfa.globalProviderId=mfa-
```

If one of these **globalProviderId** parameters is currently uncommented, then your PAM is configured to use that uncommented MFA provider as its global default. In this configuration, deny login cannot be used, you should stop and contact our Support Team <https://support.imprivata.com/communitylogin> for further help.

4. In this file, use search to confirm or update so that the following line is **uncommented** (remove the # character before the line):

```
1 | cas.authn.mfa.groovyScript=[path/to/file/xtam-mfa.groovy]
```

The exact file path after the equal sign will differ between PAM deployments depending on the underlying operation system (Linux vs Windows) as well as the location where PAM was installed on the host server. Simply *uncomment* this line and do not modify the existing file path after the equal sign.

5. In this file, use search to find and **uncomment** the below parameter if it already exists (remove the # character before the line) **or** if not found, **add it** as a new line:

```
1 | cas.authn.mfa.u2f.name=mfa-u2f
```

6. When complete, **save and close** this file.
7. **Restart** the PamManagement/pammanager service.

## Deny Login to a Specific Users or Groups

A System Administrator can apply the *Deny Login* feature to a User or Group using the MFA configuration page in PAM.

1. Navigate to Administration > MFA and click the **Add** button.
2. For the *Principals* option, click **Add** and then add the User(s) or Group(s) that you wish to apply to the Deny Login policy. Click **Select** when complete.
3. Next, from the *Provider* dropdown menu, choose the **deny login** choice.
4. Finally, click the **Save** button to finish this configuration.

**New**

Save

Cancel

Default ?

☐

Principals ?

Add

bravo test (bravotest) /AD ▾

TestBGroup /AD ▾

Provider ?

deny login ▾

Only one MFA provider may be applied to a principal. If the principal already has a policy applied, you will need to remove the current provider and apply the *Deny Login* policy for this feature.

## Deny Login to Everyone with Allowed Exceptions

To configure PAM to only allow authentications from selected users or groups, you can use the *Deny Login* default state.

The Deny Login policy as the default state will deny login to all valid logins except for the allowed exceptions that have been configured.

The following configuration will provide an example of how *Deny Login* can be used to allow only specific Principals to authenticate into PAM.

Only one Provider may be assigned the *Default* state. If another provider is using the *Default* state, then please consider how best to configure *Deny Login* with your existing MFA providers to meet your requirements.

The example requirement is to allow only the local System Administrator, one Domain user account and one Domain Group to login to PAM with MFA enforcement. We will start the example assuming there are no current MFA configurations (i.e., Administrators > MFA is empty).

- 1. Navigate to Administration > MFA and click the **Add** button.
- 2. For the *Principals* option, click **Add** and then add the User(s) or Group(s) that you wish to not include to the Deny Login policy. In our example, this will be the local System Administrator, our one *Domain User Account* and our one *Domain Group*. Click **Select** when complete.
- 3. Next, from the *Provider* dropdown menu, select the **none** choice. You may also select a different MFA provider, but for testing we recommend using *none* until you are comfortable with this process.
- 4. Click the **Save** button to finish this configuration.
- 5. Click the **Add** button again to create another new MFA policy. For this next policy, click the **Default** checkbox and select the **deny login** option from the *Provider* dropdown menu.

New

Save

Cancel

Default ?

☒

Provider ?

deny login

▼

- 6. Click the **Save** button to finish this added configuration. Our completed example configuration is shown below.

MFA Configuration

Found 4 entries.

Add

Delete

↺

Show

50

▼

entries

CSV

PDF

XLSX

PDF Protected

CSV Protected

XLSX Protected

Search:

Showing 1 to 4 of 4 entries

User	Provider	Enabled	Actions
<input type="checkbox"/> bravo test (bravotest) /AD	none		...
<input type="checkbox"/> TestBGroup /AD	none		...
<input type="checkbox"/> Service Administrator (pamadmin) /Local	none		...
<input type="checkbox"/> <b>DEFAULT</b>	deny login		...

First

Previous

1

Next

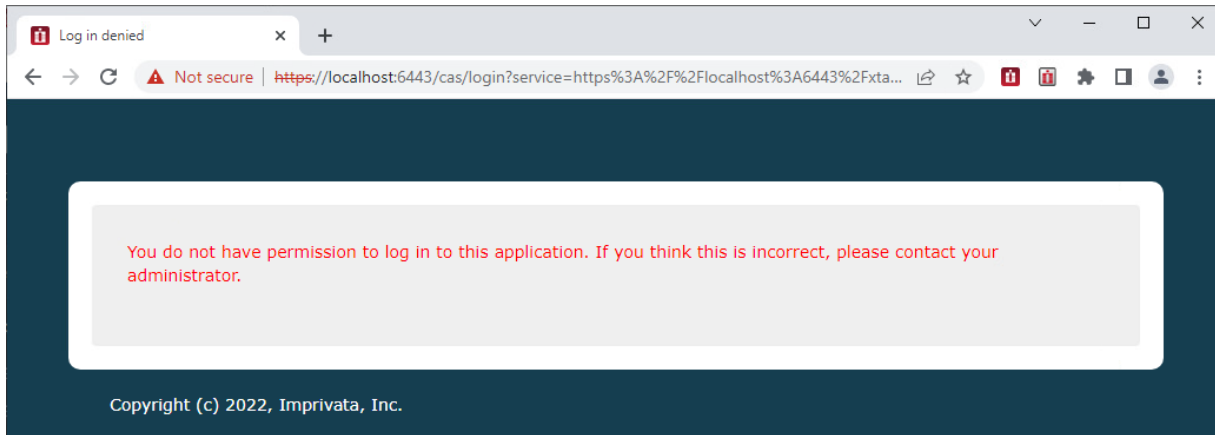
Last

To test this configuration, first login to PAM using one of the allowed user accounts. The expected experience for this account is that they should successfully login to PAM.

If you configured a provider other than *none*, you would be expected to supply your MFA requirement prior to successful login to PAM.

Next, login with any other valid user account that is not one of our *allowed* accounts.

After this user successfully authenticates their credentials to PAM, they will be denied login to the software.



## Customizing the Deny Login Message

When a *Deny Login* user attempts to login to the PAM web console, they are presented with a page that displays a message saying that their login does not have permission to access this application. On this page, both the *Page Title* text and *Message Body* text can be customized.

To change this text, login to the PAM server and perform the following procedure:

1. **Open** the `$PAM_HOME/web/webapps/cas/WEB-INF/classes/custom_messages.properties` file in a text editor.
2. **Locate** the two parameters **pam.mfa.deny.pagetitle** and **pam.mfa.deny.message**
3. **Update** the text of one or both parameters and **save** the file when finished.
4. A service restart is not needed, but it may take several minutes before the updated message appears to the users. Wait a few minutes and **retest** a *Deny Login* account to confirm the customized message is now visible.

## Blocked Users or Groups

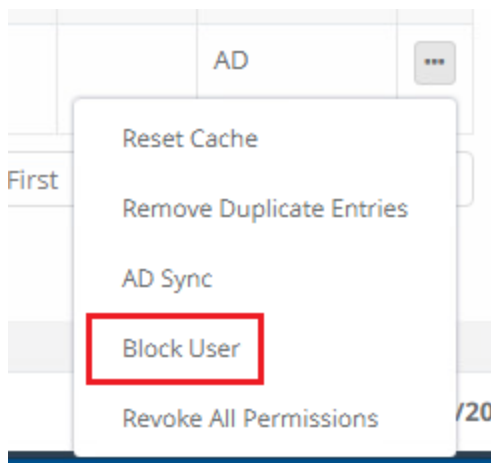
To remove a user's access to objects and settings within PAM, a System Administrator can apply the Blocked role to their account. When a user is blocked, they may still log in to PAM, but their access to objects stored in the vault is no longer available until they have been unblocked or this role is removed.

This can be a useful method if a System Administrator wants to easily remove a user's access to PAM objects without making changes to the permissions on objects. Conversely, a user can be unblocked or have the blocked role removed from their account to quickly restore their access to PAM objects.

## To Block a User or Group

A System Administrator can block a user directly from the Users Report:

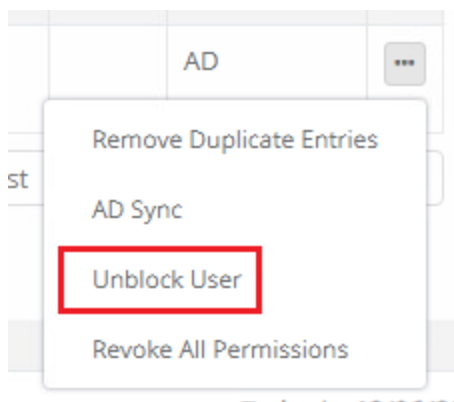
1. Navigate to Records > Report Center > Users Report and find the user that you wish to block.
2. From this user's Actions menu (...) select the **Block User** option and click **OK** on the confirmation dialog.



After the selected user has been blocked, you will notice that their Username in the Users Report is now crossed out showing this account is blocked. Additionally, you will see the *Blocked role* has been applied to the account in the report's *Global Role* column.

<del>bravo-test (bravotest) /AD</del>	User	12/06/2022 08:58:26				Blocked (Direct)
---------------------------------------	------	---------------------	--	--	--	------------------

To unblock this user, from their Actions menu (...) select the **Unblock User** option and click **OK** on the confirmation dialog. After unblocking, the crossed-out font on the *Username* and the *Global Role Blocked* will be removed from this account.



A System Administrator may also block a user from the *Global Roles* page:

1. Navigate to Administration > Global Roles and click the **Add** button.
2. Add the user you wish to block to the Principal field and then select the **Global Role Blocked** from the dropdown menu.
3. Click the **Select** button to complete the operation.



### Grant Access

**Principal ?**

Add

Q

**Selected Principals**

bravo test (bravotest) /AD

▼

**Global Role ?**

Blocked

▼

Cancel

Select

After the selected user has been blocked, you will notice that their account is now visible in the *Global Role* list with the *Blocked* role applied. Their account will also be crossed out and have the Blocked role if you also find it in the [Users Report](#).

To unblock this user, select this user by clicking on the checkbox on their Blocked row and click the **Remove** button. This will remove the *Blocked* role from the account and the user will be unblocked.

Found 2 entries.

Add

Remove

↺

Principal	Type	Role
<input type="checkbox"/> Service Administrator (pamadmin) /Local	User	System Administrator
<input checked="" type="checkbox"/> bravo test (bravotest) /AD	User	Blocked

# Privileged-Elevation-Management Ephemeral Accounts

PAM can create *Ephemeral Accounts* to support *no standing access* to privileged systems.

This helps support the concept of least privileged using time based workflows to provision and de-provision an account when needed and only with the permissions that are required.

# Creating Ephemeral Account Records

1. Login to PAM with a System Administrator account.
2. Navigate to Administration > Record Types, locate the type **Windows Host Ephemeral Account** and click the **Edit** button.
3. Uncheck the Hidden box and click **Save**.

Now that the Record Type is unhidden, you can log out of the System Administrator account. It is no longer required to complete the configuration.

4. Navigate to a location in the Vault where you wish to create the record and select Add Record > Windows Host Ephemeral Account.
5. Create your record using the below as guidance:
  - **Name:** enter a name for your record.
  - **Description:** optionally, enter a description for your record.
  - **Host:** enter the host for the endpoint where the ephemeral account will be created.
  - **Port:** enter the port that will be used for connectivity.
  - **User:** enter the username that will be created for the ephemeral account.
  - **Password:** leave this field empty.
6. Click **Save and Return**.

After the record is saved, we will now configure the Task that performs the ephemeral account creation process.
7. In this new record, click Manage > Tasks.
8. For the Shadow Account, select an existing record that contains the credentials of an account that can create new local accounts on this endpoint. For example, in a Windows domain, this could be a record that contains the credentials of a Domain Administrator account.
  - If the [Shadow Account](#) field is read-only, that means it is set to inherit this Shadow Account from the record type. In this situation, you will need to navigate to Administrator > Record Types and add this [Shadow Account](#) directly to the Tasks list of this type. This will require your System Administrator account again. Alternatively, you can click the **Make Unique** button to break inheritance from the *Record Type*.
  - If the Shadow Account field is *read/write* enabled, then enter the name of the record that contains the credentials of an account that can create local accounts on this endpoint.
9. Once you have the *Shadow Account* configured, save your change and return to the record.
10. After the Shadow Account is saved, we will next configure the Workflow, whose approval and subsequent expiration, will trigger the creation and ultimate removal of the ephemeral account.
11. From the Record, select Manage > Workflows to configure a workflow binding.
12. On the Workflow Bindings page, you will create a new workflow binding that will be used to request access and once approved, will be used to generate the ephemeral account.
13. Create the Workflow Binding as needed and click the **Save** button to complete the process.

14. That completes the configuration of the *Ephemeral Account* process. In the next section, we will illustrate the User experience from workflow request through the workflow expiration when the ephemeral account is removed from the host.

## The Ephemeral Account Process

1. Login to PAM with the user account that was bound by the workflow created in the previous section.
2. Navigate to this Ephemeral Account record and click the **Request Connect** button.
3. Fill out the request access form as required and submit it when completed. During testing, we would recommend requesting a short amount of time (i.e. 5 minutes) so that you do not have to wait too long for the workflow to eventually expire.
4. If the submitted workflow was not configured for automatic approval, Approve the submitted request to continue.
5. Once approved, PAM will begin the Ephemeral Account creation process. Depending on the PAM queue, this process may take a few seconds or a few minutes to complete. You can follow the process by monitoring the Job History tab of this record.
6. After the Ephemeral Account is successfully created, the user's *Connect Requested* button will change to *Connect* indicating that the user may now connect to the Host with the Ephemeral account.
7. Click **Connect** to create your remote session.
8. The User will connect to the Host with this newly created ephemeral account. When done, simply *Disconnect* or *Sign Out* of the remote session to complete.
9. Finally, after the workflow's approved time expires, the user's *Connect* button will change back to *Request Connect* and PAM will delete this Ephemeral Account from the Host.

## Just-In-Time Permission Elevation

A *Just-In-Time Permission Elevation* option is designed to promote increased security using the principle of no standing trust.

This design also limits the time a privileged account exists on a critical system, especially with enabled special access.

The goal is not just about limiting time, but to have a zero standing privilege strategy on users and servers.

*Just-In-Time* (JIT) Permission Elevation helps customers implement these strategies and reduce the number of privileged accounts in their network and control access to active privileged accounts.

### Prerequisites:


Just-In-Time Permission Elevation is supported **ONLY** for Windows Hosts.

## Create Just-In-Time Permission Elevation Record Type

### *Step 1. Create a new PAM record*

1. Login to PAM as a System Administrator.
2. Navigate to Administration > **Record Types**.
3. Click on the **New Record Type** button.

4. Enter a **unique name** for this new record type, select in the first field: Session Manager > RDP. Leave the second field **Hidden Field** unchecked (blank).
5. Click **Save** in the top right corner.

Create Record Type 

Root Folder / Record Types / Windows Host JIT Permission Elevation

Record Type: Windows Host JIT Permission Elevation

Found fields. Save Cancel

Name: Windows Host JIT Permission Elevation

Description:

Session Manager: RDP

Parent Type:

Hidden: ☐

Personal Vault: ☐

Vaults:

## Step 2. Add Just-In-Time (JIT) Record type

The fields of this Just-In-Time (JIT) [Record type](#) will need to be added.

1. Click the **Add Field** button towards the bottom of this page and add the minimum required fields: *Host*, *Port*, *User* and *Password*.

If other fields for the Just-In-Time (JIT) record type are required per your configuration, please also add those fields as well during this step.

Edit Field: Host Save Delete Cancel

Field Type: String

Name: Host

Display Name: Host

Hidden: ☐

Secured: ☐

Indexed: ☐

Order: 100

Helper:

Default Value:

## Edit Field: User

[Save](#) [Delete](#) [Cancel](#)

Field Type	<input type="text" value="String"/>
Name	<input type="text" value="User"/>
Display Name	<input type="text" value="User"/>
Hidden	<input type="checkbox"/>
Secured	<input type="checkbox"/>
Indexed	<input type="checkbox"/>
Order	<input type="text" value="120"/>
Helper	<input type="text"/>
Default Value	<input type="text"/>

## Edit Field: Port

[Save](#) [Delete](#) [Cancel](#)

Field Type	<input type="text" value="Number"/>
Name	<input type="text" value="Port"/>
Display Name	<input type="text" value="Port"/>
Hidden	<input type="checkbox"/>
Secured	<input type="checkbox"/>
Indexed	<input type="checkbox"/>
Order	<input type="text" value="110"/>
Helper	<input type="text" value="3389"/>
Default Value	<input type="text"/>

## Edit Field: Password

[Save](#) [Delete](#) [Cancel](#)

Field Type	<input type="text" value="String"/>
Name	<input type="text" value="Password"/>
Display Name	<input type="text" value="Password"/>
Hidden	<input type="checkbox"/>
Secured	<input checked="" type="checkbox"/>
Indexed	<input type="checkbox"/>
Order	<input type="text" value="130"/>
Helper	<input type="text"/>
Default Value	<input type="text"/>

As a minimum requirement now the record type should look as below:

Record Type: Windows Host JIT Permission Elevation

Found 4 fields.

Formula

Tasks

Commands

Edit Icon

Save

Delete

Cancel

Reindex

Name

Windows Host JIT Permission Elevation

Description

Session Manager

RDP

Parent Type

Hidden

Personal Vault

Vaults

Add Field

Field	Display Name	Field Type	Default Value	Hidden	Secured	Indexed	Helper	Actions
Host	Host	String						<div>Edit</div>
Port	Port	Number					3389	<div>Edit</div>
User	User	String						<div>Edit</div>
Password	Password	String			✓			<div>Edit</div>

### Step 3. Add Tasks

- Next, click on the **Tasks** button to add the required tasks to perform the Permission Elevation against the host.
- Click **Add Task** and add the following tasks:
  - Script: Windows Local Account Permission Elevation Post-Access with Policy: After Expire
  - Script: Windows Local Account Permission Elevation Pre-Access with Policy: After Approval
- Once added the tasks page should now be set as shown below:

Tasks

Root Folder / Windows Host JIT Permission Elevation / Tasks

Tasks for Windows Host JIT Permission Elevation

Add Task

Save

Shadow Account

Search records...

Time Window

Script	Policy	Actions
Windows Local Account Permission Elevation Post-Access	After Expire	<div></div>
Windows Local Account Permission Elevation Pre-Access	After Approval	<div></div>

### Step 4. Create your record

- Navigate to a location in the *Records* vault where you wish to create the record and select Add Record > **Windows Host JIT Permission Elevation**.

© 2025 Imprivata, Inc. All Rights Reserved.

| 600

2. Use this guidance to create your record:

<b>Name</b>	enter a name for your record
<b>Description</b>	*optionally, enter a description for your record
<b>Host</b>	enter the host for the endpoint where the Permission Elevation will be required
<b>Port</b>	enter the port that will be used for connectivity
<b>User</b>	enter the username that will get Permissions Elevated
<b>Password</b>	enter the password of the user

3. Click **Save and Return**.

## Step 5. Configure the Task

Configure the Task that performs the Permission Elevation process.

1. In your new created record, click Manage > **Tasks**.
2. For the [Shadow Account](#), select an existing record that contains the credentials of an account that can assign and remove user roles on this endpoint.

For example, in a Windows domain, this could be a record that contains the credentials of a *Domain Administrator* account.

- **read-only**: if the [Shadow Account](#) field is **read-only**, that means it is set to inherit this Shadow Account from the record type. In this situation, you will need to navigate to Administrator > Record Types and add this **Shadow Account** directly to the *Tasks* list of this type. This will require your *System Administrator* account again. Alternatively, you can click the **Make Unique** button to *break inheritance* from the [Record Type](#).
- **read/write**: if the Shadow Account field is **read/write** enabled, then enter the name of the record that contains the credentials of an account that can create local accounts on this endpoint.

3. Once you have the **Shadow Account** configured, save your change and return to the record.

## Step 6. Configure the Workflow

Next, configure the Workflow, whose approval and subsequent expiration, will trigger the creation and ultimate removal of the Permission Elevation.

Here is the help article about [Workflows](#) as well as a table of contents on the right-hand side about other [Workflow](#) related knowledge articles.

1. In the Record field select Manage > **Workflows** to configure a Workflow binding.
2. On the Workflow Bindings page, you will create a new Workflow binding that will be used to request access and once approved, the permission of the user in the record will get elevated to Administrator on the end point host.

3. Create the Workflow Binding as needed and click the **Save** button to complete the process. The required minimum of Workflow configuration for *Just-In-Time Permission Elevation*:

- Actions
- Time selectors

**Actions** ?

<input type="checkbox"/>	Administration
<input type="checkbox"/>	Record Control
<input checked="" type="checkbox"/>	Connect Control
<input type="checkbox"/>	Task Control

**Time Selector** ?

<input checked="" type="checkbox"/>	Work Hours
<input checked="" type="checkbox"/>	After Hours
<input checked="" type="checkbox"/>	Weekends
<input checked="" type="checkbox"/>	Holidays

Cron Expression

4. That completes the configuration of the *Just-In-Time Permission Elevation* process.

In the next section, we will illustrate the User experience from Workflow request through the Workflow expiration when the *Permission Elevation* is removed from the host.

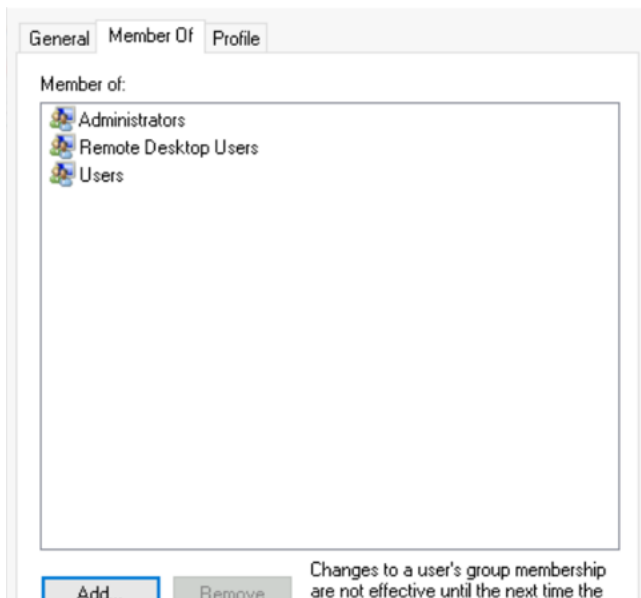
## The Just-In-Time Permission Elevation Process

1. Login to PAM with the user account that was bound by the *Workflow* created in the previous section.
2. Navigate to this *Just-In-Time Permission Elevation* record and click the **Request Connect** button.
3. Fill out the request access form as required and submit it when completed.

During testing, we would recommend requesting a short amount of time (i.e. 5 minutes) so that you do not have to wait too long for the workflow to eventually expire.

4. If the submitted workflow was not configured for automatic approval, Approve the submitted request to continue.
5. Once approved, PAM will begin the *Permission Elevation* process. Depending on the PAM queue, this process may take a few seconds or a few minutes to complete. You can follow the process by monitoring the **Job History** tab of this record.
6. After the *Permission Elevation* is successfully completed, the user's *Connect Requested* button will change to *Connect* indicating that the user may now connect to the Host with the *Permission Elevation* as an Administrator on the host.
7. Click **Connect** to create your remote session. The User on the *Record* which is used to connect to the host is now an *Administrator*.





8. Finally, after the Workflow's approved time expires PAM will execute the task to remove the Permission Elevation of Record User. The PAM user's *Connect* button will change back to *Request Connect* and the Permission Elevation on the host will be removed.




## Secure Remote Sessions (Connect)

PAM can be used to establish secure, interactive sessions to remote [Windows](#), Linux, Unix or Mainframe endpoints, Network Devices like [Cisco](#), [Juniper](#) or [Palo Alto](#), and [Websites](#) or Web Management Portals, all while using a standard web browser or [native SSH clients](#) without disclosing your secrets or passwords.

### Connect

Connections to these remote endpoints or assets originate from the record that contains the values for the endpoint.

**To create a new connection to a remote endpoint**, click the **Connect** button from the Record List page (  ) or click the **Connect** button located in the record when it is viewed. A new session will be launched in your browser using the settings as configured from your [preferences](#).

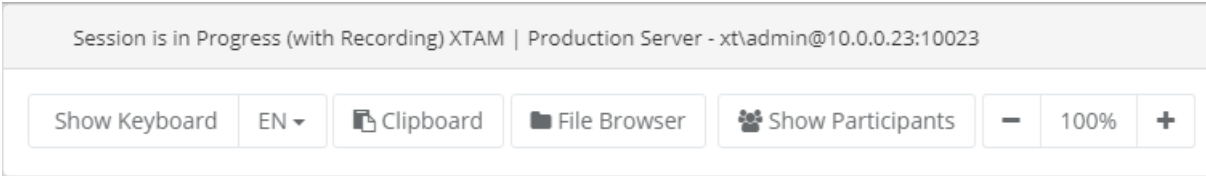
- If you are presented with both a **Connect** and **Connect and Record** option, then choose the method that you wish to connect using.
- The *Connect and Record* option will record your session as defined by your Session Control permissions, while *Connect* will not record.
- The *Connect* option may be shown as **Request Connect** which indicates that you are required to request access before you are able to connect.
- Once your request has been submitted and approved, the *Request Connect* button will switch to *Connect* for the time period that you have been approved.
- When the requested time expires, the *Connect* button will return to the *Request Connect* state and you will need to request access again.
- To check the status of your Workflow Requests, visit your [My Workflows](#) pages.
- If the Connect option is not available, then either the record is not configured to support remote sessions or you lack the required permissions to create a connection to the endpoint.

# In-Session Menu

While in an active browser session, you can open the In-Session Menu to utilize additional options.

To activate the In-Session Menu hover your mouse pointer in the top 30 pixels of the remote session for a second or two.

The menu will then dropdown from the top of the session and provide the following options:



Show Keyboard / Hide Keyboard	Click to Show or Hide the onscreen keyboard.
Keyboard Layout Selector	Used to select your keyboard language layout.
Clipboard	Opens the clipboard menu so that text can be copied into or out of the remote session.
File Browser	Opens the File Browser to allow files to be transferred into or out of the remote session.
Show Participants	If multiple participants are joined to the same session, this will display the list of participants, their IP address and the Owner label indicating who is the user who created the initial session. When the Owner disconnects, the session will complete for all participants.
Zoom Controls	Click the + and – buttons to zoom in or out of the session in your browser. Click the 100% button to return to full screen.

To close the menu simply move your mouse pointer away from the menu for a few seconds or press the **Esc** key on your keyboard.

## Join

An Active remote session can be joined by one or more additional participants. These additional participants may either watch the session in real time or they can interact with it and take control of the keyboard and mouse.

**To join an active session**, locate the session you wish to join from the Record's *Session* or System's *Session* report, click the Actions menu and then select the **Join** option.

- Confirm that you wish to join the active session and you will enter the active session in a few seconds.
- Newly joining participants will be visually announced to all current participants and will appear in the *Show Participants* menu along with their current IP address.
- To leave a joined session, simply close your session's browser or tab window.
- Departing participants will be visually announced to all current participants and will then be removed from the *Show Participants* menu.
- If the Owner of the session, the user who created the initial connection, leaves or disconnects then the session will complete for all participants within a few seconds.

## Terminate

An Active remote session can be terminated by another user with the required permissions.

When an active session is queued for termination, the session will be force completed without warning within approximately one minute.

**To terminate an active session**, locate the session you wish to terminate from the Record's *Session* or System's *Session* report, click the **Actions menu** and then select the **Terminate** option.

Confirm that you wish to terminate the active session and it will be queued for termination.

Neither the session's Owner nor any other participants will receive a warning or notification that their session is being forcibly terminated.

Their active session will close and be logged as *Completed* within approximately 60 seconds.

## Automatically terminate

The inactivity timeout option automatically terminates RDP Proxy sessions.

To enable the option specify idle timeout in seconds in the global parameter RDP Proxy Idle Timeout.

Disconnect open RDP proxy session if it is idle for the specified number of seconds.

If set to 0 then it will never disconnect idle sessions. Use **zero** to disable idle timeout enforcement.

## Windows Logoff Disconnection

When a user closes remote RDP sessions without a proper log off procedure leaving open disconnected sessions on the remote computers waiting to timeout, the Windows Logoff Disconnected Sessions script could be used in the After Session event trigger to forcefully log off disconnected inactive sessions from Windows computers.

The script assumes PowerShell access to the remote endpoint with the option to terminate sessions.

The script could be scheduled to run using a shadow account with administrator privileges and allows maintaining data security on the remote servers by minimizing the time of opened RDP sessions.

## Recording

Sessions that are configured for recording via [Object Permissions](#), will be done so either automatically or by the user’s decision in the case of Optional recording.

- When a user has the *Always* recording configuration assigned, their sessions will always be recorded. The option to not have their session activities recorded is unavailable. The *Connect* option will always record their session.
- When a user has the *Optional* recording configuration assigned, their sessions can be recorded or not depending on the user’s decision. When this user selects the *Connect* option, a dropdown menu will appear and present their choice to either **Connect** or **Connect and Record**.
- When a user has the *No* recording configuration assigned, their sessions will not be recorded. The *Connect* option will not record their session.

Session recording consists of two components; Screen Video Recording and Session Event Recording.

## Video Recording

A session with video recording enabled is generating a full resolution video all user interactions performed while connected, that can be later played back using your web browser or converted to a video file.

Playback includes Play, Pause and Scrubbing functions and is made available immediately after the session changes from *Active* to *Completed* status.

**To view the playback of a recorded session in your browser**, locate the session you wish to view from the Record’s *Session* or System’s *Sessions* report, click the Actions menu and then select the **Instant Video Playback** option.

A new browser window or tab will open to load the playback, and you can press the **Play** button to start at the beginning of the recording or use your mouse to start at another time by clicking on the playback timeline.

The Instant Video Playback cannot be viewed outside of the system.

**To convert the playback to a video file** that can be viewed or shared outside of PAM in a native video player, locate the session you wish to convert from the Record’s *Session* or System’s *Sessions* report, click the Actions menu and then select the **Convert to AVI**, **Convert to MOV** or **Download (zip)** options.

The video will be queued for *Rendering* and will eventually change to a *Download* link when the rendering is complete.

Click the available Download link to save the file to a file share.

Convert to AVI	(In-browser web sessions only) Select this option to convert the video recording to a .avi video file.
----------------	--

Convert to MOV	(In-browser web sessions only) Select this option to convert the video recording to a .mov video file.
Download (zip)	(SSH Proxy sessions only) Select this option to download the native SSH proxy session recording. The zip download will include typescript recorded session in a native format (individual metadata, timing and typescript files). These files can be used for playback using the native Linux <i>scriptreplay</i> command.

## Session Event Recording

A session with session event recording enabled is generating a Session Event report containing user interactions performed while connected.

Session Events include keystrokes, clipboard copy and file transfers, both to and from the remote endpoint.

These Session Events are recorded while the session is still active, so you can review the report during *Active* sessions and after *Completed* sessions.

To view the Session Event report, locate the session you wish to review from the Record's *Session* or System's *Sessions* report, click the Actions menu and then select the **Events** option.

The Session Events report will open and display a list of events that have been generated.

If the session is still Active, you can use the **Refresh** button to update the session as events are captured, while Completed sessions will display all events, sorted from newest to oldest in terms of session time.

For each event, there is an Action menu that may provide additional options:

Details	For keystroke and clipboard events, the Preview column displays the first 1024 characters. If the event is larger than 1024 characters, this Details option will display the full series of characters.
Jump to Recording	For completed sessions that were also video recorded, this option will start the in-browser Instant Video Playback at this event's timestamp.

For more information about the Session Event report itself, see our [Session Event Report](#) article.

## RDP Client Proxy Sessions

When PAM's RDP Proxy feature is enabled, you can use a native RDP desktop or mobile client or prompt to connect to a record and provide a secure experience while maintaining control of the privileged rdp-enabled endpoint.

**NOTE:** The RDP Proxy feature must be enabled and configured by a System Administrator. If you would like to use this feature, please talk with your System Administrator for additional information.

## Connecting to a Managed Windows Endpoint using an RDP Client

To connect to a managed endpoint from your RDP client, enter the PAM host and port as provided to you by your System Administrator in the client's *Host* or *Computer* field.

For example, the RDP Host or Computer you would enter into your RDP client would be `xtam.company.com` and the default port would be `3388`.

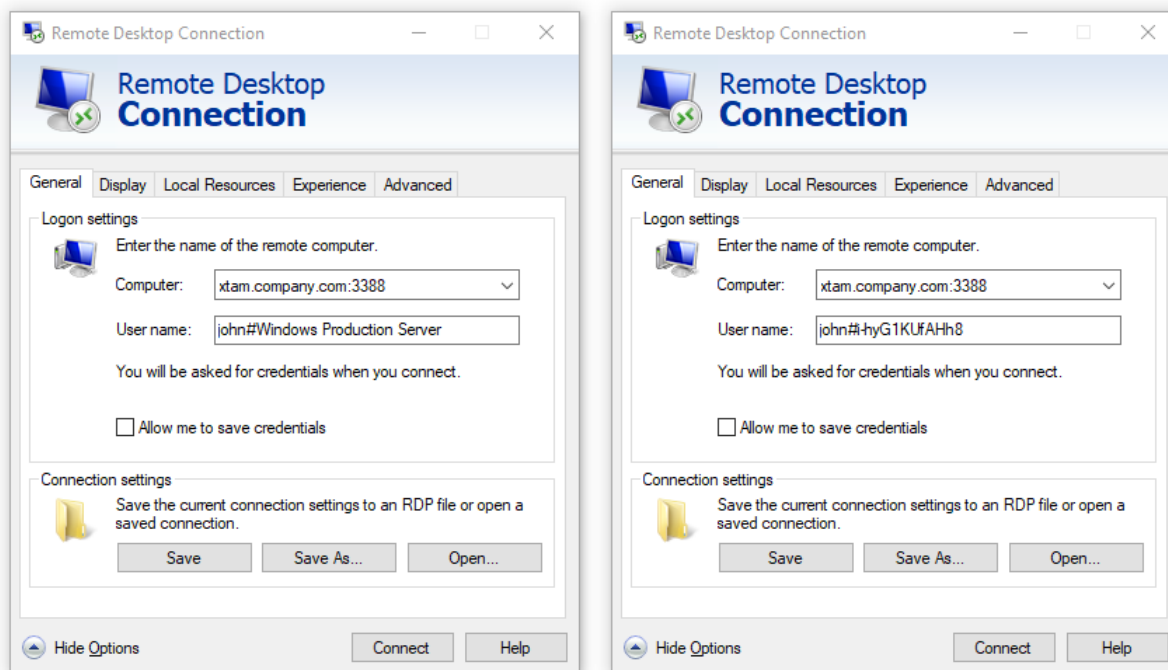
For the Username value, you will enter a connection string as shown demonstrated in the example scenario below.

This connection string as the User will both provide a means to authenticate your account in PAM and determine which record to use to create the secure session.

We want to connect to a rdp-enabled Windows endpoint managed by the record with the name **Windows Production Server** and ID **i-hyG1KufAHh8**.

In the RDP client's Username field, we will enter the string **john#Windows Production Server** or **john# i-hyG1KufAHh8** where *john* is our login name for PAM.

After the connection is initiated, enter your password when prompted and in a moment your RDP client will connect to the rdp-enabled endpoint stored in this record.



NOTE: To connect directly using the record name, the name must be unique. If two or more records exist with the same name, then you must use the record ID to connect as that is always a unique value.

When you are finished with your RDP proxy session, simply use the normal Disconnect or Sign out option in Windows to complete your session.

## SSH Client Proxy Sessions

When PAM's SSH Proxy feature is enabled, you can use a native SSH desktop client or prompt to connect to a record and provide a secure experience while maintaining control of the privileged ssh-enabled endpoint.

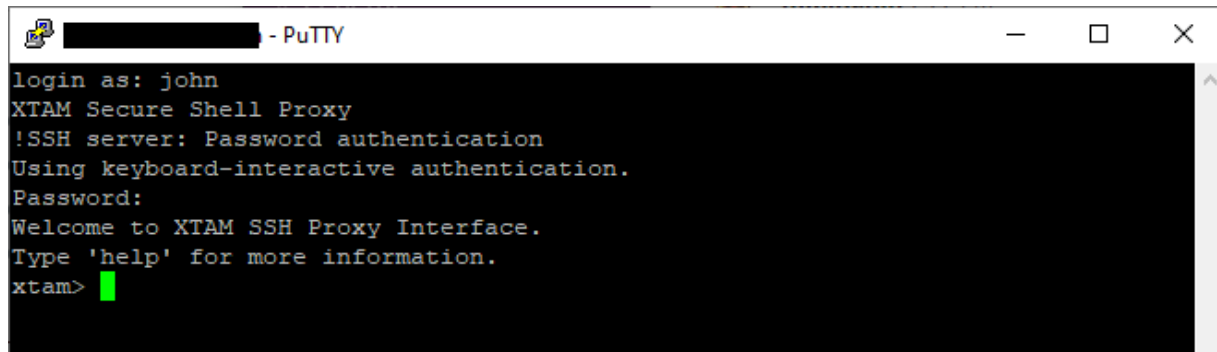
NOTE: The SSH Proxy feature must be enabled and configured by a System Administrator. If you would like to use this feature, please talk with your System Administrator for additional information.

## Connecting to the SSH Proxy Interface

To connect to the PAM SSH Proxy Interface in your SSH client, enter the PAM host and port as provided to you by your System Administrator.

When authenticating to the PAM SSH Proxy Interface, enter your same username and then password that you enter to login to the PAM web portal.

Optionally, the SSH Proxy connection also supports the use of [Public/Private key pairs](#) for authentication.



```
login as: john
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
Welcome to XTAM SSH Proxy Interface.
Type 'help' for more information.
xtam>
```

Once successfully connected, you will be greeted with the message *Welcome to PAM SSH Proxy Interface* and an *xtam>* prompt.

From the *xtam* prompt, these commands are available for use:

help, ? or help <command name>	The Help command prints a list of available commands and a brief description.
records or rec	The Records command generates a list of records, in the format <i>List Number) Id: Record ID Record Name</i> , that are available to you based on permission and type. The list number, record ID or unique record name can be used for selection when creating an SSH Proxy session.
connect or conn	The Connect command is used to connect to the record defined by its list number, record ID or record name. You can only connect by record name if the name is unique.
filter or filt	The Filter command is used to filter the list of available records that is returned. You can add <i>-i</i> to ignore case.
less	The Less command adds pagination to the list of available records. Use <b>q</b> to exit pagination and return to the prompt.
exit	The Exit command closes the SSH proxy session.

TIP: You can use the TAB key to auto complete commands.

Use the **connect** or **conn** command to connect to an available record and when you are finished use the **exit** command to complete your session.

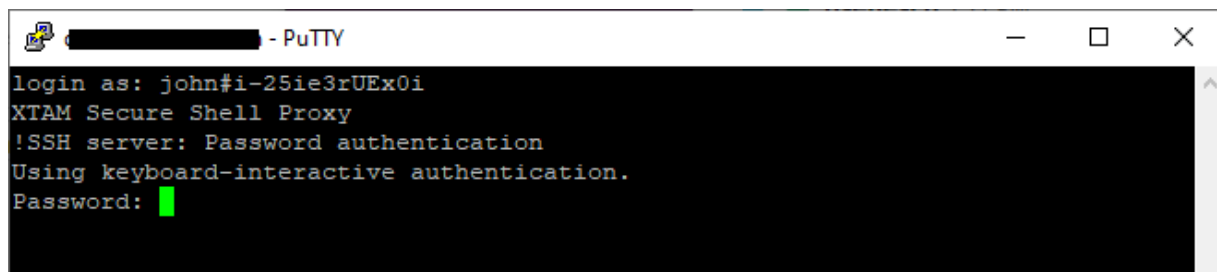
## Connecting Directly to a Managed Endpoint

In some scenarios, using the PAM SSH Proxy Interface can be more time consuming if you already know which record you want to connect to, or you have several saved.

For these situations, the SSH Proxy also supports direct connections to a specific record by bypassing the PAM SSH Proxy Interface all together.

**To connect directly to a record managing your ssh-enabled endpoint**, open your SSH client and enter the PAM host and port as provided to you by your System Administrator.

- At the user login prompt, you will enter a connection string as shown demonstrated in the example scenario below.
- We want to directly connect using our record with the name **Unix Production Server** and a record ID **i-25ie3rUEx0i**.
- At the SSH proxy login prompt, we will enter the string **john#Unix Production Server** or **john#i-25ie3rUEx0i** where *john* is our login name for PAM.
- Hit the Enter key and you will be greeted with the message *PAM Secure Shell Proxy* indicating that you are connecting to the PAM SSH Proxy.
- At the next prompt, enter your password, followed by the Enter key again and in a moment your SSH client will connect to the ssh-enabled endpoint stored in this record.



```
login as: john#i-25ie3rUEx0i
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password: █
```

NOTE: To connect directly using the record name, the name must be unique. If two or more records exist with the same name, then you must use the record ID to connect as that is always a unique value.

- When you are finished with your SSH proxy session, simply use your normal Exit or Logout command to complete your session.

## Connecting with an SSH Tunnel

The SSH Proxy feature in PAM can also be used to connect to an SSH Tunnel to make internal systems like databases, externally available through a native desktop client.

Connecting with an SSH Tunnel is an advanced option so we would encourage you to read our [SSH Tunnel](#) article for more information.



## Windows Remote PowerShell access

Custom port and protocol for Windows Remote PowerShell access options allow to execution of password reset and other remote job scripts on the servers with custom PowerShell port and protocol.

Define a custom port for password reset and job execution for Windows Remote PowerShell strategy using WinRM protocol by specifying the port number in the record type:

- ServicePort: **[Number]** (default 5985)

Define transport protocol for password reset and job execution for Windows Remote PowerShell strategy using WinRM protocol by selecting SSL option in a record type:

- EnabledSSL: **[Checkbox]** (default off)

## Joining an Active Web Session

When a remote System session is *Active*, other users' with the required permissions may join this session to monitor activities or to interactively participate in the session. Depending on this other user's permissions, they may either have an option to **Join** or an option to **Request Join**.

Regardless of which Join option is available, this user must have at least Record Control: Viewer and some level Session Control greater than None. Additionally, the option to Join will not be available if this other user is blocked due to a Workflow requirement on Session connect (Request Connect).

Join is only supported for web browser created sessions.

## To Join from the Record View

1. Login to PAM with a user that has at least Record Control: Editor and Session Control permissions to the record or is a System Administrator.
2. To the right of the Active Sessions entry along the top of the record, click the **Join** button for the *Active Session* you wish to join.

Please note there may be more than one active session to choose from.

### Production Server

#### Active Sessions

Michael Scott (user02) /Local





Dwight Schrute (user03) /Local

3. When the confirmation message appears, click the **OK** button to join the active session as an interactive participant.

## To Join from the Record's Session Report

1. Login to PAM with a user that has at least Editor and Session Control permissions to the record or is a System Administrator.
2. Click the **Sessions** tab along the bottom of this record.
3. Select the Active session in the list, click the **Actions** menu and then select the **Join** option.

Showing 1 to 50 of 70 entries

Record	User	Start Time	Completion Time	Status	Recording
Windows Host (internal)	Chris Kolodziejski (chrisk)	04/20/2018 11:58:00		Active	Not recording... 
Windows Host (internal)	Chris Kolodziejski (chrisk)	04/20/2018 11:56:24	04/20/2018 11:56:31	Completed	
Windows Host (internal)	Chris Kolodziejski (chrisk)	04/20/2018 11:43:06	04/20/2018 11:48:59	Completed	
Windows Host (internal)	Chris Kolodziejski (chrisk)	04/20/2018 10:59:00		Active	

Join

Terminate

Events

4. When the confirmation message appears, click the **OK** button to join the active session.

## To Request to Join from the Record View

When the requesting user only has Record Control: Viewer or Record Control: Unlock and some level of Session Control connectivity permissions, instead of a Join option they will be given the ability to Request Join.


When Request Join is selected, the session's Owner will receive a prompt that this user is requesting to join their session and they may either Allow or Deny this request.


- If allowed, the requested joiner will then have the option to Join as a view-only participant, meaning they may not interact with the session, but only monitor.
  - If denied, then they will be unable to join nor request again to join, this active session.
1. Login to PAM with a user that has Record Control: Viewer or Record Control: Unlock and Session Control permissions to the record.
  2. To the right of the Active Sessions entry along the top of the record, click the **Request Join** button for the Active Session you wish to join.

Please note there may be more than one active session to choose from.

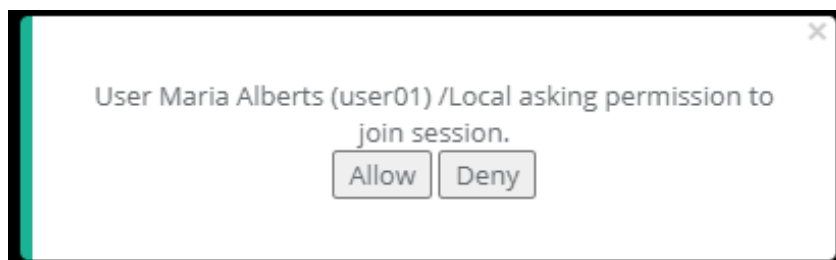
### Production Server

#### Active Sessions

Michael Scott (user02) /Local 

Dwight Schrute (user03) /Local 

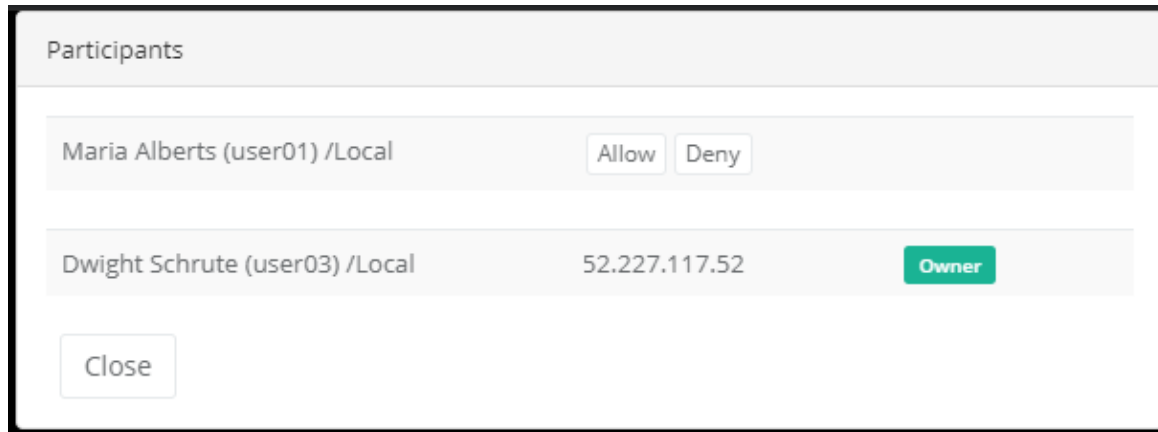
3. After the Request Join button is clicked, this active session's Owner will receive a prompt for them to either Allow or Deny the user's request to join their session. The requesting user must now wait until the session Owner chooses to allow or deny their request.



- If the session Owner clicks **Allow**, then the requester's *Request Sent* will change to *Join* and they may use it to join this session.

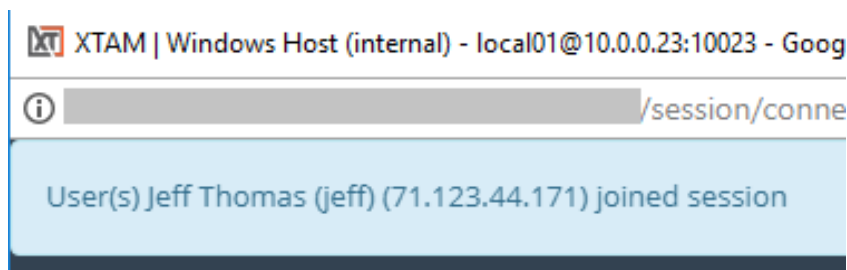
- If the session Owner clicks **Deny**, then the requester's *Request Sent* will change to *Join Denied* and they may not join nor request to join this active session again.

The request join prompt will appear in the session Owner's browser for about 10 seconds. If the selection is not made within this time period, then the session Owner can open the **Show Participants** panel from their session browser menu to locate the Allow or Deny buttons to make the desired selection for the requesting user.

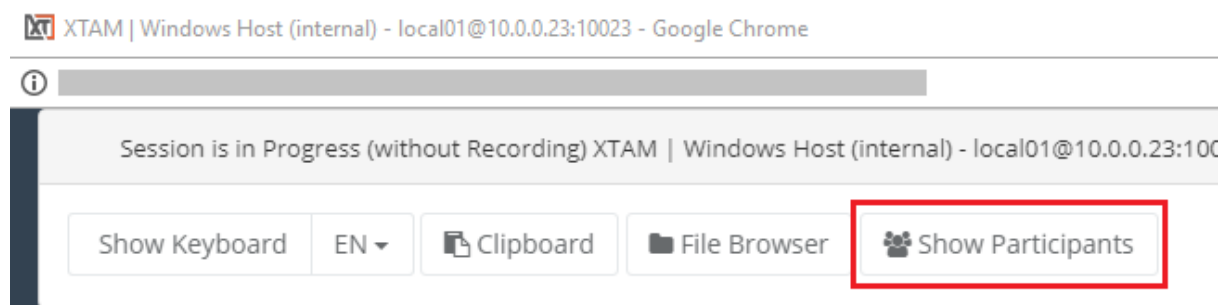


4. After the request is allowed, click the **Join** button, followed by the **OK** button on the confirmation dialog, to join this active session as a view only participant.

When a new user joins the Active session, all current participants will receive a notification alerting them to the new user's arrival.



From within the session, any user may also select the **Show Participants** option in their menu control to see the current list of participants in this session. The user who created the initial session will be marked as the Owner.



Participants

Chris Kolodziejski (chrisk)	71.123.44.171	Owner
John Williams (john)	71.123.44.171	
Jeff Thomas (jeff)	71.123.44.171	

Close

When a user leaves the session, all remaining participants will receive a notification alerting them to the user's departure. If the Owner leaves the session, then the session will automatically complete for all remaining users.

XTAM | Windows Host (internal) - local01@10.0.0.23:10023 - Google Chrome

User(s) John Williams (john) (71.123.44.171) left session

The arrival and departure of all participants is recorded and available as Audit events for all appropriately permission-ed users to review.

Showing 1 to 4 of 4 entries

User	Start Time	End Time	Type	Preview	Action
Jeff Thomas (jeff)	04/20/2018 11:48:46 ( +5m 40s )		SessionLeft	User left session	...
John Williams (john)	04/20/2018 11:47:19 ( +4m 12s )		SessionLeft	User left session	...
Jeff Thomas (jeff)	04/20/2018 11:44:34 ( +1m 28s )		SessionJoin	User joined session	...
John Williams (john)	04/20/2018 11:43:20 ( +13s )		SessionJoin	User joined session	...

First Previous 1 Next Last

## Session Joining as Request approver

If you have a Workflow Binding with an Action Connect control of the Record and Workflows with a template of the Interactive approval type, approvers of this Workflow template can Join the Session, regardless of their permissions to the records.

Even without the additional permissions, these approvers can Join a Session. Navigate to Management > My Workflows > My requests.

To join the active session:

1. Click **Details** to see all the information related to this session, which can be opened by the one who is a Request approver of the Request connect:

Workflows

Home / Workflow Instances

Requests for Approval

My Requests

Found 2 requests.

Request Time: Last Day Columns Saved filters

Show 50 entries Search:

CSV PDF XLSX PDF Protected CSV Protected XLSX Protected

Showing 1 to 2 of 2 entries

Request ID	Requester	Object	Requested Time	Approved	Request	Reason	Workflow Design	Approvers	Status
i-63vm3gJXxB	- ks4 /AD	unix	06/30/2021 16:28:30	06/30/2021 16:28:48	Connect:10	request connect	Step 1: Service Administrator (xtamadmin) /Local (1)	Service Administrator (xtamadmin) /Local: Approved 06/30/2021 16:28:48	Approved

2. If there is an active session there will be a **Join** button:

Workflow Instance

Home / Workflow Instance

Workflow Instance: interactive

Join -> 06/30/2021 16:30 Terminate

Request ID

i-63vm3gJXxB

Template

interactive

Created By

- ks4 (ks4) /AD

Requested By

- ks4 (ks4) /AD

Requested At

06/30/2021 16:28

Approved

06/30/2021 16:28

Requested Action

Connect

Reason

request connect

Object

unix

Approvers

Step 1: Service Administrator (xtamadmin) /Local at 06/30/2021 16:28 Approved

Workflow Design

Step 1: Service Administrator /Local (1)

3. Click the **Sessions** button that appears at the bottom of the page Workflow Instance to see the Session events or Session recording:

Reason	request connect
Object	unix

---

Approvers	Step 1: Service Administrator (xtamadmin) /Local at 06/30/2021 16:28 Approved
-----------	---

---

Workflow Design	Step 1: Service Administrator /Local (1)
-----------------	--

---

Status	Approved
Completed At	06/30/2021 16:28
Requested Time	10
Enabled From	06/30/2021 16:28
Enabled To	06/30/2021 16:38

---

Sessions

Cancel

## Video Recording

Privileged Access Management (PAM) Secure Session Video or Event Recordings.

PAM provides the ability to video record remote sessions (excluding HTTP(S) proxy and SSH Tunnel sessions) which then can be used to monitor or investigate all activity that has taken place during this session.

In combination with the Video recordings, PAM also generates [Keystroke and Clipboard recordings](#) that are can be used to quickly locate and “jump” to this event in the video itself.

Session Events are also overlayed on the Instant Video Playback timeline to ease the process of session recording investigations.

## Session Recordings

When supported, Session Recordings are available immediately after the Remote Session is completed and can be viewed with the following methods:

- **Instant Video Playback:** When applicable, this option will instantly play the recorded video directly in your browser without requiring a conversion or export operation.
- **Convert to AVI, Convert to MOV or Convert to MP4** (*Web browser created sessions only*): This option will convert the video into an `.avi`, `.mov` or `.mp4` video file so that it can be given to users outside of PAM.
- **Download (zip):** (*SSH Proxy sessions*) This option will download the typescript recorded session in a native format (individual metadata, timing and typescript files). These files can be used for playback using the native Linux scriptreplay command.
- **Download (zip):** (*HTTP Proxy sessions*) This option will download the HTTP proxy recorded session in a native `.har` format (HTTP Archive). These files can be used for review in an http archive viewer like [HAR Analyzer](#) or [HTTP Archive Viewer](#), among others.

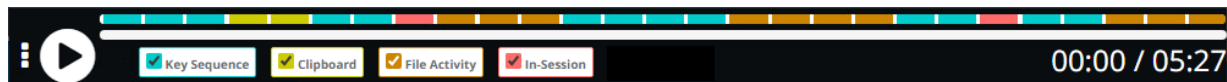
- **Jump to Recording:** From the Session Events report, use the **Jump to Recording** option to automatically open the video playback where the playhead will be placed at the beginning of this keystroke or clipboard event. This option is only available when the session was recorded.

Videos are captured at the resolution of the user's session so they may appear larger or smaller when played back on different resolutions (scrollbars or borders).

## Session Recordings with Event Overlay

Instant Video Playback displays the history of recorded session events in a bar located above the video playback timeline. This Session Event overlay bar displays each recorded session event from this session in a color-coded category as described below:

- Key Sequence events are shown in blue and includes:
  - KeySequence, CommandSequence, ShellInput, ShellExec, InputStream, OutputStream, AwsCliCommand
- Clipboard events are shown in yellow and includes:
  - Clipboard
- File Activity events are shown in orange and includes:
  - FileUpload, FileDownload, FileListing, SftpListDir, SftpUpload, SftpDownload, SftpRename, SftpRemove, SftpMkdir, SftpRmdir, ScpUpload, ScpDownload
- In-Session events are shown in red and includes:
  - SessionJoin, SessionLeft

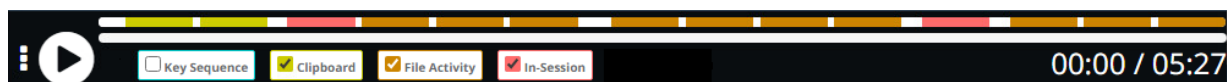


The session event category filters can be displayed or hidden with a single click to adjust which category of session events will be displayed in the overlay bar.

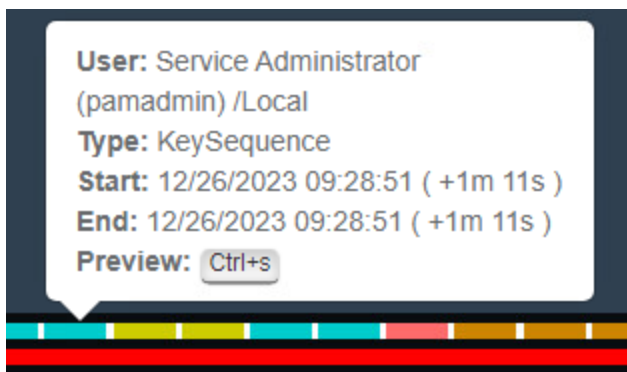
Each session event is displayed in equal width blocks with a small white space between each and ordered by event start time.

These event blocks are not intended to match the timestamps to the video playback, but rather display each event chronically as they were recorded during the user's session.

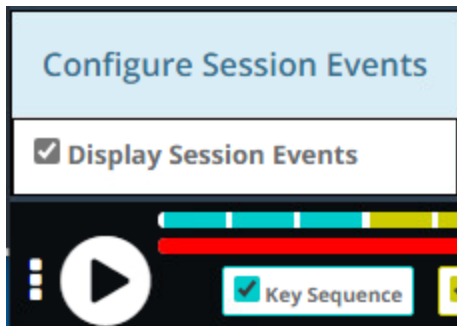
When a keyframe category is *disabled*, a larger white space (gap) may appear between other visible category blocks indicating the presence of these hidden events.



The viewer may hover over any session event in the overlay bar to see additional details about each event.



The viewer may use the vertical ellipsis button, to the left of the play button, to access the *Configure Session Events* menu to adjust options.



## PAM Permissions

[PAM Permissions](#) are used to define which sessions are recorded by default and which sessions have recording enabled via the user's choice.

When configuring your Session Control permissions, the following options are available for Principals (users or groups):

- **None**
  - The principal may not establish a remote session using this record.
- **Connect (Optionally recording without session events)**
  - The principal may establish a remote session using this record and can choose whether their session is video recorded or not. Session events (keystrokes, clipboard and file transfer) will not be recorded.
- **Connect (Always recording without session events)**
  - The principal may establish a remote session using this record and their session will always be video recorded. Session events (keystrokes, clipboard and file transfer) will not be recorded.
- **Connect (Optionally recording with session events)**
  - The principal may establish a remote session using this record and can choose whether their session is video recorded or not. Session events (keystrokes, clipboard and file transfer) will be recorded.
- **Connect (Always recording with session events)**
  - The principal may establish a remote session using this record and their session will always be video recorded. Session events (keystrokes, clipboard and file transfer) will be recorded.
- **Connect (No Recording with session events)**
  - The principal may establish a remote session using this record and their session will not be video recorded. Session events (keystrokes, clipboard and file transfer) will be recorded.



- **Connect (No Recording without session events)**
  - The principal may establish a remote session using this record and their session will not be video recorded. Session events (keystrokes, clipboard and file transfer) will not be recorded.
- **Convert to AVI, Convert to MOV, Convert to MP4**
  - This option will convert the video into an `.avi`, `.mov` or `.mp4` video file so that it can be given to users outside of PAM.

Please note that SSH Proxy recordings will only occur for users that have the *Always Recording* permission. Users with the *Optional Recording* permission will not be recorded.

Session Recordings are accessible from the following locations and requires an account with either *Owner*, *Auditor* or *System Administrator* privileges.

- **From the Record:** Open the Record and navigate to Sessions > Recording and use the Action button to choose your playback option.
- **From the Sessions Report:** Locate or Search for the Record and then use the Recording's Action button to choose your playback option.
- **From the Session Events Report:** Locate or Search for the Keystroke or Clipboard event and then use the Action button to select the Jump to Recording option.
- **From My Sessions:** Navigate to Management > My Sessions, locate or search for the Record and then use the Recording's Action button to choose your playback option.

By default, session recordings are stored in a directory within your PAM installation location.

If you would like to change this location to a new path (for example, a network share or external drive), please see the steps required [here](#).

## Session Recording Retention

All session recording video files are stored indefinitely, however if you would like to implement a retention schedule for these video recordings then please configure the option described below:

1. Login to PAM as a System Administrator
2. Navigate to Administration > Settings > Parameters > **Session Recording Retention**
3. Enter a value (defined in Days). PAM will delete all session video recordings after this specified number of days. A value of 0 (zero) will disable the retention schedule.
4. Click the **Save** button next to this option.

Please note that this retention schedule is applied **Globally** for all session video recordings and video recordings that have been purged due to this schedule cannot be recovered.

## Session Event Recording

PAM Remote Sessions with Video, Keystroke and Clipboard Recording.

When a user connects to a privileged system using a secure session in PAM it is also recording the user's keystrokes as well as any [clipboard text copies](#) that are made into the session (video can optionally be recorded too).

Keystroke and clipboard event recording is captured regardless of the video recording, so you can be sure that all sessions will have a searchable event report that can be used for investigations.

Any user that has the [PAM permission](#) to review Session History and Video recordings will also have access to the Keystroke and Clipboard events as well.

## Locating and reviewing a session’s Session Events

1. Login to PAM with a user account that has sufficient permissions and either open a record that you wish to review and open the All Sessions section located in Management > Sessions.
2. From within the Record view, click the **Session** tab.
3. Locate the Session that you would like to review, open its menu option under the Recording column and select **Events**.

System Sessions

Found sessions.

Time: Last Week ▾ State: Any ▾ Refresh

Show 

50 ▾

 entries Search:

Copy

CSV

Excel

PDF

Print

Showing 1 to 7 of 7 entries

Record ▴ ▾	User ▴ ▾	Start Time ▴ ▾	Completion Time ▴ ▾	Status ▴ ▾	Recording ▴ ▾
<a href="#">Windows Host (internal)</a>	Chris Kolodziejski (chrisk)	12/07/2017 13:57:51	12/07/2017 14:10:19	Completed	Not recorded <div>⋮</div>
<a href="#">Windows Host (internal)</a>	Chris Kolodziejski (chrisk)	12/07/2017 13:54:44	12/07/2017 13:56:22	Completed	Events <div>⋮</div>
<a href="#">Windows Host (internal)</a>	Chris Kolodziejski (chrisk)	12/06/2017 10:34:59	12/06/2017 10:41:47	Completed	Available. <div>⋮</div>
<a href="#">Windows Host (internal)</a>	Chris Kolodziejski (chrisk)	12/01/2017 10:14:13	12/01/2017 10:14:25	Completed	Not recorded <div>⋮</div>

4. The Session Events view will open displaying all keystroke and clipboard text that were entered during this session.

User	Start Time	End Time	Type	Preview
Chris Kolodziejcki (chrisk)	12/07/2017 18:02:09	12/07/2017 18:02:22	KeySequence	<div> <div>Shift+S</div> <div>e</div> <div>s</div> <div>s</div> <div>i</div> <div>o</div> <div>n</div> <div>Space</div> <div>Shift+K</div> <div>e</div> <div>y</div> <div>s</div> <div>t</div> <div>r</div> <div>o</div> <div>k</div> <div>e</div> <div>Space</div> <div>a</div> <div>n</div> <div>d</div> <div>Space</div> <div>Shift+C</div> <div>i</div> <div>p</div> <div>b</div> <div>o</div> <div>a</div> <div>r</div> <div>d</div> <div>Space</div> <div>Shift+R</div> <div>e</div> <div>c</div> <div>o</div> <div>r</div> <div>d</div> <div>i</div> <div>n</div> <div>g</div> <div>Enter</div> </div> <p>Session Keystroke and Clipboard Recording</p>
Chris Kolodziejcki (chrisk)	12/07/2017 18:02:38		Clipboard	This text was copied in from the remote session's clipboard
Chris Kolodziejcki (chrisk)	12/07/2017 18:02:41	12/07/2017 18:02:41	KeySequence	<div> <div>Enter</div> </div>
Chris Kolodziejcki (chrisk)	12/07/2017 18:02:42	12/07/2017 18:02:43	KeySequence	<div> <div>Ctrl+v</div> <div>Enter</div> </div>
Chris Kolodziejcki (chrisk)	12/07/2017 18:02:44	12/07/2017 18:02:44	KeySequence	<div> <div>Enter</div> </div>
Chris Kolodziejcki (chrisk)	12/07/2017 18:02:50	12/07/2017 18:02:54	KeySequence	<div> <div>g</div> <div>e</div> <div>t</div> <div>-</div> <div>p</div> <div>r</div> <div>o</div> <div>c</div> <div>e</div> <div>s</div> <div>Enter</div> </div> <p>get-process</p>
Chris Kolodziejcki (chrisk)	12/07/2017 18:03:02	12/07/2017 18:03:12	KeySequence	<div> <div>t</div> <div>h</div> <div>a</div> <div>t</div> <div>Space</div> <div>w</div> <div>a</div> <div>s</div> <div>Space</div> <div>e</div> <div>x</div> <div>e</div> <div>c</div> <div>u</div> <div>t</div> <div>e</div> <div>d</div> <div>Space</div> <div>t</div> <div>h</div> <div>r</div> <div>o</div> <div>u</div> <div>g</div> <div>h</div> <div>Space</div> <div>a</div> <div>Space</div> <div>Shift+P</div> <div>o</div> <div>w</div> <div>e</div> <div>r</div> <div>Shift+S</div> <div>h</div> <div>e</div> <div>l</div> <div>l</div> <div>Space</div> <div>c</div> <div>o</div> <div>m</div> <div>m</div> <div>a</div> <div>n</div> <div>d</div> <div>Enter</div> </div> <p>that was executed through a PowerShell command</p>
Chris Kolodziejcki (chrisk)	12/07/2017 18:03:12	12/07/2017 18:03:12	KeySequence	<div> <div>Enter</div> </div>
Chris Kolodziejcki (chrisk)	12/07/2017 18:03:16	12/07/2017 18:03:39	KeySequence	<div> <div>a</div> <div>n</div> <div>d</div> <div>Space</div> <div>t</div> <div>h</div> <div>i</div> <div>s</div> <div>Space</div> <div>r</div> <div>e</div> <div>c</div> <div>o</div> <div>r</div> <div>d</div> <div>i</div> <div>n</div> <div>g</div> <div>Space</div> <div>w</div> <div>o</div> <div>r</div> <div>k</div> <div>s</div> <div>Space</div> <div>l</div> <div>i</div> <div>n</div> <div>Space</div> <div>Shift+U</div> <div>n</div> <div>i</div> <div>x</div> <div>Space</div> <div>Shift+L</div> <div>i</div> <div>n</div> <div>u</div> <div>x</div> <div>Space</div> <div>Shift+T</div> <div>e</div> <div>l</div> <div>n</div> <div>e</div> <div>n</div> <div>t</div> <div>Space</div> <div>a</div> <div>n</div> <div>d</div> <div>Space</div> <div>o</div> <div>t</div> <div>h</div> <div>e</div> <div>r</div> <div>Space</div> <div>r</div> <div>e</div> <div>m</div> <div>o</div> <div>t</div> <div>e</div> <div>Space</div> <div>s</div> <div>e</div> <div>s</div> <div>s</div> <div>i</div> <div>o</div> <div>n</div> <div>s</div> <div>Space</div> <div>a</div> <div>s</div> <div>Space</div> <div>w</div> <div>e</div> <div>l</div> <div>l</div> <div>Space</div> <div>Shift+I</div> <div>Space</div> <div>Space</div> <div>Shift+P</div> <div>r</div> <div>e</div> <div>t</div> <div>y</div> <div>Space</div> <div>Backspace</div> <div>Backspace</div> <div>t</div> <div>y</div> <div>Space</div> <div>c</div> <div>o</div> <div>d</div> <div>l</div> <div>Space</div> <div>Shift+)</div> <div>Shift+)</div> <div>Enter</div> </div> <p>and this recording works in Unix, Linux, Telnet and other remote sessions as well! Pretty cool :)</p>

5. If the session is completed and it was recorded, you can use the **Jump to Recording** option located in the **Action** menu to automatically open the in-browser video player and jump to this event.

# Recording enforcement for Personal Vaults

The System Administrator is able to require session and session events recording for all assets created in User's Personal Vaults.

The option enables control over the devices in isolated data-centers, air gap networks or Virtual Private Clouds even for the users using personal accounts with privileged access.

Two global parameters are located in the Administration > Settings > Parameters > Sessions category: Personal Vault Session Recording and Personal Vault Event Recordings.

When set to **Enforced** these parameters overwrite the default records permission scheme to enforce sessions or session events recordings.

# Session Event Masking

In some situations, it may be necessary for a user to type or paste a password during a recorded remote session.

Although such actions are not recommended, unfortunately it might be required. As a result, session event recording, when enabled, will capture such *KeySequence* and *Clipboard* events and display this password in its report, potentially viewable by other privileged PAM users.

In an attempt to prevent user typed passwords from being visible in a Session Events Report, PAM can apply a password detection algorithm to the content of the report.

This feature attempts to detect single word events that most likely are a password and in response, mask them from the report making it unviewable by all users.

## Masking Conditions

Before you consider enabling this feature, you should understand how the algorithm processes perceived passwords and the conditions in the function.

When enabled and a [Session Event Report](#) is accessed, the Password Detection Entropy is applied to all events captured in the report, using the following conditions, before it is viewable:

- It will evaluate *KeySequence* and *Clipboard* events for potential masking. *KeySequence* events represent keystroke recording or someone using a keyboard during a remote session to input text, while a *Clipboard* event would represent someone pasting a potential password into a session. This will work for any PAM remote session that supports native event recording including RDP web or proxy and SSH web or proxy types.
- It will only evaluate single word events. This means that if an event contains multiple words, then it is not evaluated and this entire *KeySequence* or *Clipboard* event will remain unmasked. Single word events are more likely to be a user typing in a password at a prompt or pasting one into a session using the clipboard, followed by an **Enter** or **Tab** command rather than a series of words likely representing commands or parameters.
- It will only evaluate single word events that are longer than 8 characters. Even a minimally secure password should be at least 9 characters long so the likelihood of a 4- or 6-character string being a password is significantly less. *If you use passwords that are less than 9 characters, we strongly recommend you increase the length and complexity of your password policy for many reasons beyond the use of this feature.*


If all the above conditions are satisfied, the [Password Detection Entropy](#) algorithm will be applied to the recorded Session Event.

## Password Detection Entropy Configuration

When the algorithm detects a perceived password in the Session Event Report, it will prevent the password event from appearing in the report and instead, display a series of asterisks indicating that it is a masked event. This prevents all users from viewing the recorded event.

### *To configure Password Detection Entropy:*

1. Login to PAM using a System Administrator account. [Only System Admins](#) may enable/disable and configure this feature.
2. Navigate to Administration > Settings > Parameters > Password Detection Entropy.
3. Set a numerical value into this parameter and click its **Save** button. The next section of this guide describes the concept of this value.



Password Detection Entropy 35 ? Save

4. Open a [Session Events Report](#) to evaluate the results and adjust the entropy value as required. If adjustments are required because a known password is visible or non-password values are masked, change the value, click the **Save** button again and refresh the report to see the updated results. You do

not have to create newly generated *Session Events* to observe the results of an updated entropy value.

Tip: If a known password is unmasked, your entropy value is too large and should be decreased to adjust for the less complex nature of that password. If a known password is masked and known non-password events are also masked, your entropy value is too small and should be increased to find the middle ground between the two (i.e., password masked, non-password unmasked). There is a mix of art and science (and trial and error) in determining the appropriate value for your password detection.

## Entropy Value Description

There is no universally *correct* entropy value, so expect a bit of trial and error in finding your middle ground. To understand how the numerical range operates, let us begin with the value.

First, to disable this feature enter a 0 (zero) value into this parameter and click **Save** (disabled is the default state).

When disabled, no *Session Events* will be processed, and all recorded events will be visible in the report.

When any value greater than 0 is saved to the parameter, the feature will be enabled, and the supplied value will be used.

Now, how to determine which value to use must be understood in conjunction with the algorithm, beginning with the previously mentioned conditions. When a single word *KeySequence* or *Clipboard* event greater than 8 characters is present in a [Session Events report](#), the algorithm assumes it is a password regardless of the parameter's non-zero value.

It starts evaluating with the assumption that it is a password and not, for example, a PowerShell or Linux command.

Next, it processes the strength of this perceived password using the value entered to this entropy parameter.

This considers the probability that it is a password, and not a command, based on characteristics like randomized characters, dictionary checks and several other methods.

As a result of the processing of the event, the algorithm generates a numerical value for each of these events relative to its complexity.

If the resulting numerical value of the processed event is greater than the Entropy parameter, PAM determines it is a password and is therefore masked from the report.

Conversely, if the numerical result of the processing is less than the Entropy value, PAM determines it is not a password and therefore is not masked.

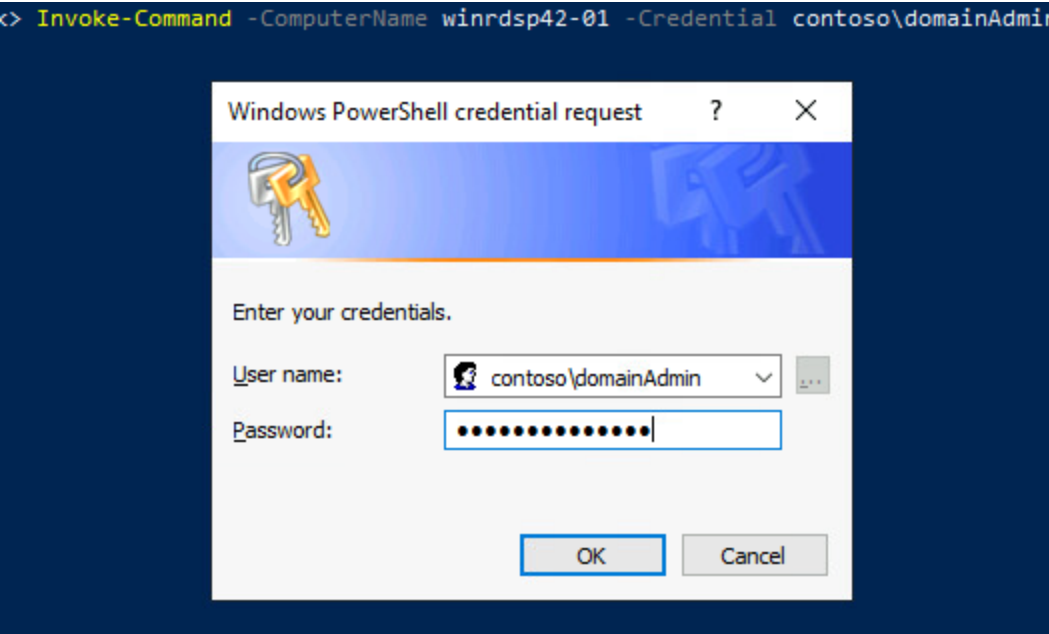
To further illustrate this, use the example of an Entropy value set to 50. If a single word event is processed and returns a value of 15, PAM determines this is not a password because if it were, it would represent a very 'weak' password and therefore likely it is a command that should not be masked.

However, an event that returns a value of 80 would indicate that this value is complex compared to a 50 valued event and therefore highly unlikely, under these conditions, to be anything but a password so it is masked.

The "trial and error" aspect of determining the ideal Entropy value is required so that it masks passwords and does not make other non-password events. And if such an exact middle ground value does not exist, then considerations would need to be made to determine if a lower value would be more ideal to ensure passwords are masked with the understanding that some other single word non-password events may also be masked.

## Password Detection Entropy Example

The following example intends to provide a demonstration of this feature. A user starts a remote Windows session (RDP) where session event recording is enabled. When running a PowerShell command, the user is presented with a password prompt where they type in the required password to execute the command.



Due to the user's session having event recording enabled, this event is captured and included in the [Session Events report](#) displaying the password they typed in the prompt.

Service Administrator (pamadmin) /Local	12/21/2022 14:22:35 ( +49s )	12/21/2022 14:22:49 ( +1m 2s )	KeySequence	Q t w @ 3 n G 9 7 # n J s 2
				Qtw@3nG97#njs2

However, with a Password Detection Entropy of 60 applied, this single word event is determined to be a strong password and is masked from the report, while the remaining non-password event, the PS command, remains unmasked.

Service Administrator (pamadmin) /Local	12/21/2022 14:22:35 ( +49s )	12/21/2022 14:22:49 ( +1m 2s )	KeySequence	*****
Service Administrator (pamadmin) /Local	12/21/2022 14:21:54 ( +7s )	12/21/2022 14:22:25 ( +38s )	KeySequence	Invoke-Command -ComputerName winrdsp42-01 -Credential contoso\domainAdmin -Scriptblock {dir /}
Invoke-Command -ComputerName winrdsp42-01 -Credential contoso\domainAdmin -Scriptblock {dir /}				

A similar example could be presented with login credentials used for a website on a remote session or during a SSH session where a user who knows the root or sudo password and types it when prompted.

The Password Detection Entropy feature is applied to the [Session Events report](#) meaning any PAM remote session protocol or type can support password masking.

```

01:~$ sudo adduser demouser123
[sudo] password for :
Adding user `demouser123' ...
Adding new group `demouser123' (1026) ...
Adding new user `demouser123' (1026) with group `demouser123' ...
Creating home directory `/home/demouser123' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for demouser123
Enter the new value, or press ENTER for the default
  Full Name []: Demo
  Room Number []:
  Work Phone []:

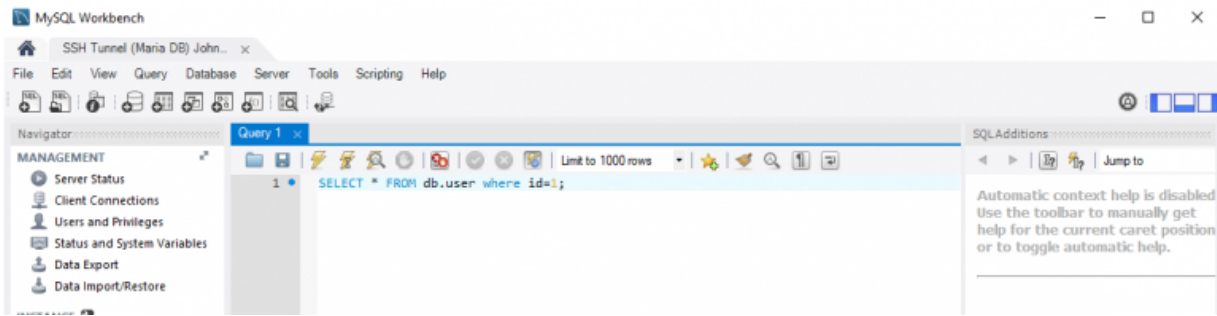
```

(pamadmin) /Local					
Service Administrator (pamadmin) /Local	12/21/2022 15:02:52 ( +54s )	12/21/2022 15:03:05 ( +1m 7s )	KeySequence	s u d o Space a d d u s e r Space d e m o u s e r 1 2 3 Enter	...
				sudo adduser demouser123	
Service Administrator (pamadmin) /Local	12/21/2022 15:03:09 ( +1m 11s )	12/21/2022 15:03:12 ( +1m 15s )	KeySequence	*****	...
Service Administrator (pamadmin) /Local	12/21/2022 15:03:28 ( +1m 31s )	12/21/2022 15:03:37 ( +1m 39s )	KeySequence	*****	...
Service Administrator (pamadmin) /Local	12/21/2022 15:03:45 ( +1m 47s )	12/21/2022 15:03:50 ( +1m 52s )	KeySequence	*****	...
Service Administrator (pamadmin) /Local	12/21/2022 15:04:54 ( +2m 57s )	12/21/2022 15:04:55 ( +2m 58s )	KeySequence	D e m o Enter	...
				Demo	

## SQL Traffic Recording

PAM Session Event recording enables the ability to save SQL statements to the Session Events Logs when connecting to a MySQL or MS SQL Server database through the use of a SSH Proxy tunnel using native clients such as MySQL Workbench, MS SQL Studio, command line SQL prompts or other client applications.

The option to record this SQL traffic helps management and auditors to understand typical administration activities, alert stakeholders about suspicious queries or to comply with regulations.



The traffic recording option is enabled automatically for PAM channels opened through the SSH Tunnel using the database's standard ports (port 3306 for MySQL and port 1433 for MS SQL).

It is also possible to provide hints to the SSH Tunnel to enable traffic monitoring established over non-standard ports.

See the section below named *Capturing SQL Traffic from PAM SSH Tunnel Sessions Over Non-Standard Ports* for configuration.

The traffic recording option is enabled by PAM's Session Control Recording roles.

To capture the SQL traffic of a user or group, simply assign one of the [Session Control](#) levels that include the with [Session Events](#) options.

More information about PAM Permission Levels can be found [here](#).

#### [Capturing SQL Traffic from PAM SSH Tunnel Sessions Over Standard Ports](#)

The following section describes how to enable SQL Traffic to be recorded to a session's Session Event report when the tunnel is using standard ports (for example, port 3306 for MySQL or port 1433 for MS SQL).

It is assumed that an [SSH Tunnel session](#) is already configured properly in PAM.

#### [Capturing SQL Traffic from PAM SSH Tunnel Sessions Over Non-Standard Ports](#)

## RDP Client Proxy Sessions

Privileged Access Management (PAM) can create quick, easy and secure native client high-trust logins using your own desktop or mobile RDP client like Windows RDP client (MSTSC), Mac RDP client, Remote Desktop Connection Manager and mRemote while enforcing audit events, notifications, permissions, access request and password rotation.

Unlike other products, the PAM RDP Proxy provides this without having to download, install or maintain any custom launchers, agents or deployment packages to your computer or device.

Now your privileged users can securely connect to your managed Windows endpoints over RDP without disclosing passwords:

1. Using their native Web browser (desktop or mobile) without installing any custom launchers, agents or packages.
2. Using their native RDP client (desktop or mobile) without installing any custom launchers, agents or packages.



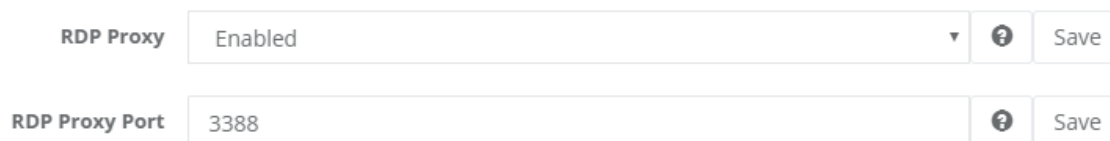
Secured passwords are never sent or synced to the user's computer or mobile device. PAM maintains complete and total control of all passwords while the user connects to the managed endpoint and it can even reset the password after the user's session has completed.

To learn about how PAM can provide secure SSH Proxy access using native SSH clients, please read our [SSH client](#) article.

The following sections describe how to create secure Windows Host RDP records in PAM and then how to use these records in your native desktop or mobile clients.

## Enabling RDP Proxy

1. Login to PAM with a System Administrator account.
2. Navigate to Administration > Setting > Parameters.
3. Locate and modify the following settings:
  - a. **RDP Proxy:** Switch this option to *Enabled* and click the **Save** button to its right;
  - b. **RDP Proxy Port:** Use or change the port value that the System will use for RDP proxy and click the **Save** button to its right.



The screenshot shows two configuration fields. The first field, labeled 'RDP Proxy', has a dropdown menu set to 'Enabled' and a 'Save' button to its right. The second field, labeled 'RDP Proxy Port', has a text input containing '3388' and a 'Save' button to its right. Both fields have a question mark icon to the left of the 'Save' button.

4. Once both settings have been updated and saved, restart the **PamManagement** service (Windows) or **pammanager** service (Unix/Linux).
5. When the services is fully restarted (can take 1-5 minutes), the RDP proxy module is online.

## Session record

Creating a RDP session record in PAM:

1. In PAM, navigate to a Vault or Container and create a new record using the **Windows Host** record type.
2. Populate all the fields with your endpoint's connection details.
3. Click the **Save and Return** button.

Your record is now saved and under management in PAM.

All access to this record will be captured in the audit log, including Active and Completed sessions.

Permissions and workflows can also be applied to your users or groups ensuring that only authorized personnel have access to the record.

## RDP session record in a native Client

Use your RDP session record in a native RDP Client.

You can create your remote session in your native RDP client using one of two methods.

The first method is to populate your connection parameters into the client manually and the second method is to download a remote desktop file that already contains your Host and User values.

If you choose to download the remote desktop file, then you can skip to step 5 in this section.

Please note that for MFA authentication, your User value will need to be updated to contain the MFA token or MFA type as described below.

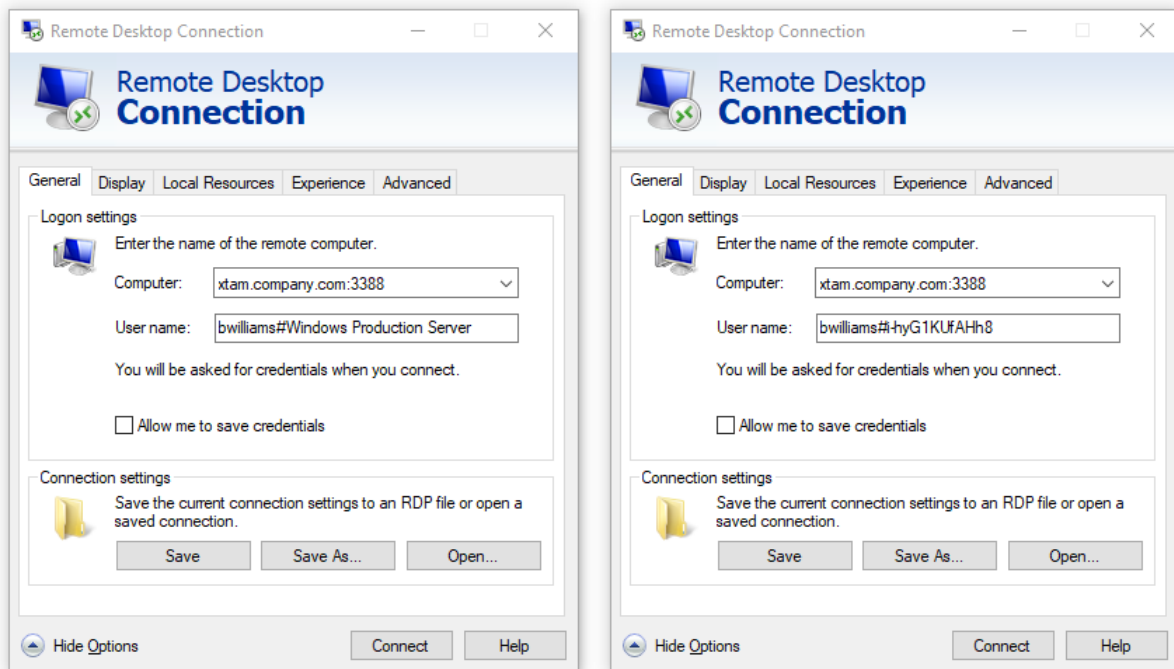
1. If you are currently logged into PAM, please logout and log back in to the web portal. Any users that wish to connect using the RDP Proxy must sign in to PAM web portal once so their account can be automatically registered for this feature. They only need to do this login once, not every time they wish to connect with the RDP Proxy.
2. Open your local RDP client (we will use the native Windows 10 RDP client in our example but most other RDP clients function similarly) and create a new session.
3. In the **Computer** field, enter the hostname of your PAM server followed by the configured RDP proxy port. For example, **xtam.company.com:3388**.
4. In the User name field, enter a user string as described below:

**YourPAMLoginName#PAMrecordName or YourPAMLoginName#PAMrecordID**

For example, if your login to the System was the username bwilliams and PAM record that contains the Windows Host RDP details has the name Windows Production Server and ID *i-hyG1KUfAHh8*, then the login string would be

**bwilliams#Windows Production Server or bwilliams#i-hyG1KUfAHh8**

When using the record Name to define the connection string, the record Name must be unique in PAM. If the name is not unique, the connection will fail and you must use its record ID instead.



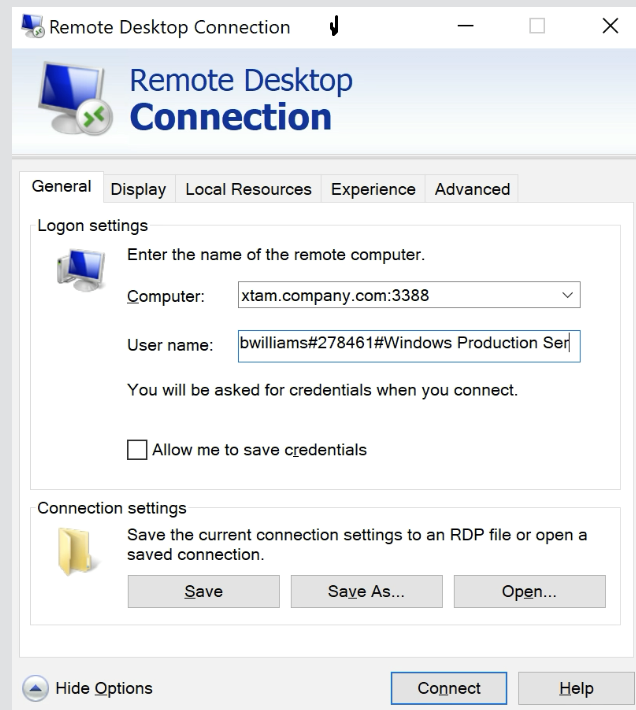
A # (hash), % (percent) or : (colon) character may be used as a separate between the login and recordID values. The record's ID can be found in the records's URL or when viewing the record's Details ([https://xtam.company.com/xtam/#/records/record\\_view/i-hyG1KUfAHh8/type](https://xtam.company.com/xtam/#/records/record_view/i-hyG1KUfAHh8/type)).

For users that are required to authenticate using MFA, your connection string for the *Username* name needs to include your MFA token or type. Please use the following examples to illustrate MFA connection strings.

- For TOTP like Google Authenticator or RADIUS like RSA, the Username string will follow this pattern:

PAM Username#Your MFA code#Unique PAM Record Name or ID

**bwilliams#278461#Windows Production Server**



The **278461** represents an example of your TOTP token.

- For Duo Security, the Username string will follow this pattern:

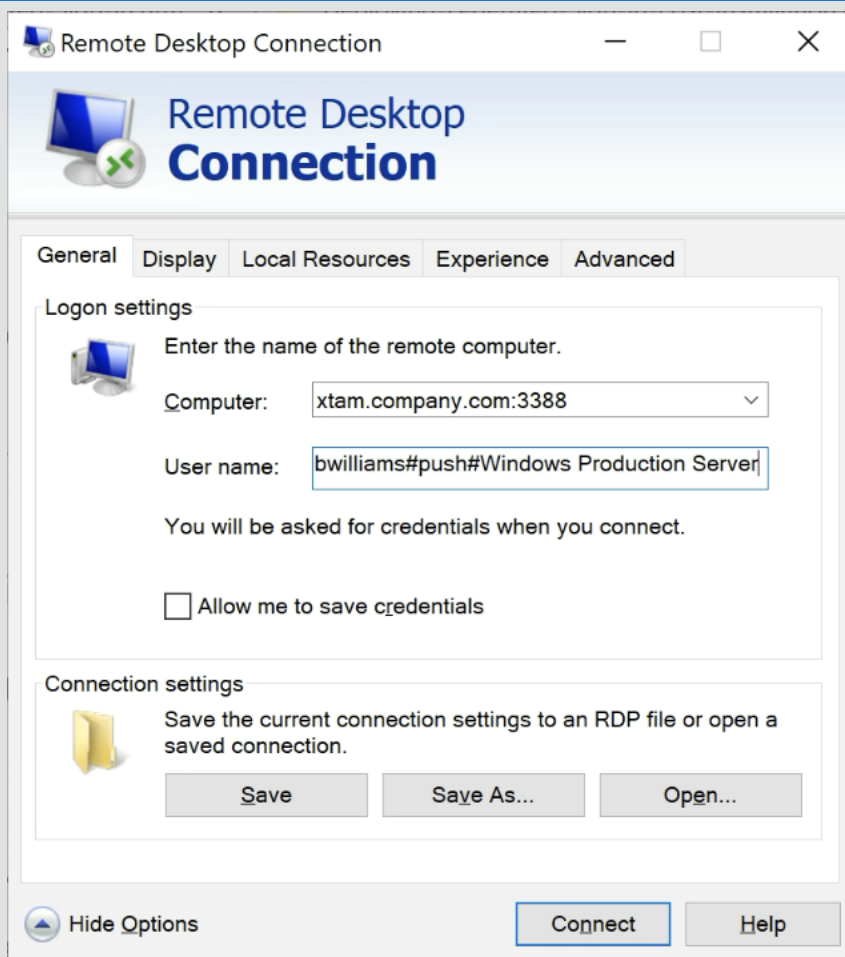
PAM Username#Duo type or passcode#Unique PAM Record Name or ID

**bwilliams#auto#Windows Production Server**

**bwilliams#push#Windows Production Server**

**bwilliams#phone#Windows Production Server**

**bwilliams#397623#Windows Production Server**

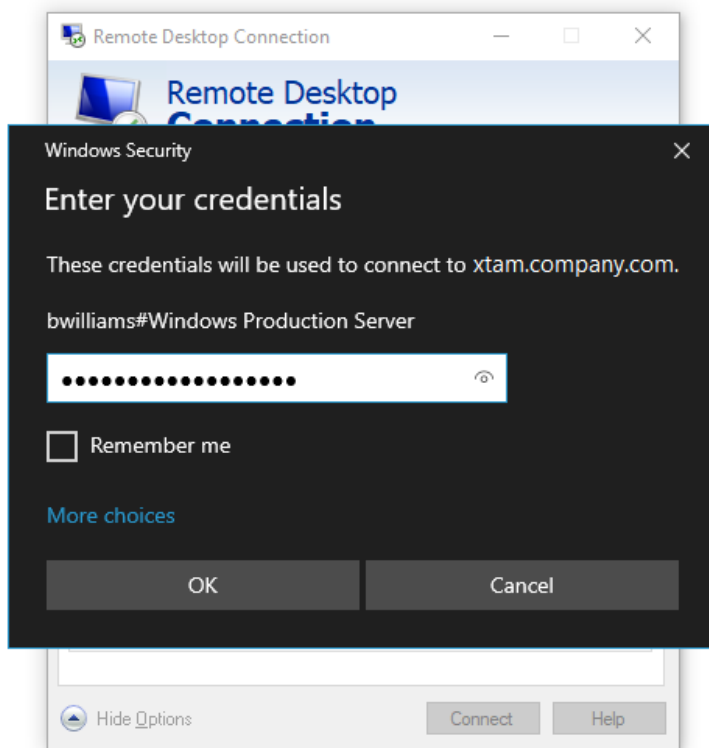


The *auto* type will use your default Duo method, the *push* type will send a Duo Push to your registered device, the *phone* type will generate a phone call to your registered device and the **397623** represents an example your unique Duo Passcode. SMS is not supported because there is no prompt to enter the code after it is generated.

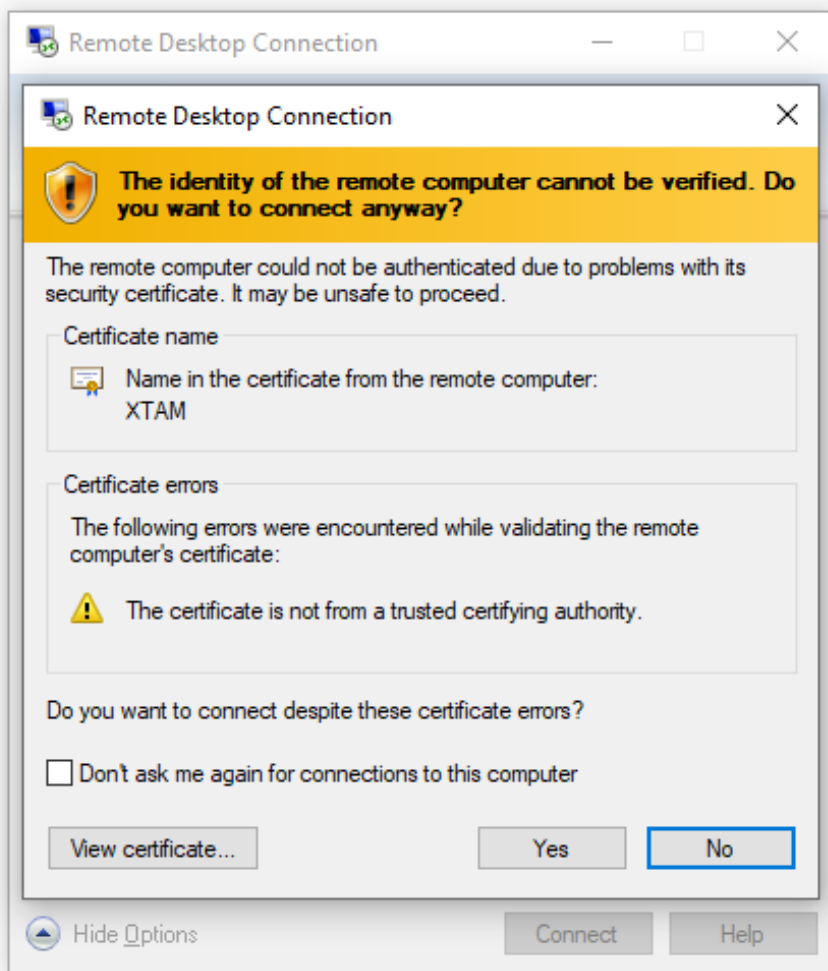
Please note when using either the *auto*, *push* and *phone* options, the connection process of the RDP Proxy will pause until you Approve the Duo challenge on your registered device.

5. Now, click the **Connect** button in your client.
6. Enter the password for your PAM user account when prompted and click **OK**.

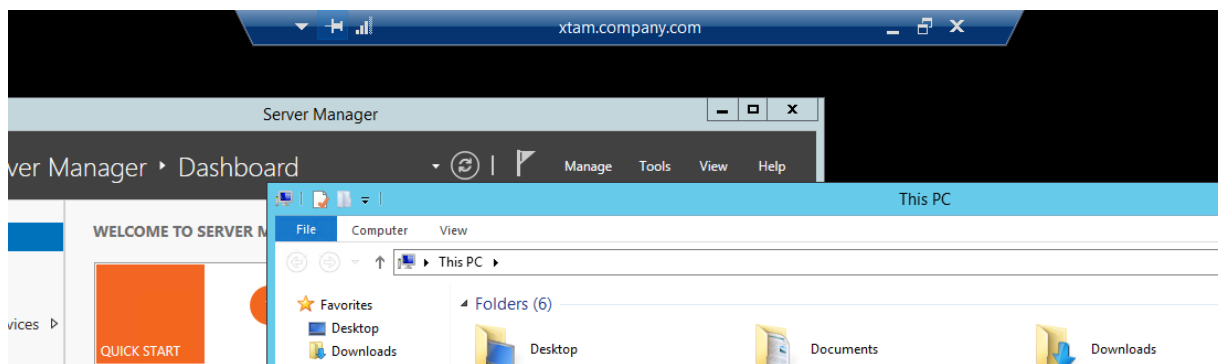
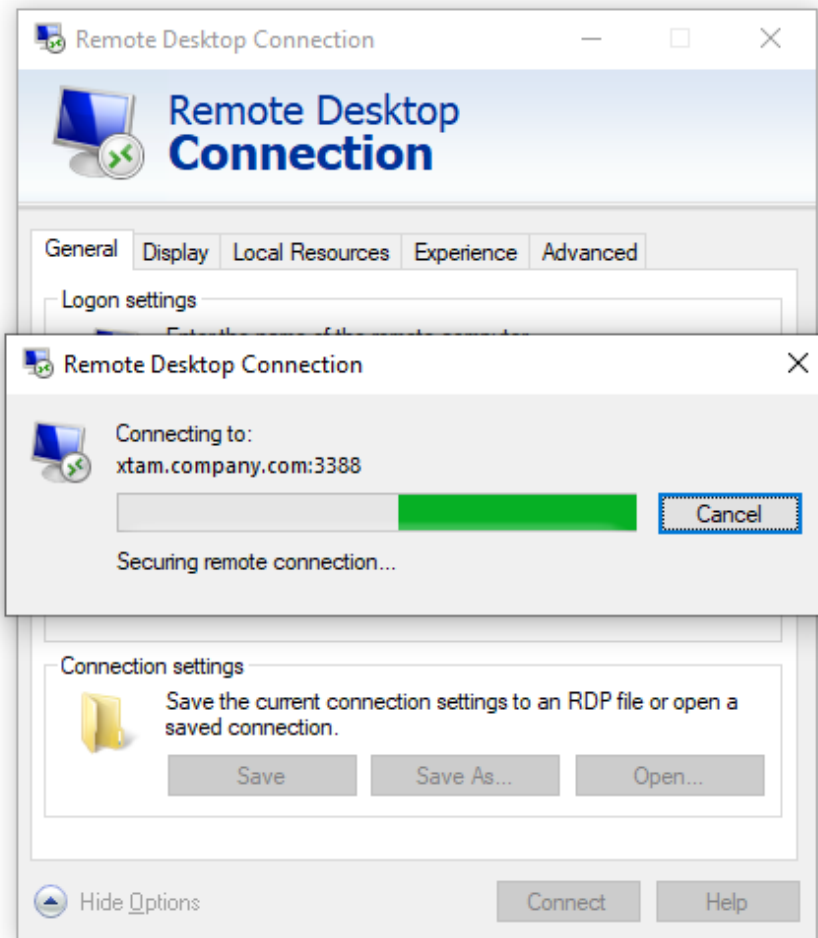
Note that you will be connecting to the PAM server rather than directly to this Windows endpoint.



7. Confirm the PAM security certificate by clicking the **Yes** button.



8. After a few moments, you will be connected to the remote RDP endpoint using the secured connection details in the referenced PAM record.





9. To confirm that the session is being provided via PAM, you can navigate to the Session tab of this record and note that there is now an Active session using this record. When you end the session using the native *Disconnect* or *Sign Out* options, the session will be reported as *Completed*.



System Sessions

Found 1 sessions.


Time: Last Day State: Any Columns  

Show 50 entries

Search:

CSV PDF

Showing 1 to 1 of 1 entries

Record	User	Start Time	Completion Time	Type	Status	ID	Recording
<a href="#">Windows Production Server</a>	Brian Williams (bwilliams) /Local	11/29/2019 10:34:26	11/29/2019 10:38:17	RDPP	Completed	i-dWcXogvSTjy	Not recorded 

First

Previous

1

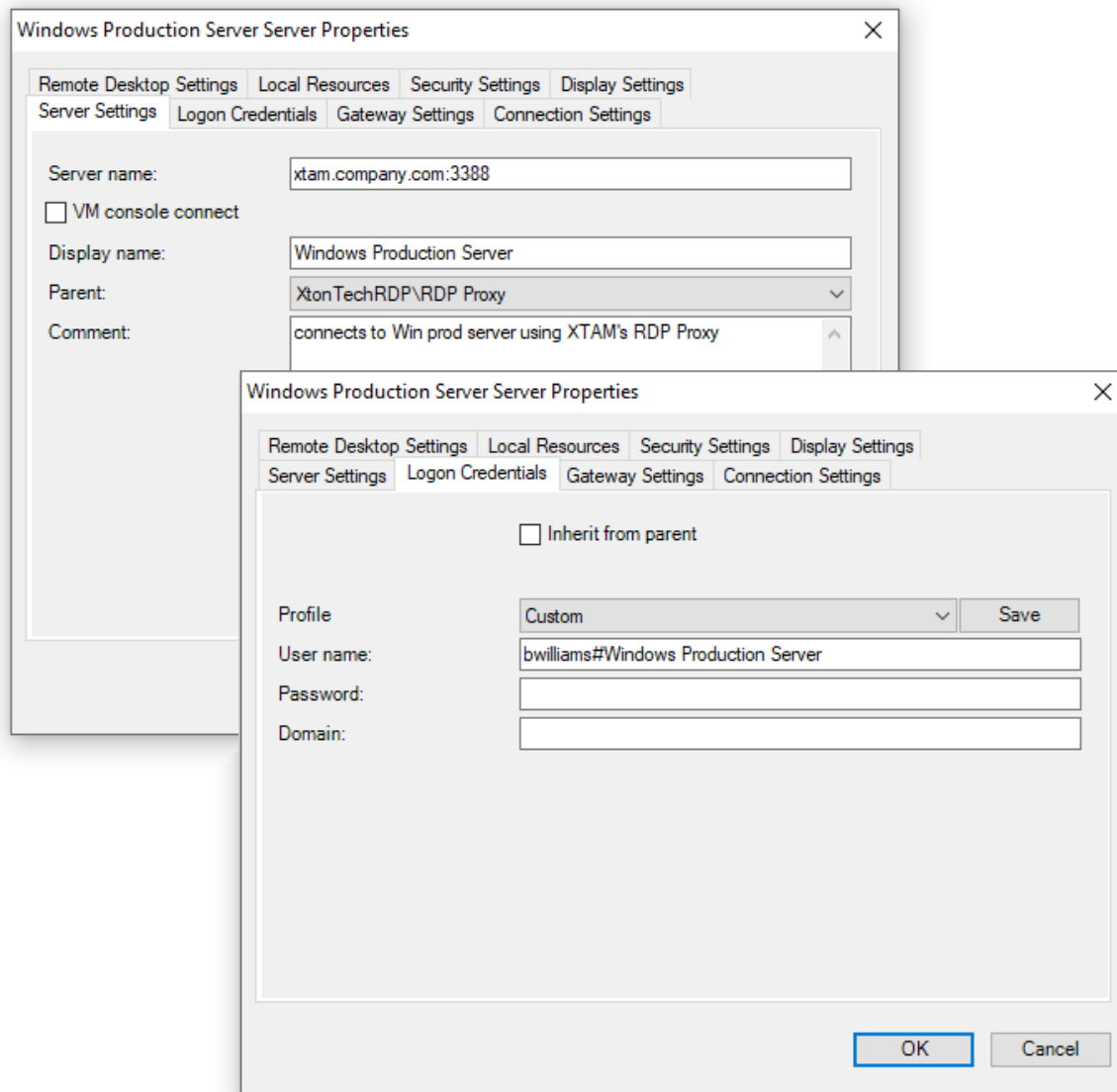
Next

Last

Note that the **Type** *RDPP* indicates a RDP Proxy Session whereas the **Type** *RDP* indicates a *RDP Web Session*.

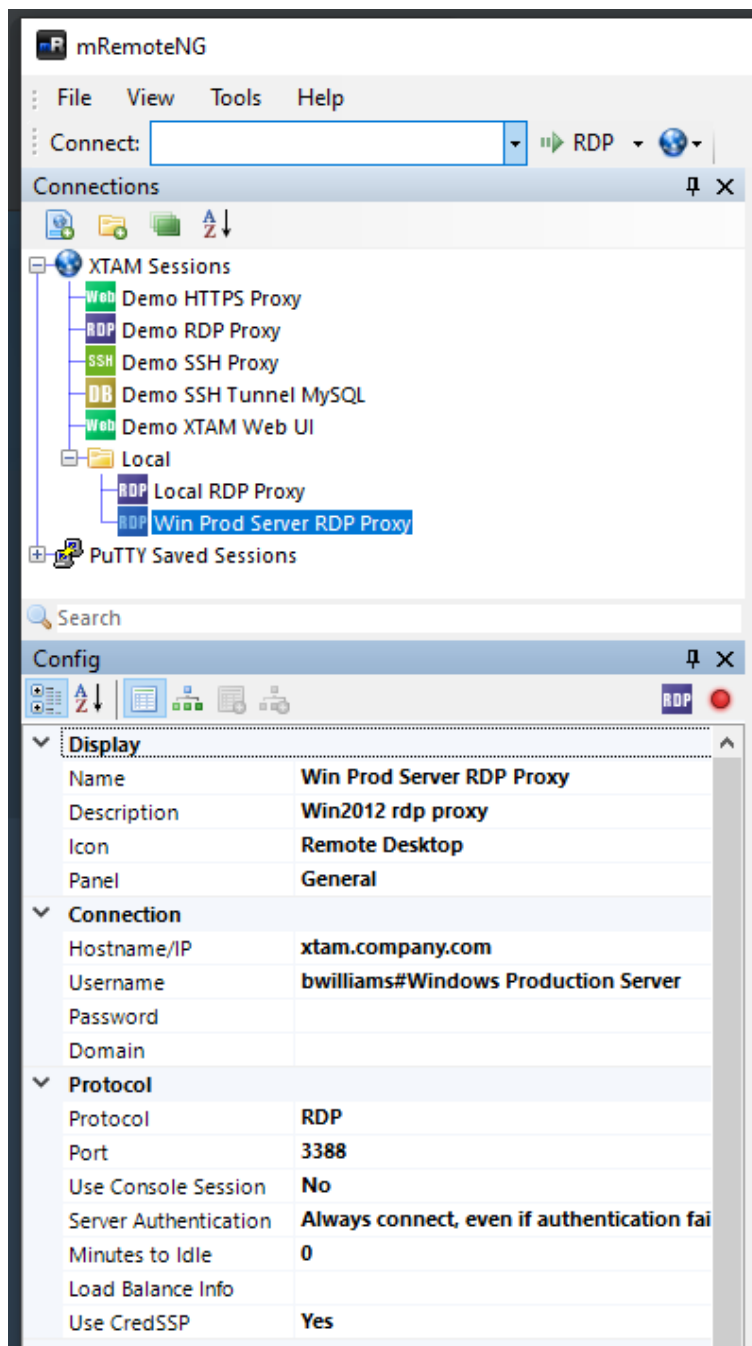
Example: Remote Desktop

Example using Remote Desktop Connection Manager.



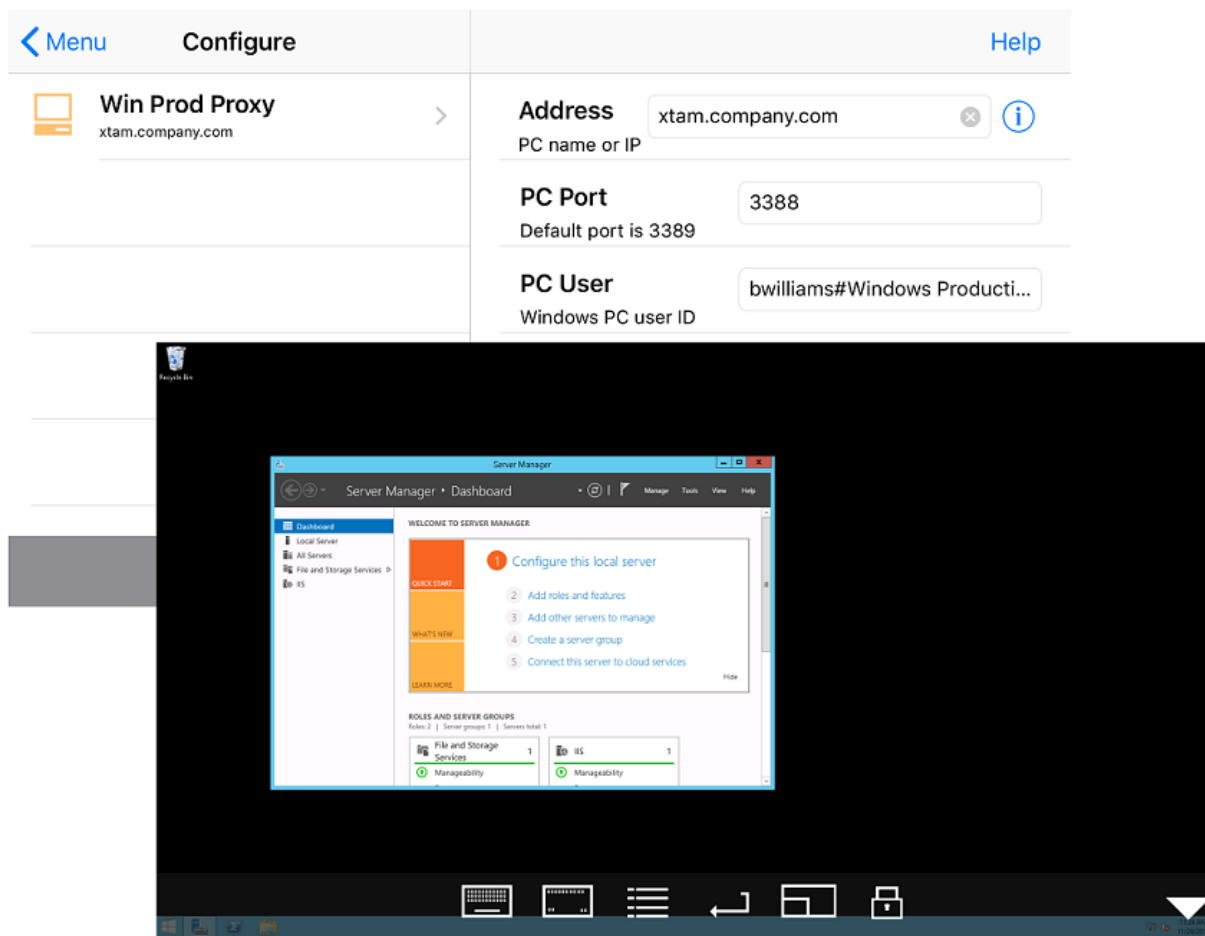
### *Example: mRemoteNG*

Example using mRemoteNG.



### Example: generic RDP Mobile App

Example using a generic RDP Mobile App.



## Troubleshooting

RDP Proxy connections troubleshooting:

1. In PAM GUI search using the query: **computer name**. Does the search one single Windows Host record?
  - If the search finds no records or several records, try to connect to the record using Record-ID (you can grab it from the Record view screen) that you can use after # sign.
2. If only one record is found, can you connect to this record using WEB RDP Session?

[Contact the Support team](#) and share a screen shot of the record view so we can check whether it has user or \$login for pass-through connection.

- If WEB Session does not connect check the password on record is correct or PAM server does not have a connection route to the destination server.
  - If PAM is on a Windows computer, can you connect to the destination server using a native RDP client from PAM computer?
  - If you use \$login as a User name then try to use a real user name and password to test the connectivity.
3. On PAM GUI using login name navigate Management > My Profile > **Re-Enable RDP Proxy**. Enter password > **Save**.
    - Try to perform the RDP Session connection again. Does it work now?

4. Did you enable RDP Proxy in Administration > Settings > **Global Parameters** screen?
  - RDP Proxy is disabled by default. After enabling it, please restart service **pammnager / PamManagement** and try to connect again.
5. Is it possible that port **3388** is closed on PAM host server firewall or on the route to it (AWS Security Group or Azure NG)?
  - Please reopen a port and try to connect again.
6. Finally, if nothing works or gives a clue how to proceed, [please contact the Support team](#) and send all log files from the folder `$PAM_HOME/web/logs`.

## AWS Command Line Utility Proxy

AWS CLI Proxy is an add-on to support zero trust connections for Amazon [AWS command line](#) tool.

The option allows users to share privileged access to AWS infrastructure without sharing AWS keys.

The function uses AWS Access Keys record type to create records to store an AWS Access Key and a Secret Key.

Users with Connect [permissions](#) to the record can execute AWS command line utility directing it through PAM AWS CLI Proxy using an PAM [REST API token](#) as a secret key and a Record ID-based access key.

PAM AWS Proxy will forward the request to AWS servers using AWS keys from the record and return the result back to the client while generating audit logs, a session report and session events with the commands executed by the command line utility.

PAM AWS CLI Proxy respects role-based [Permissions](#) to the record, configured access request workflows including time-, location- and approval-based access as well as API Token expiration and location validation.

PAM AWS CLI Proxy operates on the protocol level allowing tools other than native AWS CLI tool to take advantage of AWS CLI Proxy.

## Instructions

1. Enable HTTP Proxy by going to Administration / Settings / Parameters under the Proxy section and setting the value from Disabled to **Enabled**.

Note that AWS CLI Proxy requires [a special license](#) to enable the option.

2. **Restart** the PamManagement service and *wait for 2 minutes* before proceeding to the next step.
3. Go to Administration / Record Types and **enable the AWS Access Keys record type**.
4. Go to Records / All Records or Favorites and **add a new AWS Access Keys record**.
5. Set the required *Name* value and the optional *Description* and/or *Reference Record* values.
6. The Access Key ID field should be the ID of the same Access Key used to run the AWS CLI tool, and the Secret Key field value should be the raw AWS Access Key. Both values can be found under Security credentials in AWS.

7. Users with Connect permissions to the record can execute AWS command line utility directing it through PAM AWS CLI Proxy.
8. To redirect AWS CLI tool to PAM record, users should use the following properties.

Note that AWS CLI tool has multiple ways to specify these properties. The description below references environment variables. Follow [documentation for AWS CLI](#) tool about different methods to specify these parameters.

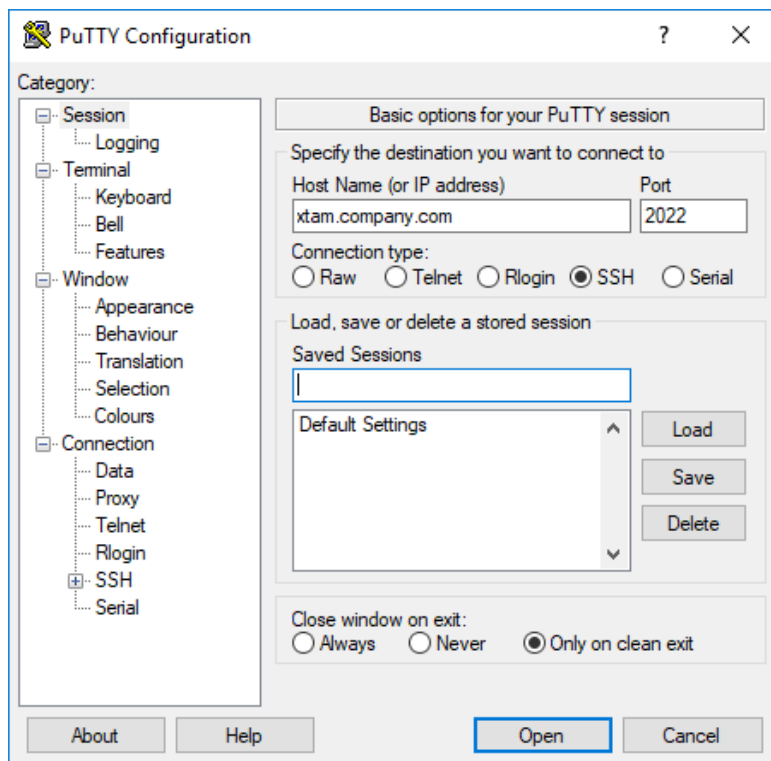
- **HTTPS\_PROXY** – PAM HTTP Proxy URL in the form **pam.company.com:8081**
- **AWS\_CA\_BUNDLE** – Path to PAM HTTP Proxy certificate downloaded from Management / My Profile / Preferences / Certificate
- **AWS\_ACCESS\_KEY\_ID** – PAM user and asset definition in the form **TOKEN-ID#RECORD** where **TOKEN-ID** is REST API token ID generated using Administration / Tokens screen. **RECORD** is either PAM Record ID or record search criteria identifying a single record with AWS access keys.
- **AWS\_SECRET\_ACCESS\_KEY** – REST API token generated using Administration / Token screen. **TOKEN-ID** in the **AWS\_ACCESS\_KEY** specification references the ID of the same token.

## SSH-Client-Proxy-Sessions

### SSH Client Proxy Sessions

Now its time to make your Administrators, Developers and Contractors happy too.

1. Open your local SSH client (we will use PuTTY in our example but most other SSH clients function similarly) and create a new session
2. In the **Host Name** field, enter the hostname of your PAM server (for example: xtam.company.com)
3. In the **Port** field, enter the port number you assigned in the PAM configuration from the previous section (default port in PAM is 2022)
4. For the **Connection Type**, select SSH.
5. Save the session and then **Open** the SSH connection



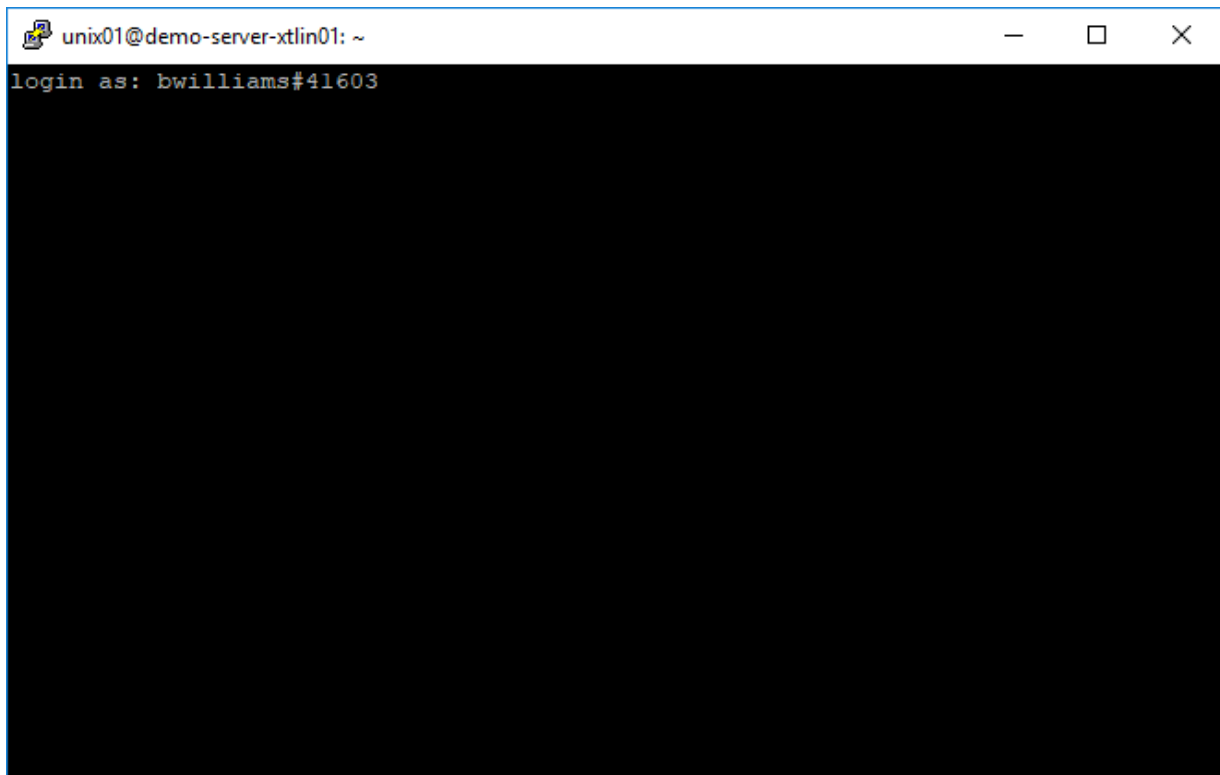
6. When PuTTY prompts for a **login as** account, enter a user string as described below:

If you do not know the record ID or Name, you can access the PAM SSH Proxy Interface to display and select from a list of available records for connection. You can access this Proxy Interface simply by not specifying a record ID or Name. For additional information, please read the [PAM SSH Proxy Interface](#) article.

#### **YourXTAMLoginName#XTAMrecordName or YourXTAMLoginName#XTAMrecordID**

For example, if your login to PAM was the username bwilliams and the PAM record that contains the SSH details has the name Unix Production Server and ID 41603, then the login string would be **bwilliams#Unix Production Server** or **bwilliams#41603**

When using the record Name to define the connection string, the record Name must be unique in PAM. If the name is not unique, the connection will fail and you should use its record ID instead.

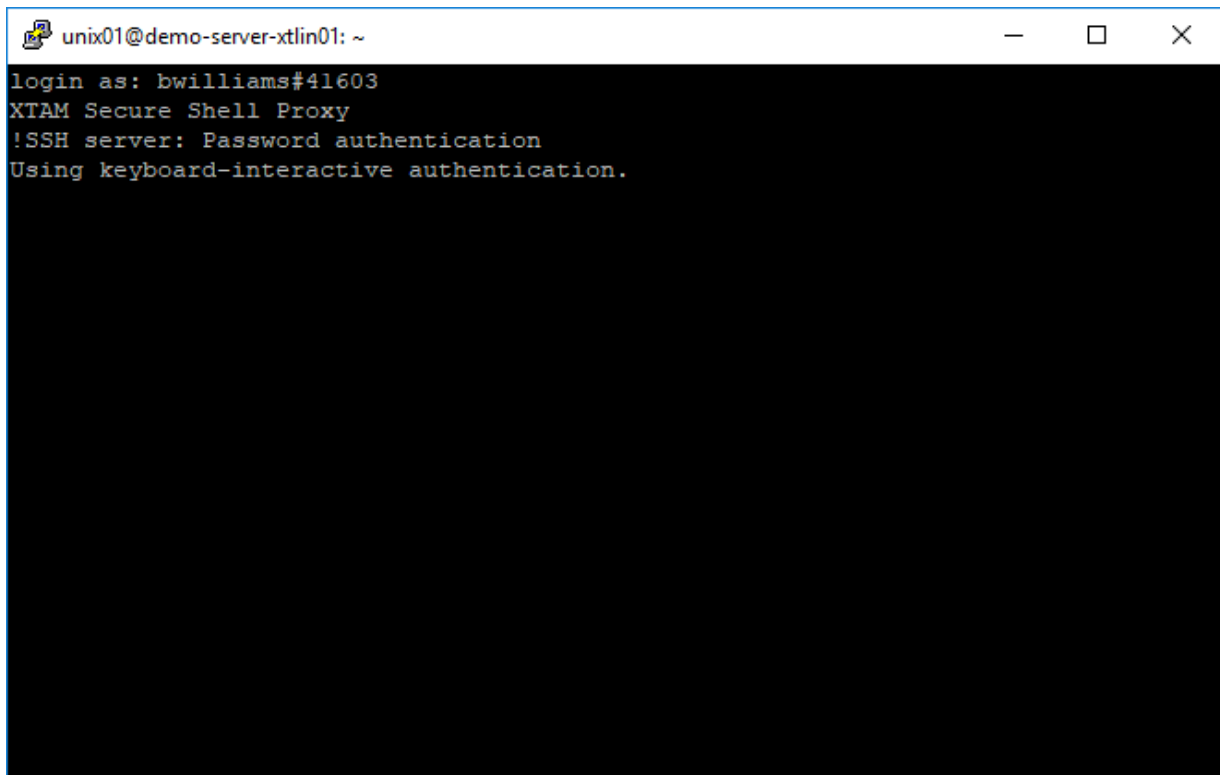


A # (hash), % (percent) or : (colon) character may be used as a separator between the login and recordID values.

The record's ID can be found in the URL when viewing the record's Details ([https://xtam.company.com/xtam/records/record\\_view/41603/type](https://xtam.company.com/xtam/records/record_view/41603/type))

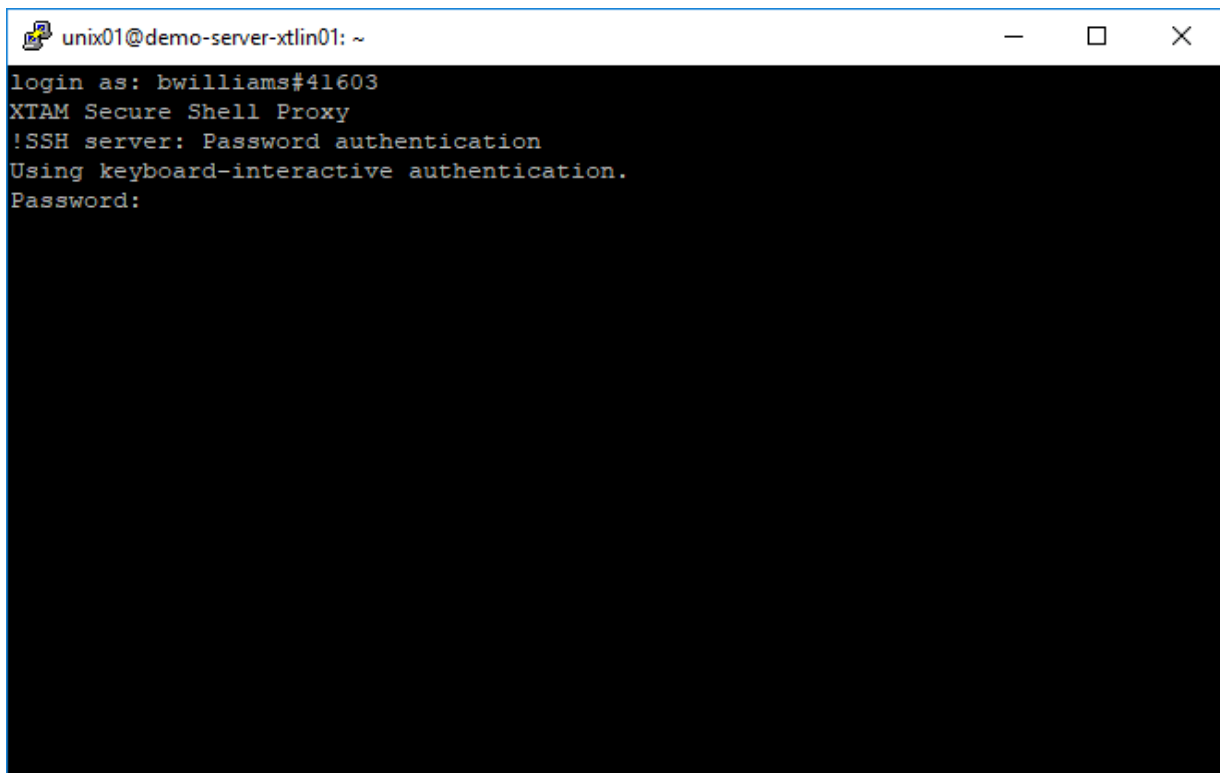
7. Press your **Enter key**
8. You will now observe an Authentication Banner is displayed to illustrate that the session is being provided via the *PAM Secure Shell Proxy*



A terminal window titled 'unix01@demo-server-xtlin01: ~' with standard window controls. The terminal output shows the SSH login process: 'login as: bwilliams#41603', 'XTAM Secure Shell Proxy', '!SSH server: Password authentication', and 'Using keyboard-interactive authentication.'

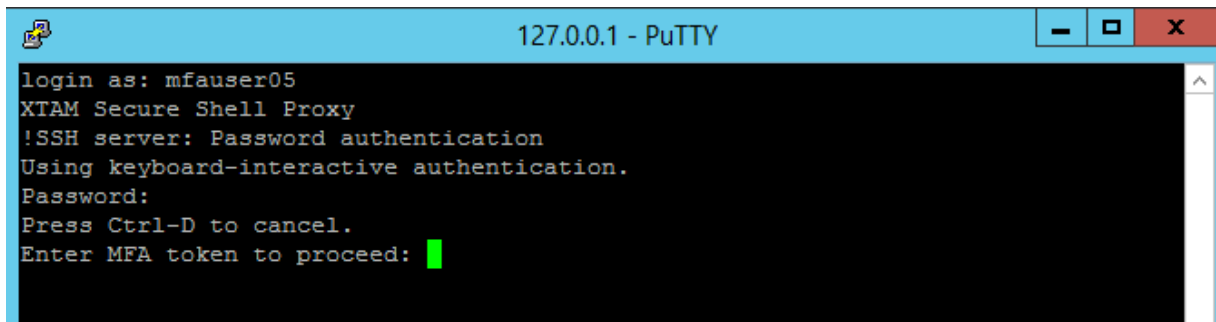
```
unix01@demo-server-xtlin01: ~
login as: bwilliams#41603
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
```

9. At the **Password** prompt, enter the password for your PAM login

A terminal window titled 'unix01@demo-server-xtlin01: ~' with standard window controls. The terminal output shows the SSH login process up to the password prompt: 'login as: bwilliams#41603', 'XTAM Secure Shell Proxy', '!SSH server: Password authentication', 'Using keyboard-interactive authentication.', and 'Password:'.

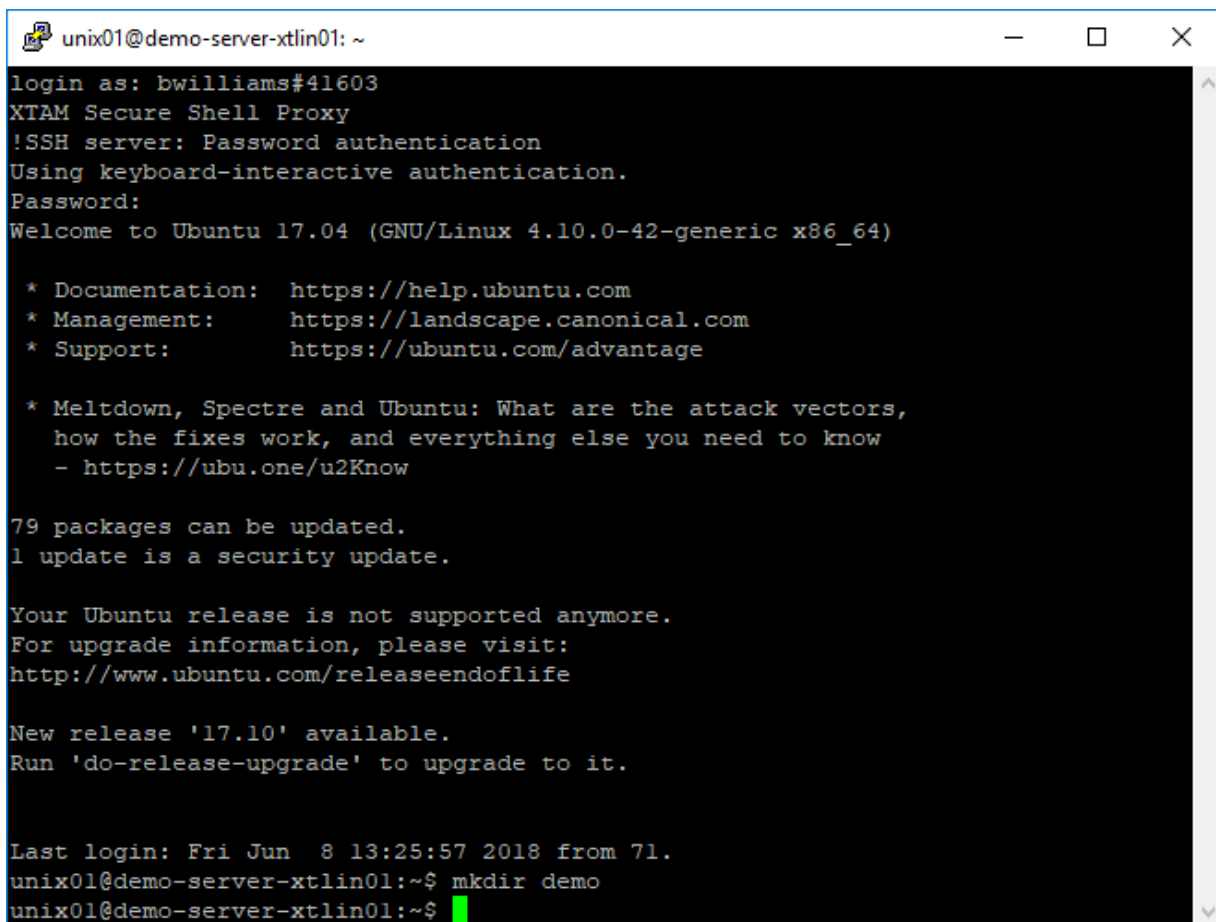
```
unix01@demo-server-xtlin01: ~
login as: bwilliams#41603
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
```

If you are using MFA, please enter your MFA token at the prompt to continue.



```
127.0.0.1 - PuTTY
login as: mfauser05
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
Press Ctrl-D to cancel.
Enter MFA token to proceed: █
```

10. Press your **Enter** key to complete the authentication process
11. After a few moments, you will be connected to the remote SSH endpoint using the secured connection details in the referenced PAM record.



```
unix01@demo-server-xtlin01: ~
login as: bwilliams#41603
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
Welcome to Ubuntu 17.04 (GNU/Linux 4.10.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Meltdown, Spectre and Ubuntu: What are the attack vectors,
   how the fixes work, and everything else you need to know
   - https://ubu.one/u2Know

79 packages can be updated.
1 update is a security update.

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '17.10' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Jun  8 13:25:57 2018 from 71.
unix01@demo-server-xtlin01:~$ mkdir demo
unix01@demo-server-xtlin01:~$ █
```

12. To confirm that the session is being provided via PAM, you can navigate to the Session tab of this record and note that there is now an Active session using this record. You can also execute commands in the PuTTY session and see them appear in the PAM event log.

User	Start Time	End Time	Type	Preview	Action
Barb Williams (bwilliams)	06/08/2018 13:59:13 ( +4m 56s )	06/08/2018 13:59:17 ( +4m 59s )	ShellInput	<div> <div>m</div><div>k</div><div>d</div><div>i</div><div>r</div><div>Space</div><div>d</div><div>e</div><div>m</div><div>o</div><div>Enter</div> </div> <div>mkdir demo</div>	...

## Example using Command or Terminal Prompt

```

unix01@demo-server-xtlin01: ~
chrisk@ckdell:~$ ssh chrisk#176@demo.xtontech.com -p 2023
XTAM Secure Shell Proxy
!Password authentication
Password:
Welcome to Ubuntu 17.04 (GNU/Linux 4.10.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Introducing Minimal Ubuntu for docker and clouds. 30 MB base image and
   optimised kernels on public clouds. Made for machines and containers.

   - https://bit.ly/minimal-ubuntu

0 packages can be updated.
0 updates are security updates.

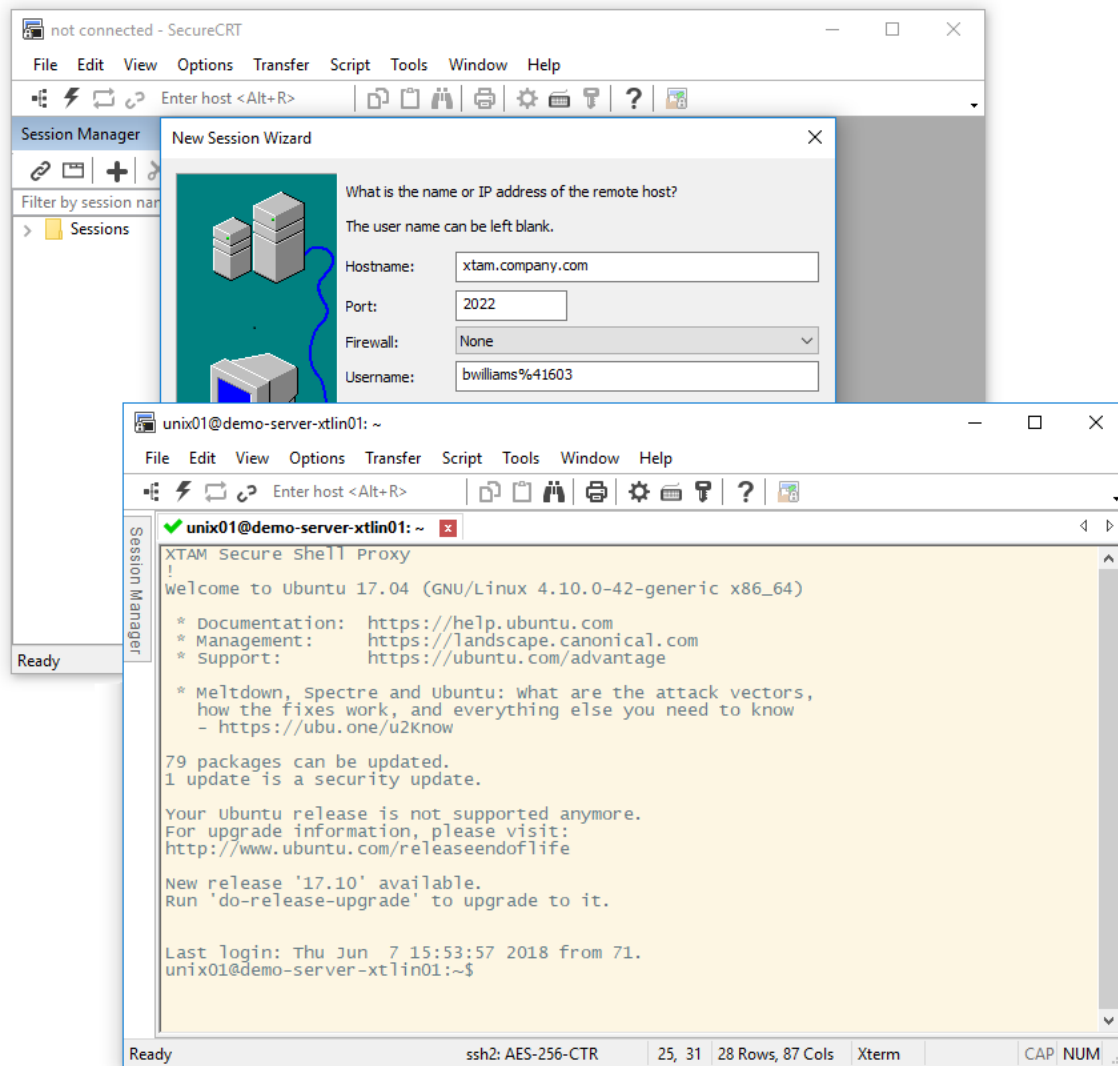
Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '18.04 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

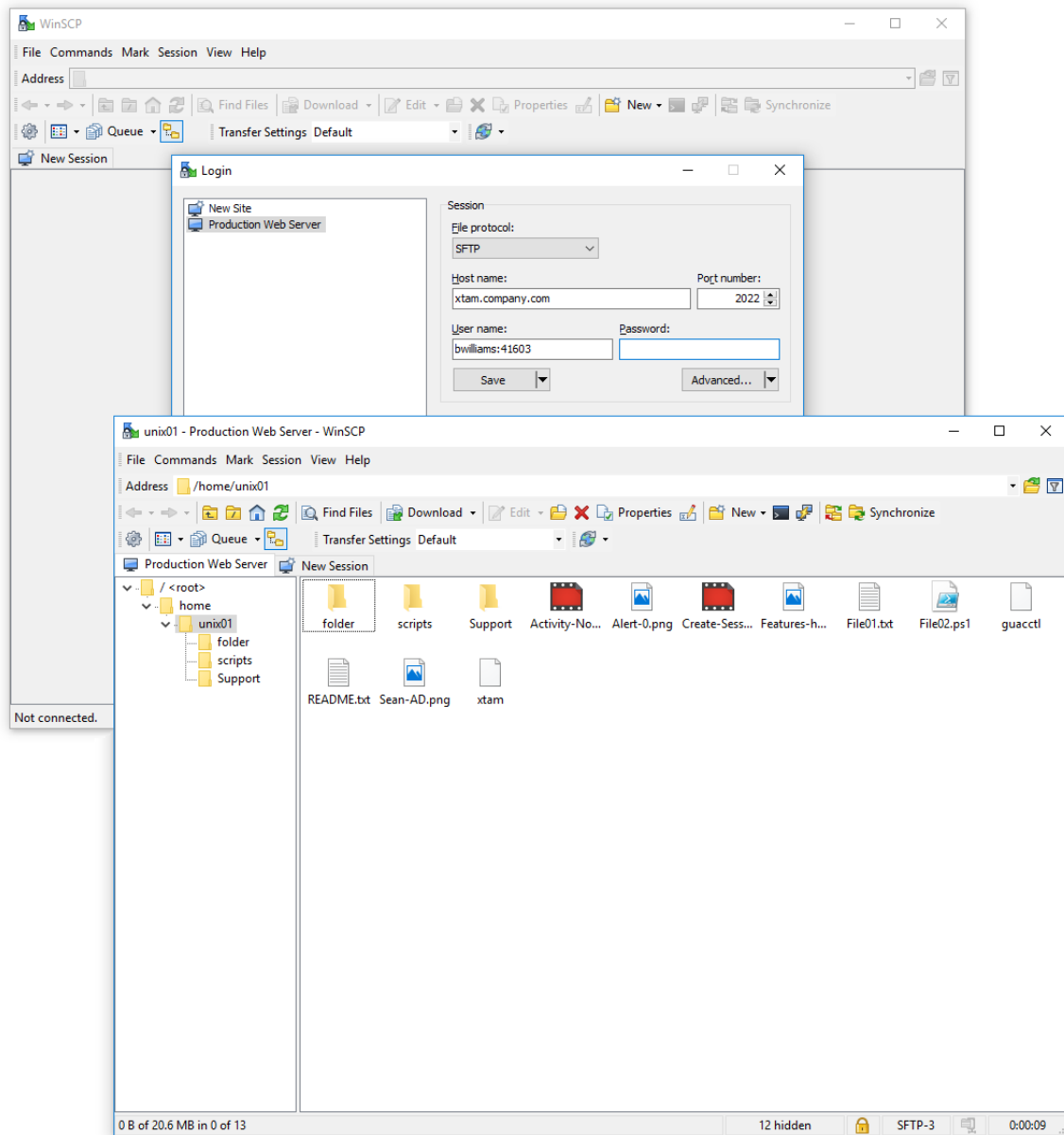
*** System restart required ***
Last login: Thu Jul 26 14:09:10 2018 from 10.0.0.20
unix01@demo-server-xtlin01:~$

```

## Example using SecureCRT



## Example using WinSCP



### [< Creating secure SSH records in PAM](#)

## Enabling SSH Proxy

1. Login to the System with a System Administrator account
2. Navigate to Administration > Setting > **Parameters**
3. Locate and modify the following settings:
  - a. **SSH Proxy:** Switch this option to Enabled and click the Save button to its right.
  - b. **SSH Proxy Port:** Use or change the port value that the System will use for SSH proxy and click the

Save button to its right.

SSH Proxy	Enabled	?	Save
SSH Proxy Port	2022	?	Save

4. Once both settings have been updated and saved, restart the **PamManagement** service (Windows) or **pammanager** service (Unix/Linux).
5. When the services is fully restarted (can take 1-5 minutes), the SSH proxy module is online.

## Controlling the list of channels

To control the list of channels available in SSH Proxy on a system wide level use global parameter **SSH Proxy Allowed Channels**.

This parameter controls what **channels/subsystems** allowed to use by client software when connecting through SSH Proxy server.

Supported channels are:

- **shell** - Allow shell connection
- **exec** - Allow remote command execution including scp transfer
- **sftp** - Allow file transfer using SFTP protocol
- **tunnel** - Allow SSH tunnels over SSH Proxy

The system wide settings could be overridden on record level using String custom filed named SshChannels.

There are two scenarios to override channel settings:

1. List channels allowed for current record. This will allow only shell and exec channels to open: shell, exec
2. Use system defaults but add or remove specific channel. This will use setting from system parameter but allow *sftp* and deny tunnel channels: **+sftp,-tunnel**

## PKCS#8 private key format support

System supports the accept PKCS#8 private key format when establishing connections to remote SSH end-points.

This option simplifies the process of on-boarding assets by supporting more key formats without the requirement to convert them to more popular ones.

Note password encrypted PKCS#8 keys still need to be converted to other supported formats before on-boarding them into the system records.

System supports PEM RSA, PEM OpenSSH, PPK, PKCS#8 private key formats when establishing WEB SSH sessions, SSH Proxy sessions or executing jobs on the remote servers using both SSH Remote and Interactive SSH execution strategies using either JSCH and SSHD drivers.

[< Creating a SSH session record](#)

# Public Key Authentication for SSH Clients

[PAM's SSH Proxy](#) provides support for native SSH application such as SSH Shell, PuTTY, Secure CRT, MobaXTerm, ssh.com and others to establish high-trust connections to remote servers by using a personal account (managed by Microsoft AD, eDirectory or PAM itself) without knowledge of the actual (shared or privileged) account on the destination server.

PAM's SSH Proxy allows a connection to remote servers using both **user/password** or **private/public key** authentication strategies as supported by remote server for this account.

Using the private key authentication mechanism when connecting to remote SSH servers:

- Simplifies access
- Promotes automation
- Reduces the number of passwords
- Increases overall network security

System supports the use of your existing Public/Private key pair or it can generate its own Public/Private key pair.

If you already have your own Public/Private key pair that you would like to use with PAM's SSH Proxy, please read the [To enable using your existing Public/Private Key Pair](#) to enable.

If you would like PAM to generate you a new Public/Private key pair to use with the PAM SSH Proxy, please jump to the [second section](#).

For PAM System Administrators managing these keys, please visit the [section at the bottom of this page](#) for available options.

## *To enable using your existing Public/Private Key Pair*

Only RSA generated keys are currently supported.

1. Login to your System user account and navigate to Management > My Profile > Preferences.
2. For the **Ssh2 Public Key** parameter, click the **Import** button and select your Public Key file (\*.pub) from your pair.
3. Your public key will now be imported to your System user profile and can be used to authenticate with your private key from this pair.



```
login as: sshkey
XTAM Secure Shell Proxy
!Authenticating with public key "rsa-key-20190219"
Passphrase for key "rsa-key-20190219":
Welcome to XTAM SSH Proxy Interface.
Type 'help' for more information.
xtam>
```

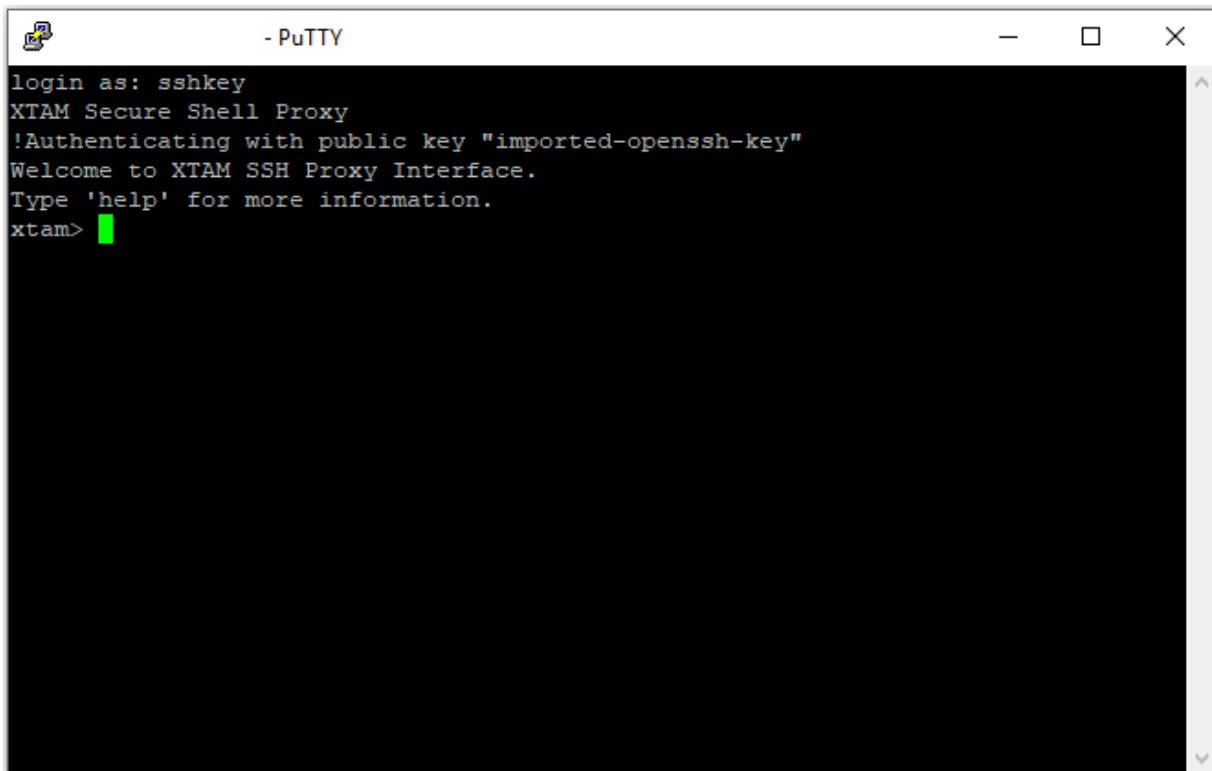
### *To enable using generated Public/Private Key Pair*

1. Login to your System user account and navigate to Management > My Profile > Preferences.
2. For the Ssh2 Public Key parameter, click the **Generate** () button.
3. Choose the parameters for your public key generation and then click the **Select** button.
4. Your public key will now be generated. This process may take several seconds to complete, so please do not refresh your browser during this time. Once the public key is generated, you will receive a Success dialog, click the **OK** button to continue.
5. Your browser will automatically prompt you to download the **Private Key** (\*.pem). **Download and save** your private key file to a safe location.

The private key is generated in .pem format.

You may need to convert this format to another in order to use it in your SSH application (PuTTY's \*.ppk format for example) or to assign a key comment or passphrase.





```
login as: sshkey
XTAM Secure Shell Proxy
!Authenticating with public key "imported-openssh-key"
Welcome to XTAM SSH Proxy Interface.
Type 'help' for more information.
xtam>
```

### *To disable using any Public/Private Key Pair*

1. Login to your System user account and navigate to Management > My Profile > Preferences.
2. For the **Ssh2 Public Key** parameter, click the **Delete** button.
3. Click the **OK** button on the Delete Public Key confirmation dialog
4. Your Public Key is now removed from your System account SSH Proxy authentication.

Note for all users using keys, if your key has expired or been blocked by a System Administrator then you will no longer be able to use it to authenticate.

To confirm your key's current status, navigate to your **Preferences** (Management > My Profile > Preferences)

- For blocked keys, the value in your **SSH Public Key** parameter will be crossed out (strike-through font)
- For expired keys, the value in your **SSH Public Key Created** parameter will be crossed out (strike-through font)

Please talk with your System Administrator for further information and assistance.

Note that PAM stores only public keys in the user's profile of the PAM vault. The keys are not stored in the back end user directory (such as Active Directory).

## System Administrator Key Management Options

### To Expire Keys

1. Login to your System with your System Administrator account and navigate to Administration > Settings > Parameters > SSH Proxy Public Key Expiration.
2. *Enter a value (in days)* to expire these keys. Leave this parameter blank or empty to disable expiration.
3. Click the **Save** button.

### Blocking

To block a user's ability to authenticate with their key:

1. Login to your System with your System Administrator account and navigate to Reports > Users.
2. Click the **Columns** dropdown menu and select the option labeled **SSH Key**. This column will display each user's Public Key creation date. If they do not have a key associated to their account, it will be empty.
3. Locate the User that you wish to block in this report, open the **Action** menu for their account and select the option **Block SSH Key**
4. Click **OK** on the confirmation dialog prompt.

User blocked SSH Keys will be shown with their key creation date crossed out.

### Unblocking

To unblock a user's ability to authenticate with their key:

1. Login to your System with your System Administrator account and navigate to Reports > Users.
2. Click the **Columns** dropdown menu and select the option labeled **SSH Key**. This column will display each user's Public Key creation date. If they do not have a key associated to their account, it will be empty.
3. Locate the User that you wish to block in this report, open the **Action** menu for their account and select the option **Unlock SSH Key**
4. Click **OK** on the confirmation dialog prompt.

The user's SSH Key creation date will now be shown without the crossed out font.

## Managing Local User SSH Keys

A System Administrator has the option to manage any Local User's SSH key configuration and in the case of folder scoped Local Users, the Folder Owner(s) may also manage any Local User's SSH key configuration within their folders.

To manage any Local User's SSH Key configuration (System Administrators only):

1. Login to your System with your System Administrator account and navigate to Administration > Local Users.
2. Click the **Edit** button for the Local User that you wish to manage their SSH Key configuration.
3. Use the Generate, Upload or Delete options to perform the desired operation. If generating a new key pair, provide the private key to the user as needed.

To manage a folder scoped Local User's SSH Key configuration (System Administrators or Folder Owners only):

1. Login to your System with your System Administrator or Folder Owner account and navigate to the folder where the Local User was created.
2. Open the Manage > Local User page from within this folder.
3. Click the **Edit** button for the Local User that you wish to manage their SSH Key configuration.
4. Use the *Generate*, *Upload* or *Delete* options to perform the desired operation. If generating a new key pair, provide the private key to the user as needed.

## Additional Information

Additional System Administrator or Auditor Information:

- **Audit Log** events are created for the generation, uploading and deletion actions related to user's SSH Public Keys.
- Audit Log events are created for the blocking and unblocking of a user's key.
- The **Users report SSH Key** column (hidden by default) will display the creation date of the user's key.
- The **Users report SSH Key** column (hidden by default) will display the creation date of the user's key with four states:
  - Empty or blank: This user does not have a key associated to their account.
  - Normal font: This user has a key associated to their account that is not blocked and has not expired. *Example:* 06/15/2017 00:00:00
  - Strike-through font: This user has a key associated to their account and their key is blocked. *Example:-* ~~06/15/2017 00:00:00~~
  - Italic font: This user has a key associated to their account and their key has expired. *Example:* *06/15/2017 00:00:00.*

## SSH Tunnels for Privileged Access

### *Creating SSH Tunnels for Secure Access*

A common scenario we hear from our users is that they want to provide access to an internal resource (for example, a production database) without having to open access to it externally.

In addition, allowing their Admins and Developers to continue to use their native client tools is usually a must have requirement.

So how can you satisfy such a requirement while maintaining security?

The answer is simple: use PAM's privileged access management while employing SSH tunnels.

Using a secure, password-less SSH session to the jump server, the user's traffic from their client is then tunneled to the desired endpoint.

Other common scenarios where SSH Tunnels are used:

- Ports cannot or should not be opened
- The service or system should only be accessible internally
- Firewall configurations
- Security architecture requires it

To enable the capturing of SQL statements to the PAM Session Event report, please read our [Capturing SQL Traffic](#) article.

In the following example, we will demonstrate how PAM is configured to use a Unix jump server in order to provide a SSH tunnel from an external SQL Developer client to an internal Oracle database.

To make use of SSH tunneling, you first must enable the SSH Proxy feature in PAM. If you have not this feature yet, please first read our [SSH Proxy](#) article and then return here when complete.

To learn how you can use a Public/Private key pair to authenticate SSH proxy sessions, please read our [SSH Session Public Key Authentication](#) article.

The [following sections](#) describe how to create secure SSH records in PAM and then how to use these records in your native desktop clients.

```
ssh -p 2022 pamuser#i-4bbAmkj4QYq@pam.company.com -L 1521:10.0.0.31:1521
```

Where:

**pamuser** is the user with permission to PAM record

**i-4bbAmkj4QYq** - record ID of Unix Host record providing tunnel service

**pam.company.com** - host name of PAM server

**2022** - PAM SSH Proxy Port

**1521** - port for tunneling

**10.0.0.31** - destination server IP address

### *Allowed Hosts*

It is possible to add security restrictions on the SSH Proxy tunnels forward hosts and ports to limit user options to connect to only allowed servers and ports in the destination networks.

The option allows strictly controlled tunnel options to be defined for specified point-to-point communications.

When the tunnel is designed to connect only to specified service on selected computers, the option restrict the option for a user to connect to other computers or to other services by building different tunnel through the same privileged asset.

SSH Proxy produces Operation Error audit log record for the attempt to build a tunnel for restricted forward host or port.

To enable the option add the following fields to the record type of the tunnel record:

- **AllowedHosts** (Type: String, Display name: Allowed Hosts) with value is a comma separated list of allowed host, mask/bits or ipFrom-ipTo range (example: 10.0.0.31,10.1.2.0/24,10.2.0.10-10.2.0.30)
- **AllowedPorts** (Type: String, Display name: Allowed Ports) with value is a comma separated list of allowed port or portFrom-portTo range (example: 1433,14000-14100)

## Command Line Secure Shell Interface (SSH)

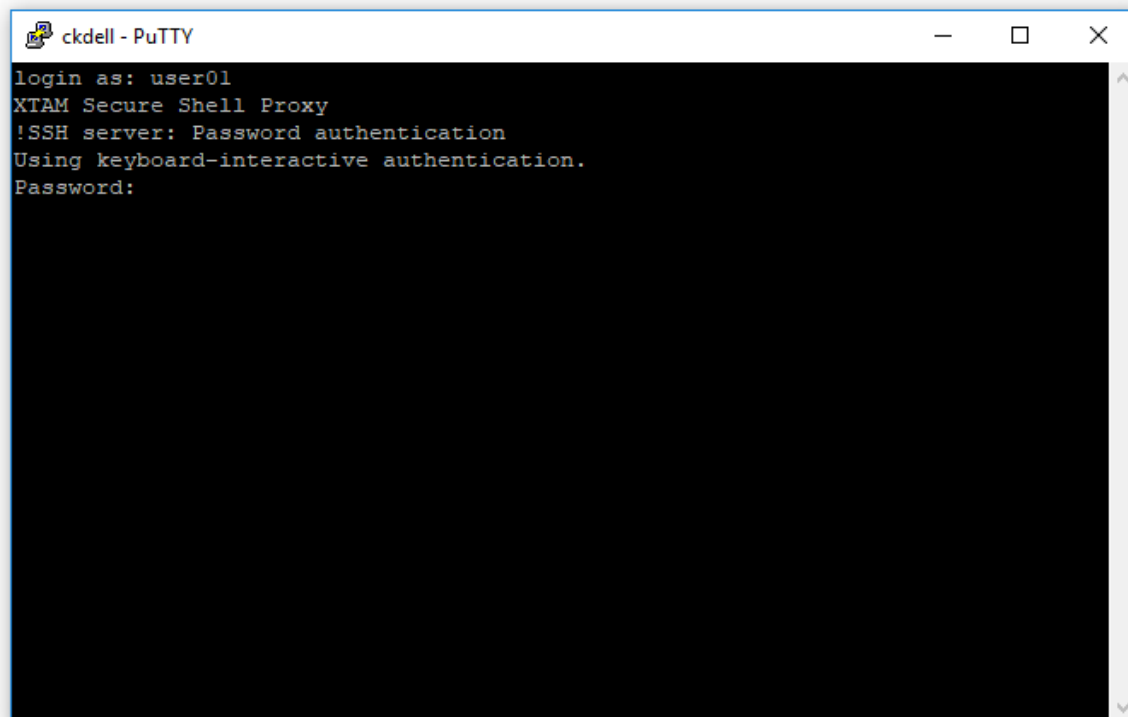
Instead of using a defined specific record to connect within your SSH proxy command, you can display a list of records that are available for connection.

This is helpful if you are unaware of the record ID or you want to use a more generic means of connection.

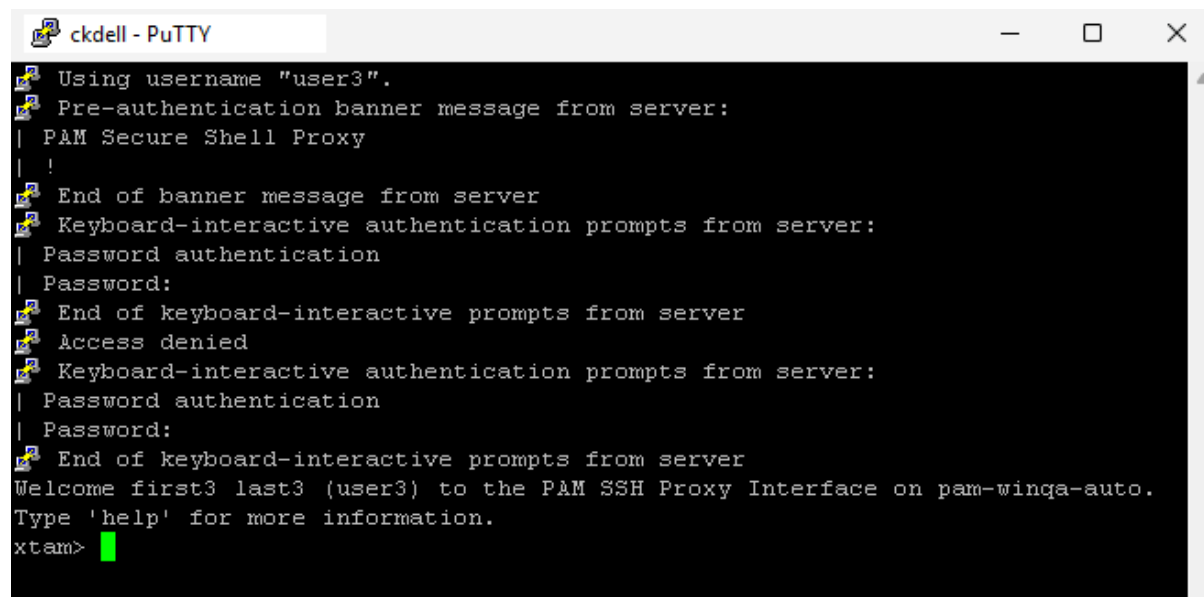
To learn about how to enable the SSH Proxy feature, please read our [SSH Proxy](#) article.

### Overview

To display a list of available records in your SSH proxy client, simply define your System login account when prompted or in your connection command and not the unique record identifier.



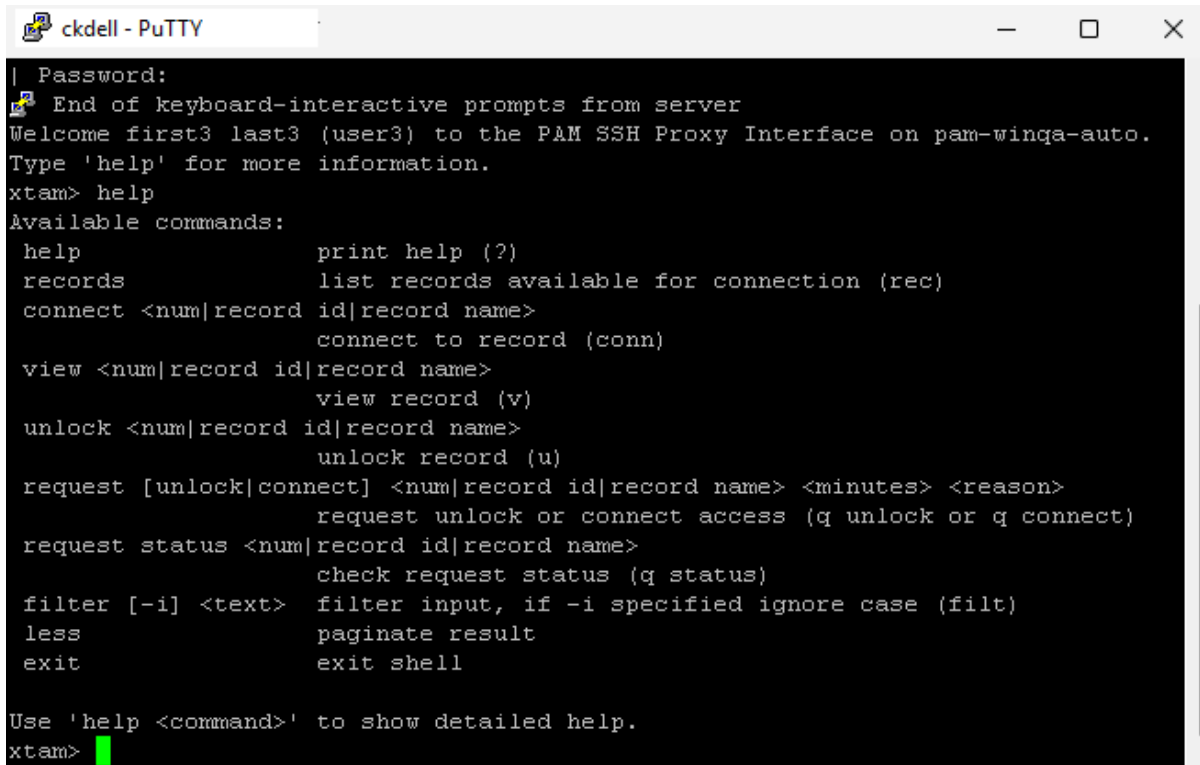
After you successfully authenticated, you will then be at the <xtam> prompt of the PAM SSH Proxy Interface. From here, the following commands are available:



```
ckdell - PuTTY
Using username "user3".
Pre-authentication banner message from server:
| PAM Secure Shell Proxy
| !
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password authentication
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password authentication
| Password:
End of keyboard-interactive prompts from server
Welcome first3 last3 (user3) to the PAM SSH Proxy Interface on pam-winqa-auto.
Type 'help' for more information.
xtam>
```

*help, ? or help<commandName>*

Command	Description
<b>help, ? or help &lt;commandName&gt;</b>	The Help command prints a list of available commands and a brief description.

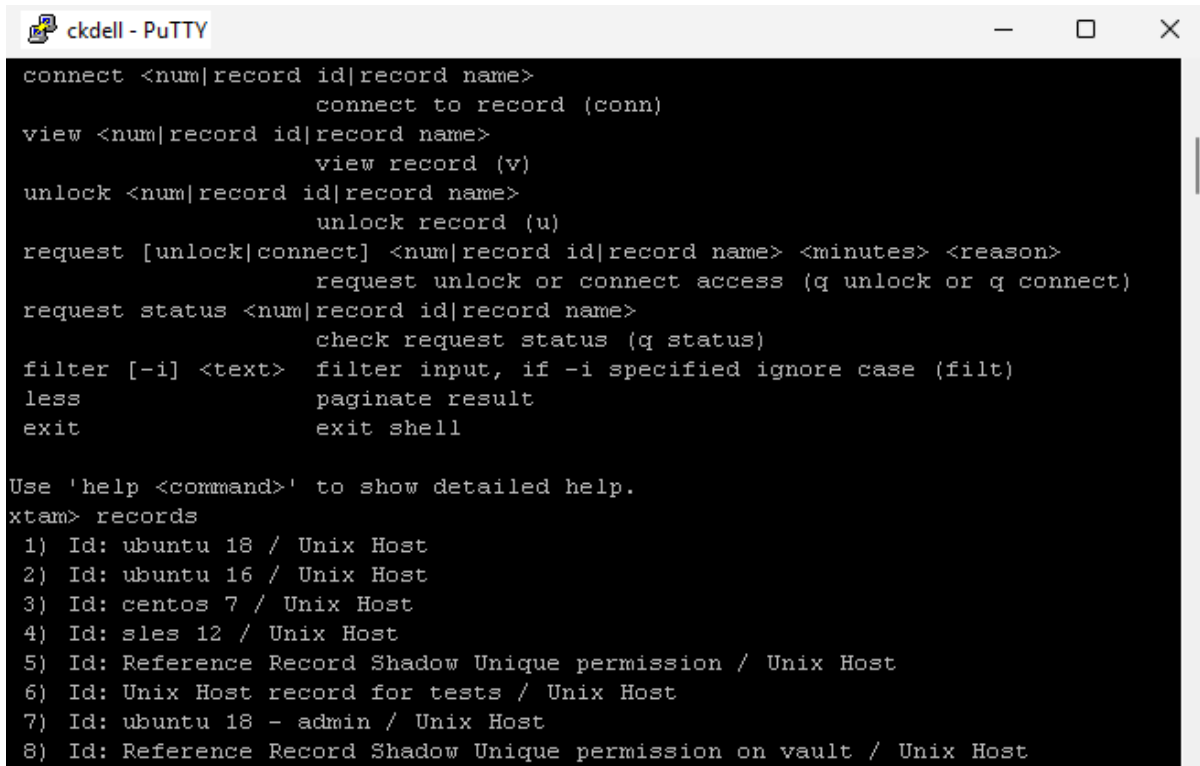


```
| Password:
End of keyboard-interactive prompts from server
Welcome first3 last3 (user3) to the PAM SSH Proxy Interface on pam-winqa-auto.
Type 'help' for more information.
xtam> help
Available commands:
help          print help (?)
records       list records available for connection (rec)
connect <num|record id|record name>
              connect to record (conn)
view <num|record id|record name>
              view record (v)
unlock <num|record id|record name>
              unlock record (u)
request [unlock|connect] <num|record id|record name> <minutes> <reason>
              request unlock or connect access (q unlock or q connect)
request status <num|record id|record name>
              check request status (q status)
filter [-i] <text> filter input, if -i specified ignore case (filt)
less          paginate result
exit          exit shell

Use 'help <command>' to show detailed help.
xtam>
```

## records or rec

Command	Description
<b>records or rec</b>	The Records command generates a list of records (displayed as List Number) Id: Record ID – Record Name) that are available to you based on permission and type. The list number or record ID is what will be used for selection when creating a SSH Proxy session.



```
connect <num|record id|record name>
    connect to record (conn)
view <num|record id|record name>
    view record (v)
unlock <num|record id|record name>
    unlock record (u)
request [unlock|connect] <num|record id|record name> <minutes> <reason>
    request unlock or connect access (q unlock or q connect)
request status <num|record id|record name>
    check request status (q status)
filter [-i] <text>
    filter input, if -i specified ignore case (filt)
less
    paginate result
exit
    exit shell

Use 'help <command>' to show detailed help.
xtam> records
1) Id: ubuntu 18 / Unix Host
2) Id: ubuntu 16 / Unix Host
3) Id: centos 7 / Unix Host
4) Id: sles 12 / Unix Host
5) Id: Reference Record Shadow Unique permission / Unix Host
6) Id: Unix Host record for tests / Unix Host
7) Id: ubuntu 18 - admin / Unix Host
8) Id: Reference Record Shadow Unique permission on vault / Unix Host
```



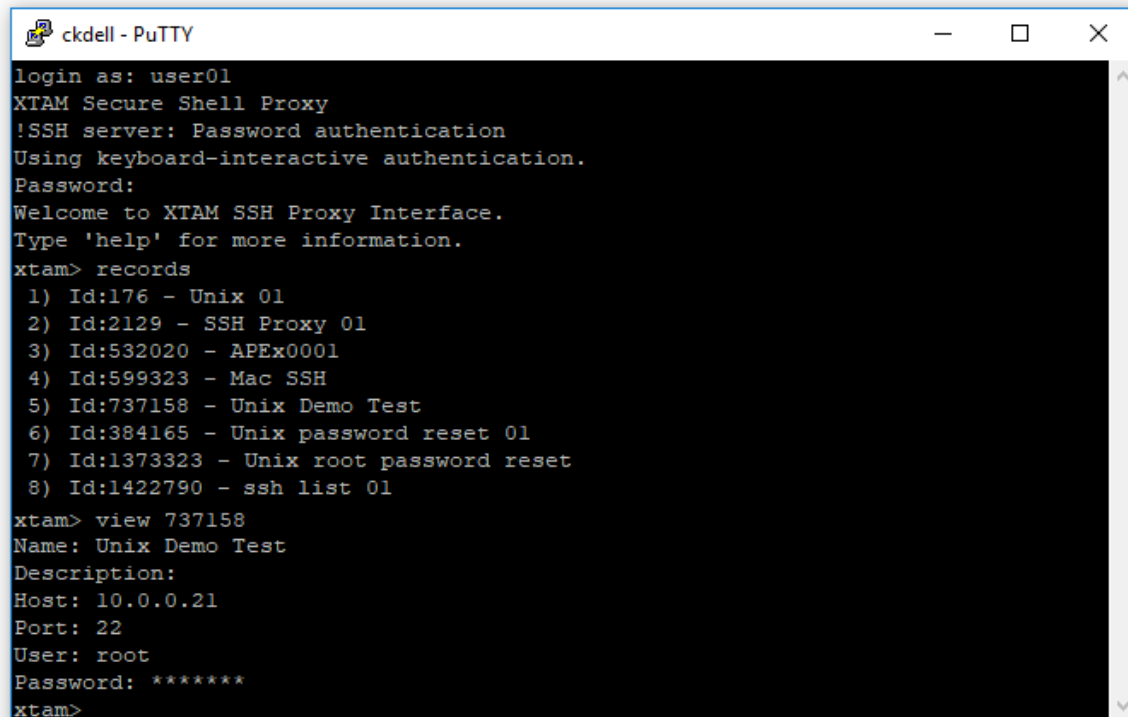
connect or conn

Command	Description
connect or conn	The Connect command is used to connect to the record defined by its list number or record ID. You can only use the record name to create a connection if it is unique. Use * (wildcard) at the end of the record name when executing request connect record-search* time-requested reason command to make mass request.

```
ckdell - PuTTY
login as: user01
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
Welcome to XTAM SSH Proxy Interface.
Type 'help' for more information.
xtam> records
 1) Id:176 - Unix 01
 2) Id:2129 - SSH Proxy 01
 3) Id:532020 - APEX0001
 4) Id:599323 - Mac SSH
 5) Id:737158 - Unix Demo Test
 6) Id:384165 - Unix password reset 01
 7) Id:1373323 - Unix root password reset
 8) Id:1422790 - ssh list 01
xtam> connect 737158
Connecting to record: Unix Demo Test
```

*view or v*

Command	Description
<b>view or v</b>	The View command is used to retrieve non-secured field information from a record defined by its list number, record ID or record name (if it is unique).



```
ckdell - PuTTY
login as: user01
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
Welcome to XTAM SSH Proxy Interface.
Type 'help' for more information.
xtam> records
 1) Id:176 - Unix 01
 2) Id:2129 - SSH Proxy 01
 3) Id:532020 - APEx0001
 4) Id:599323 - Mac SSH
 5) Id:737158 - Unix Demo Test
 6) Id:384165 - Unix password reset 01
 7) Id:1373323 - Unix root password reset
 8) Id:1422790 - ssh list 01
xtam> view 737158
Name: Unix Demo Test
Description:
Host: 10.0.0.21
Port: 22
User: root
Password: *****
xtam>
```

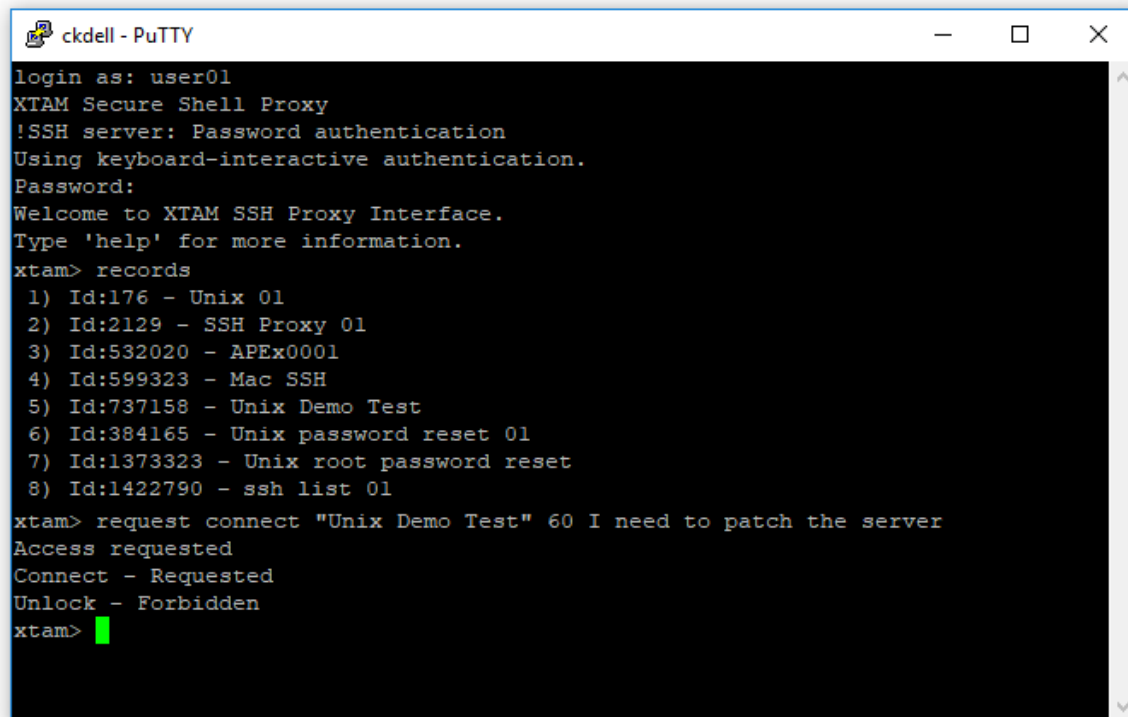
*unlock or u*

Command	Description
<b>unlock or u</b>	The Unlock command is used to retrieve both non-secured and secured (i.e. passwords) field information from a record defined by its list number, record ID or record name (if it is unique) and it can be used after the call of the command <b>records</b> or <b>rec</b> .

```
ckdell - PuTTY
login as: user01
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
Welcome to XTAM SSH Proxy Interface.
Type 'help' for more information.
xtam> records
 1) Id:176 - Unix 01
 2) Id:2129 - SSH Proxy 01
 3) Id:532020 - APEx0001
 4) Id:599323 - Mac SSH
 5) Id:737158 - Unix Demo Test
 6) Id:384165 - Unix password reset 01
 7) Id:1373323 - Unix root password reset
 8) Id:1422790 - ssh list 01
xtam> unlock 737158
Name: Unix Demo Test
Description:
Host: 10.0.0.21
Port: 22
User: root
Password: 7HXRT4FcteCx CpUReP
xtam>
```

## request or q

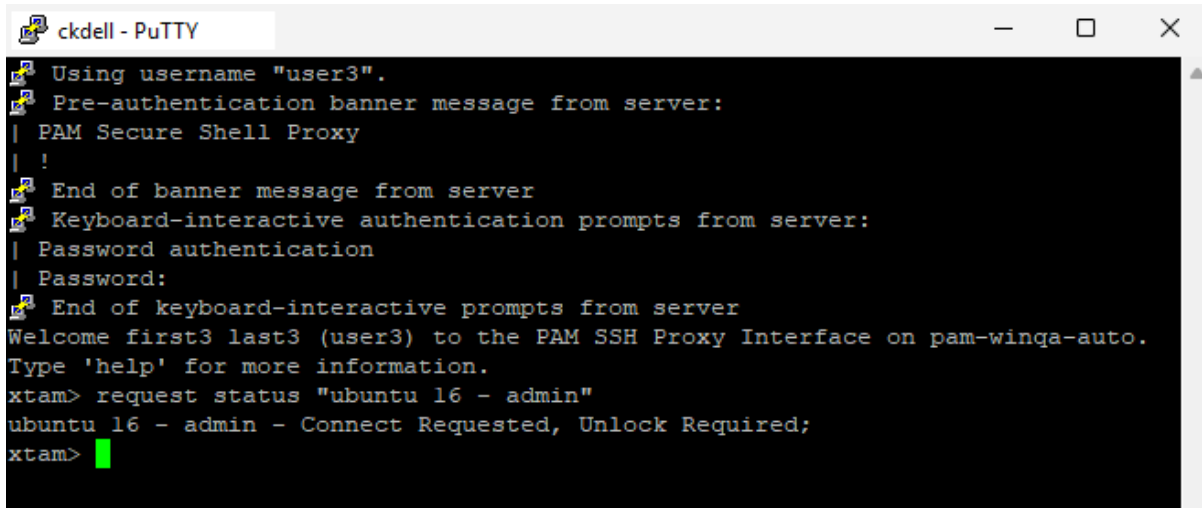
Command	Description
<b>request or q</b>	<p>The Request command is used submit an access request to either unlock or connect to a record defined by its list number, record ID or record name (if it is unique). When submitting the access request, the following values are required: request [unlock   connect] [record list number   record ID   "record name"] [requested minutes] [requested reason]</p> <p>Use a * (wildcard) character at the end of the record name to issue a bulk request access to all records that contain specified search criteria before the wildcard character.</p>



```
ckdell - PuTTY
login as: user01
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
Welcome to XTAM SSH Proxy Interface.
Type 'help' for more information.
xtam> records
 1) Id:176 - Unix 01
 2) Id:2129 - SSH Proxy 01
 3) Id:532020 - APEX0001
 4) Id:599323 - Mac SSH
 5) Id:737158 - Unix Demo Test
 6) Id:384165 - Unix password reset 01
 7) Id:1373323 - Unix root password reset
 8) Id:1422790 - ssh list 01
xtam> request connect "Unix Demo Test" 60 I need to patch the server
Access requested
Connect - Requested
Unlock - Forbidden
xtam> █
```

## request status

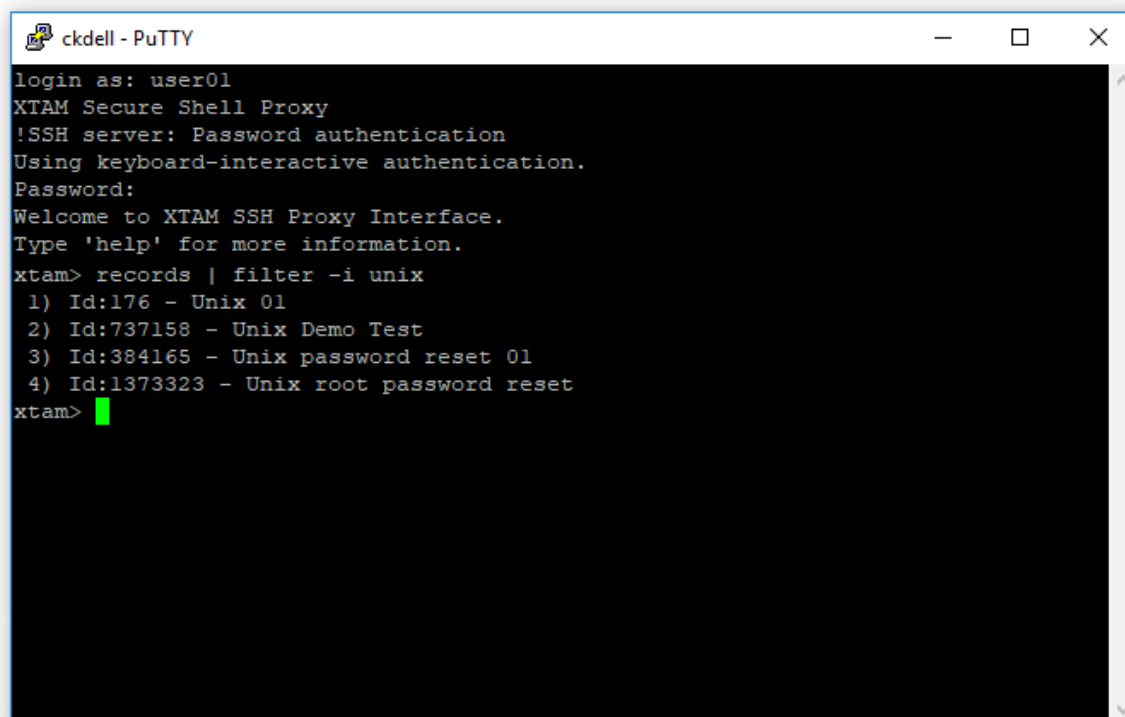
Command	Description
<b>request status</b>	<p>The Request Status command is used to check your access request status to a record defined by its list number, record ID or record name (if it is unique).</p> <p>Use a * (wildcard) character at the end of the record name to display a bulk request status for all records that contain specified search criteria before the wildcard character.</p>



```
ckdell - PuTTY
Using username "user3".
Pre-authentication banner message from server:
| PAM Secure Shell Proxy
| !
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password authentication
| Password:
End of keyboard-interactive prompts from server
Welcome first3 last3 (user3) to the PAM SSH Proxy Interface on pam-winqa-auto.
Type 'help' for more information.
xtam> request status "ubuntu 16 - admin"
ubuntu 16 - admin - Connect Requested, Unlock Required;
xtam>
```

## filter or filt

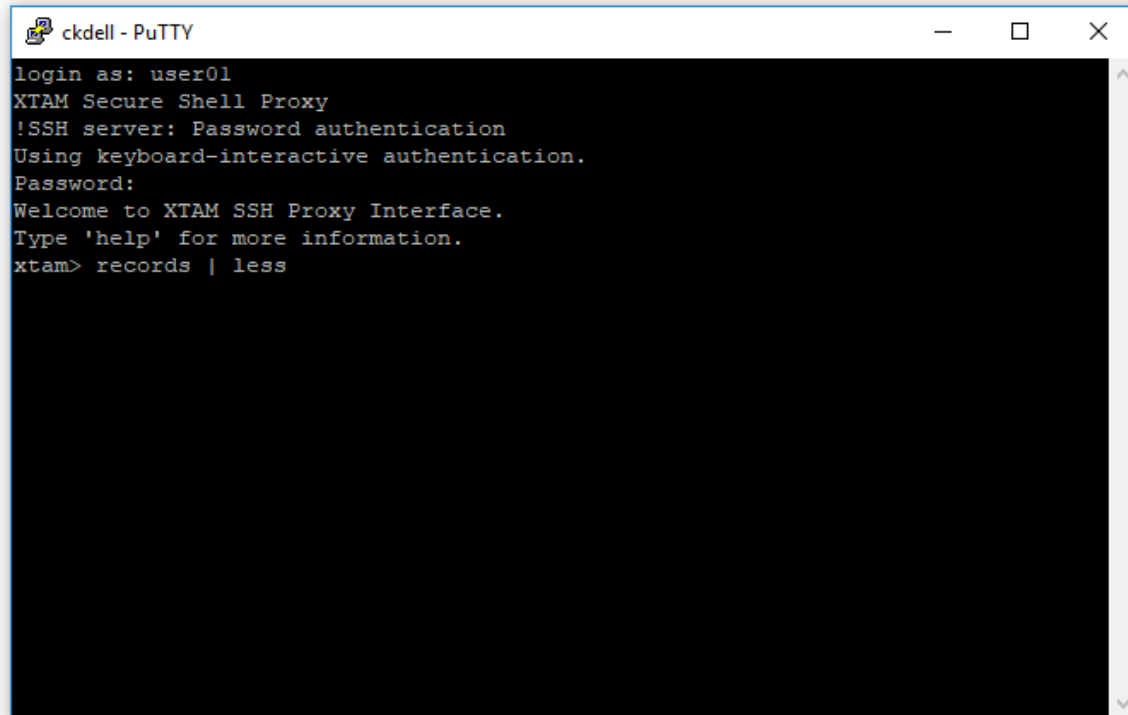
Command	Description
<b>filter</b> or <b>filt</b>	The Filter command is used to filter the list of available records that is returned. You can add -i to ignore case.



```
ckdell - PuTTY
login as: user01
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
Welcome to XTAM SSH Proxy Interface.
Type 'help' for more information.
xtam> records | filter -i unix
 1) Id:176 - Unix 01
 2) Id:737158 - Unix Demo Test
 3) Id:384165 - Unix password reset 01
 4) Id:1373323 - Unix root password reset
xtam>
```

## less

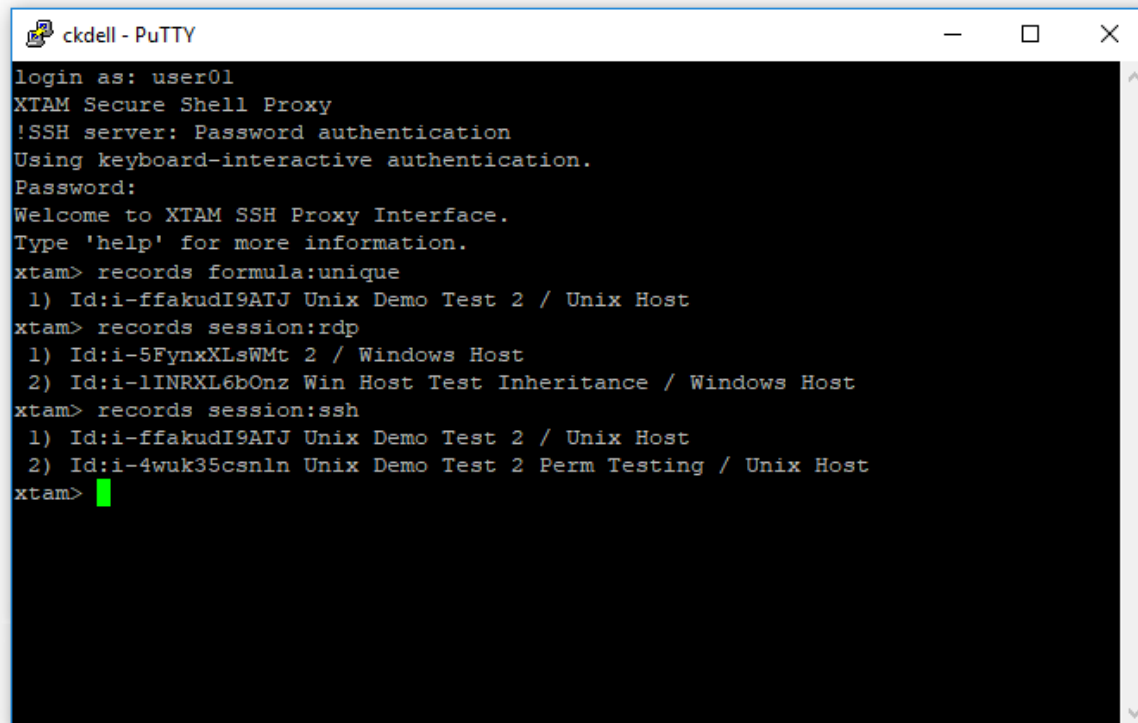
Command	Description
<b>less</b>	The Less command adds pagination to the list of available records. Use q to exit pagination and return to the prompt.



```
ckdell - PuTTY
login as: user01
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
Welcome to XTAM SSH Proxy Interface.
Type 'help' for more information.
xtam> records | less
```

## records

Command	Description
<b>records [search query]</b>	The search query command allows the user to execute a search using any of the available <b>Search Queries</b> .

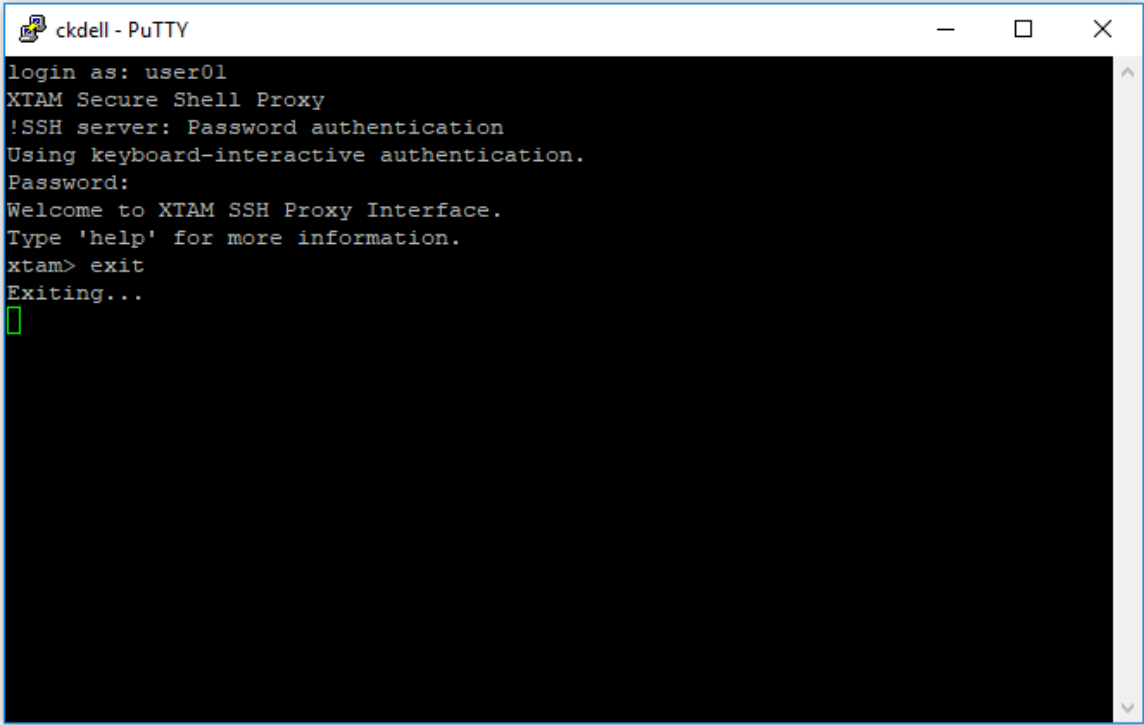


```
ckdell - PuTTY
login as: user01
XTAM Secure Shell Proxy
!SSH server: Password authentication
Using keyboard-interactive authentication.
Password:
Welcome to XTAM SSH Proxy Interface.
Type 'help' for more information.
xtam> records formula:unique
1) Id:i-ffakudI9ATJ Unix Demo Test 2 / Unix Host
xtam> records session:rdp
1) Id:i-5FynxXLsWMt 2 / Windows Host
2) Id:i-1INRXL6bOnz Win Host Test Inheritance / Windows Host
xtam> records session:ssh
1) Id:i-ffakudI9ATJ Unix Demo Test 2 / Unix Host
2) Id:i-4wuk35csnln Unix Demo Test 2 Perm Testing / Unix Host
xtam> █
```



exit

Command	Description
exit	The Exit command closes the SSH proxy session.



## Oracle-SQL-Proxy-Sessions

### Oracle SQL Proxy Configuration

Oracle SQL Proxy allows users to use native Oracle clients such as SQLplus, SQL Developer, Dell Toad Oracle, Squirrel, etc. running on their client desktop computers to connect to remote Oracle RDBMS without disclosing scheme credentials.

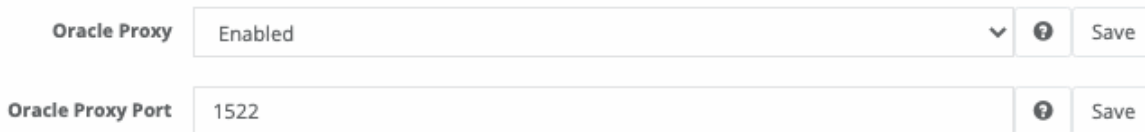
The SQL Proxy provides role-based permissions, allows users to request a workflow to the database, audits the access to the database, records SQL traffic and provides support for notifications about session events. While other PAM products claim to support secure database connections, they typically involve the use of a jump server which merely limits access to a DB client running on another host.

With PAM’s Oracle SQL Proxy, a user can run their own database client directly from their own workstation while the secure session runs through PAM where permissions and workflows are enforced and session events are tracked and monitored.

Using our SQL proxy, management of the schema credentials remains locked in the PAM vault and MFA can also be enabled to provide a secondary means of authentication to further secure access to these privileged sessions.

## Enabling Oracle SQL Proxy

1. Login to the PAM with a System Administrator account.
2. Navigate to Administration > Setting > [Parameters](#).
3. Locate and modify the following settings:
  - a. **Oracle Proxy:** Switch this option to *Enabled* and click the **Save** button to its right.
  - b. **Oracle Proxy Port:** Use or change the port value that the System will use for Oracle SQL proxy and click the **Save** button to its right.



Oracle Proxy	Enabled	Save
Oracle Proxy Port	1522	Save

4. Once both settings have been updated and saved, restart the **PamManagement** service (Windows) or **pammanager** service (Unix/Linux).
5. When the services is fully restarted (can take 1-5 minutes), the Oracle SQL Proxy module is online.
6. To confirm the proxy is started after the service restart, open the System log (`$PAM_HOME\web\logs\pam.log.[CurrentDate].log`) and search for the line below.

Note your proxy port may be different than 1522 if you changed its value in the previous step.

Oracle proxy server listening on \*:1522

## Creating Oracle SQL Proxy Records in Vault

After the Oracle Proxy is configured, create a new PAM record that will be used for Oracle Proxy connection. To create this new record, first navigate to Administration > **Record Types** and locate the type *Oracle*. Click **Edit**, uncheck the **Hidden** option and then click **Save**.

Navigate to a location where you want to create the record, click **Add Record** and select the type *Oracle* from the dropdown list.

For this new record, define the following values specific to the Oracle database:

- **Name (required):** PAM record name
- **Description (optional):** PAM record description
- **Connection String (required):** Oracle database connection string
  - Example:  
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=dbhost)(PORT=1521))(CONNECT\_DATA=(SID=orcl)))
  - Another example: host/SERVICE
  - Another example: host:port:SID

- **User (required):** The Oracle user account that has permission to connect to the database
- **Password (required):** The password of the Oracle account.

After defining your record details, click the **Save and Return** button.

With the new record having been created, be sure to configure the System [permissions](#) so that the users are able to connect with the proxy using this newly created record (Session Control: Connect).

## Monitoring Oracle Client Connection

When the client creates a successful connection to the database using the Oracle Proxy, the user may now work with the database through their client.

System will log or display at least the following information for Oracle Proxy connections:

- Session Report (Record and System Level)
  - A new session will be created indicating when the session was established. An *Active* status indicates that the user is still connected to the proxy and a *Completed* status indicates that the user is no longer connected to the proxy.
  - The session's Type will be labeled *ORAP*, meaning Oracle Proxy.
- Audit Log (Record and System Level)
  - A new Audit Log entry will be created for Oracle Proxy sessions, both Session Created and Session Completed. The Channel in the Audit entry's message will be *ORAP*.
- Record View
  - When viewing the System record that is being used by the Oracle Proxy, you will see an Active Session indicator when any user(s) is/are actively connected using this record.

Note: The Oracle Proxy connection and underlying records support native PAM permission and workflow options. The users must have at least some level of Session Control: Connect permission and cannot be bound by an unapproved workflow request to successfully connect with the proxy.

## SSL support for SQL Proxy connections

PAM supports accepting SSL connections from native Oracle clients as well as support for connections to destination Oracle RDBMS end-points using SSL connections.

This option secures Oracle RDBMS traffic from the native client to SQL Proxy to the destination Oracle RDBMS instance.

In addition to this, the option allows exposing non-SSL traffic from several RDBMS instances through an SSL-enabled channel for outside clients.

To enable SSL for the Oracle connection, include (protocol=tcps) to the address specification of the connection string.

To establish trust between native clients and SQL Proxy, import public proxy certificate found in `$PAM_HOME/content/keys/certificate_rdp.cer` to the native client key store.

For example, configuration for SQL Developer might include the following procedure:

```
1 | keytool -importcert -trustcacerts -file certificate_rdp.cer -keystore chain.jks
```

```

2 |
3 | AddVMOption -Djavax.net.ssl.trustStore=$STORE_PATH/chain.jks
4 | AddVMOption -Djavax.net.ssl.trustStoreType=JKS
5 | AddVMOption -Djavax.net.ssl.trustStorePassword=changeit

```

## Connecting to Oracle RDBMS through Oracle SQL Proxy

From the native SQL client, create a new connection that connects using the Oracle Proxy.

Depending on the client being used, these steps may vary. However, the general guidance remains the same.

- The Authentication used by the client will be the user's personal credentials to PAM. For example, if the user logs into PAM with the account 'john', then they will use 'john' and its password to authenticate their client to the PAM Oracle Proxy.
- The Connection details used by the client will be for the PAM Oracle Proxy, not the actual database as defined in the PAM record. The Host defined in the client will be your PAM instance (i.e. xtam.-company.com), the Port defined in the client will be the PAM Oracle Proxy Port (i.e. 1522 by default) and the Service Name or SID will be the ID-CAP value from the PAM record that was created (i.e. L-1IZOAKKNTAYM0).

As an example, here is a screenshot of the configuration using the Oracle SQL Developer v20 client:

New / Select Database Connection

Connection Name	Connection Details
Demo SQL Proxy	john@//demo.xt...

Name: Demo SQL Proxy

Database Type: Oracle

User Info: Proxy User

Authentication Type: Default

Username: john

Role: default

Password: .....

Save Password: ☒

Connection Type: Basic

Details: Advanced

Hostname: xtam.company.com

Port: 1522

☐ SID

☒ Service name: L-1IZOAKKNTAYM0

Status: Success

Buttons: Help, Save, Clear, Test, Connect, Cancel

Using the *Test* option in this client, the status will return *Success* when the client connects successfully to the PAM Oracle Proxy.

During Connection, the user's client will connect to the PAM Oracle Proxy that will use the PAM record to create the proxy connection to the database.

The proxy identifies the PAM record using the ID-CAP value as provided in the Service Name or SID value of the connection.

## Remote-Apps

### Remote Apps Getting Started Guide

PAM Privileged Remote Application Launcher using Windows RDS.

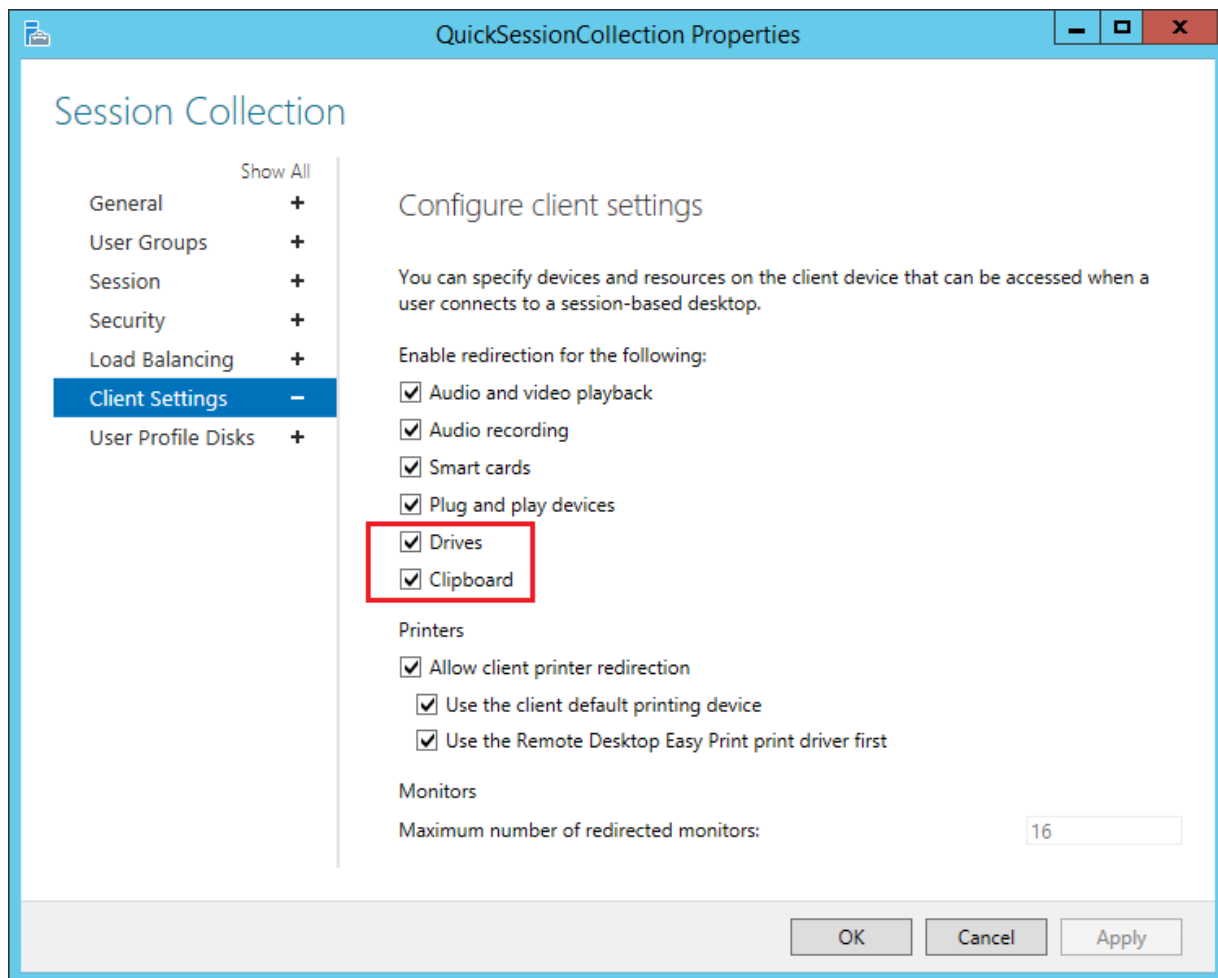
This guide is designed for System Administrators to learn about PAM Remote App Launchers and to create a secure login record to MS SQL Server Management Studio.

Please note that while this guide uses MS SQL Server Management Studio as an example, credential injection via a script is a required step for all web-based applications. PAM provides pre-built scripts for certain applications; however, for other web applications, you must create a custom script tailored to their authentication process.

Before you begin this guide, ensure you have the following pre-requisites.

#### *Pre-requisites*

1. Fully implemented, configured and working Windows Remote Desktop Services Host with Published RemoteApp functionality enabled. You will need access to the host to install our PAM Auto Shell program and to make it a Published RemoteApp Program.
2. Both the **Drives** and **Clipboard** options must be enabled in the RDS Collection's *Client Settings* configuration (shown in the screenshot below). If there are any Domain Policies that prevent *Drives* or *Clipboard* access, then exceptions must be made to accommodate this requirement.



3. Updated instance of Privileged Access Management with a System Administrator login.
4. MS SQL Server Management Studio installed on this host in the location.

Note the installation location of this application as it will be required in a later step of this guide.

5. Valid connection credentials for a MS SQL database connection (SQL Server name, Login and Password).

### *Topic guide*

**With the pre-requisites out of the way, this guide will cover the following topics:**

- [1. Deploying and publishing the PAM Auto Shell program](#)
- [2. Configuring the PAM Remote Apps record types](#)
- [3. Creating your PAM Remote App Host record](#)
- [4. Creating your PAM Remote App Launcher record](#)
- [5. Verifying or Updating Remote App Script](#)
- [6. Testing your Remote App connection](#)

## 1: Deploying and publishing

Deploying and publishing the Auto Shell program on your Windows Remote Desktop Services Host. This published Auto Shell application will be used to launch the RemoteApp application as configured in PAM.

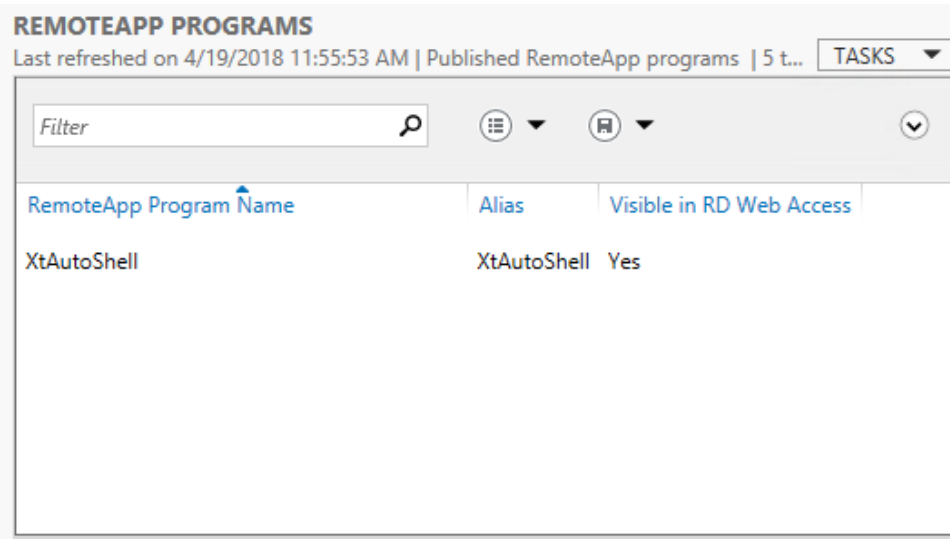
1. Copy the PAM Auto Shell program from your PAM host server to your Windows Remote Desktop Services host. The program is located at:

```
1 | $PAM_HOME\pkg\pam-app-launcher.zip
```

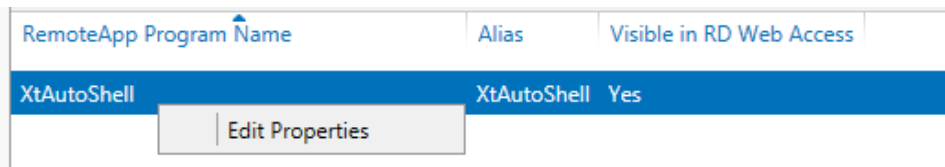
2. Login to your Windows Remote Desktop Services host.
3. On your Windows Remote Desktop Services host, extract our `pam-app-launcher.zip` to `C:\app`. The full program path should be:

```
1 | c:\app\XtAutoShell\XtAutoShell.exe
```

4. Publish `XtAutoShell.exe` as a new RemoteApp Program with the exact program name and alias `XtAutoShell`. You may set the *Visible in RD Web Access* parameter to **No** if you wish.



5. Ensure **User Assignment** is properly configured for the published `XtAutoShell` RemoteApp. To modify User Assignment, right click on `XtAutoShell` and choose **Edit Properties**.



6. Enable Remote Desktop to this host and enable permissions for the user account that you intend to define in your PAM record.

## 2. Configuring Remote Apps record types

1. Login to PAM as a System Administrator.
2. Navigate to Administration > **Record Types**.
3. Locate the Record Type **Remote App Host** and click its **Edit** button.

4. Uncheck the option Hidden and then click **Save**.
5. Return to the Record Types page and repeat this process for the Record Type **MS SQL Studio**.

### 3. *Creating your Remote App Host record*

This record will create the secure, remote connection to your Windows Remote Desktop Services server host. Users that will be starting RemoteApp sessions are not required to have permission to this record to begin their sessions. We recommend *limiting permission* to this Remote App Host record to only those that maintain or troubleshoot RemoteApp sessions.

1. Navigate to Records > All Records and (optionally) create a new folder.
2. Create a new Record using the type **Remote App Host**.
3. Enter a **Name** and **Description**.
4. Populate the following connection and configuration values:
  - **Host:** Enter the host name for the remote desktop connection to your Windows Remote Desktop Services server.
  - **Port:** Enter the port number for the remote desktop connection to your Windows Remote Desktop Services server.
  - **User:** Enter the user account that will establish the remote desktop connection and launch the published PAM Auto Shell program. This user must have RDP access to the Remote App Host and have permission to launch the published PAM Auto Shell program.
  - **Password:** Enter the password for this user account.
  - **Filter:** Enter the value MS SQL Studio. This defines which remote applications can be launched with the Remote App Host record. Empty value will permit any applications to be used.
  - **Remote App Platform:** Select Windows RDS from the dropdown menu.
  - **Enabled:** Check this box to enable this host for connection.
5. Click **Save and Return**.

### 4. *Creating Remote App Launcher record*

This record will be used by the System users to securely launch your MS SQL Server Management Studio remote application.

1. Create a new Record using the type **MS SQL Studio**.
2. Enter a **Name** and **Description**.
3. Populate the following connection and configuration values:
  - **Host:** Enter the server name for your MS SQL Database connection.
  - **User:** Enter the user account for your MS SQL Database connection.
  - **Password:** Enter the password for this user account.
4. Click **Save and Return**.

### 5. *Verifying or Updating Remote App Script*

Before you finish, we must verify or modify the launcher script to accurately reflect the installation path of our example application. If the path in the script is incorrect, then the Auto Shell program will fail to successfully launch it.



1. Navigate to the page Administration > Scripts.
2. Locate the script named “Remote Application MS SQL Studio Launcher” and click its **Edit** button.
3. The third line of this script begins with *Local Const \$SSMS\_EXECUTABLE*. In this line, verify the full path to the `Ssms.exe` application accurately reflects the installation path of this program on your Remote App Host server. Update the full path if required and click **Save** if any changes were made to the script. Failure to define the correct path to `Ssms.exe` will result in unsuccessful sessions.

## 6. Testing your Remote App connection

1. Open the MS SQL Studio record that was created in the previous step.
2. Select the Connect and Record option to establish the connection with session recording enabled.
3. A new session will open. It will first establish a secure connection to your Remote App Host server and then it will launch the PAM Auto Shell script. Now, the PAM Auto Shell program will launch MS SQL Server Management Studio, populate the Server name, User and Password parameters automatically and open the database connection. Once the connection is made, keyboard and mouse controls will be returned to you.
4. Navigate through your MS SQL database and execute a few test SQL commands. Once satisfied, you may exit MS SQL Server Management Studio and then disconnect the secure remote session by closing this browser tab or window.
5. At this point, you may review the video and keystroke recordings by opening the Sessions tab for this record.

This completes the PAM Remote App Launcher walk through.

By default, Remote App Host records could be used by any Remote App Launcher record stored in a PAM vault. To disable the ability of a Remote App Launcher record to use a Remote App Host record located in a different vault, please add the following line to PAM's `catalina.properties` file, save the file and restart the **PamManagement** service.

```
1 | xtam.apphost.crossvault.disable=true
```

List of default remote apps supported by PAM can be found [in Default Record Types article](#).

For additional remote app topics and how-to guides, return to the Remote App Launcher main page and use the topics listed at the bottom to navigate the available articles.

[< Return to PAM Remote App Launcher](#)

## Imprivata Enterprise Access Management (formerly OneSign) Web Console Session using PAM RemoteApps

Among other methods, part of the management of Imprivata EAM is done through the use of Web Portals; one for the administration of the product and a second for the administration of the appliance. The security

of both portals may be vital to the continued, uninterrupted use of EAM.

With the use of the RemoteApp feature of Imprivata PAM, it is now possible to securely vault the privileged credentials of your EAM deployment and to safely provide remote access to one or both EAM Web Portals. This remote access cannot only be provided on an “as needed” basis using powerful Permission and Workflow options, but it can also provide auditing and session recording capabilities to maintain strict compliance and security of EAM.

The guide provided in this article is designed to teach Imprivata PAM Administrators how to configure the RemoteApp feature to start securing their EAM Web Portal access.

Before we can begin, let’s cover the pre-requisites.

### *Pre-requisites*

- Fully implemented, configured, and working Windows Remote Desktop Services Host (RDS) with Published RemoteApp functionality enabled. You will need access to the host to install our PAM Auto Shell program and to make it a Published RemoteApp Program. This RDS Host will be used by PAM to launch a Google Chrome browser to access the EAM Web Portals.
- In your RDS Collection’s User Groups configuration, add a valid User or Group that PAM can use to connect to this RDS host, using RDP, to access our published RemoteApp.
- In your RDS Collection’s Client Settings configuration, both the Drives and Clipboard options must be enabled.
- Google Chrome must be installed on the RDS Host server and accessible by the PAM account to launch the browser. We recommend you disable Chrome’s Password Manager feature when using it with PAM.
- The EAM web URL for each console you wish to provide remote access and valid credentials for authentication into the console.
- Imprivata PAM using at least version 2.3.202203271414, released on March 27, 2022, and a valid System Administrator account to perform this configuration.

**CAUTION:** We are going to configure PAM to support an RDS RemoteApp session specifically for the EAM Appliance Console. If you want to support the EAM Admin Console, the configuration steps will be identical unless otherwise noted in this guide.

### *Deploy and Publish the PAM App Launcher*

1. This first step to deploy the PAM App Launcher to your RDS Host and publish it as a RemoteApp Program. Next, we will enable RDP connections to this host and install Google Chrome.
2. Obtain the PAM App Launcher from your PAM deployment located at `$PAM_HOME\pkg\pam-app-launcher.zip`. Copy this zip file to your RDS host server.
3. On RDS, extract this zip and copy its content to a non-temporary location on the host. We will use the example `C:\app` as the location in this guide. When extracted to `C:\app`, there will be 2 files, `XtAutoShell.exe` and `PamRemoteApp.jar`, and 1 directory, `/Include`, in this path.
4. Publish the `XtAutoShell.exe` as a new RemoteApp Program in your RDS collection.

## REMOTEAPP PROGRAMS

Last refreshed on 3/14/2022 4:09:12 PM | Published RemoteAp...

TASKS

Filter		
RemoteApp Program Name	Alias	Visible in RD Web Access
PAM	XtAutoShell	No

5. Enable Remote Desktop to this host and assign the required Windows permission to start an RDP session to the account that PAM will later use.
6. If not already, install the Google Chrome web browser to your RDS host and note the installation path.

### Modifying the PAM RemoteApp Script

This step may not be required if your RDS deployment is configured identically to the default script. However, if necessary, you can make the below adjustment to suit your environment.

1. Log in to PAM using a System Administrator account and navigate to Administration > Scripts.
2. Locate the script named *Remote Application EAM Appliance Console* and click its **Edit** button.
3. At the beginning of this script, locate the line *Local \$CHROME\_EXE=* and confirm the Chrome application path displayed is identical to the location where Chrome is installed on your RDS host. If it is not correct, modify the path as needed.

Custom Code (autoit)

```
1 #include <XTAM.au3>
2 #include <AutoItConstants.au3>
3
4 Local $CHROME_EXE="C:\Program Files\Google\Chrome\Application\chrome.exe"
5 ;~ Title: New Tab - Google Chrome
6 ;~ Class: Chrome_WidgetWin_1
7 Local $MAIN_WIN="[CLASS:Chrome_WidgetWin_1]"
8
9 Local $username
```

4. Click the **Save** button if any changes were made to the script.

**TIP:** If you plan to also support the EAM Admin Console, then repeat this section with the script named *Remote Application EAM Admin Console*.

### Enabling Record Types

Next, we need to enable the required Record Types to make them available for record creation.

1. Navigate to Administration > Record Types and click the checkbox next to the following types:
  - Remote App Host;
  - EAM Appliance Console;
  - EAM Admin Console (optionally, if you wish to support the EAM Admin Console).
2. With the two (or three) Record Types checked, scroll to the top of the page and click the **Bulk Actions > Enable** option to enable your selected types.

## Creating Records to Support EAM RemoteApp Sessions

Now we will create the records required to allow users to securely connect to your EAM web console session through the PAM RemoteApp feature.

1. Navigate to Records > All Records and (optionally) create a new container. A container is not required, but it allows the records to be more organized.
2. Within your chosen location, select **Add Record > Remote App Host** to create your first record. This record will be used by PAM to create the required RDP connection to your RDS host server to launch the Chrome browser. Create this record using the guidance provided below and click the **Save and Return** button when finished.
  - a. **Name:** (required) enter a name of your choice for this Remote App Host record
  - b. **Description:** (optional) enter a record description
  - c. **Reference Record:** leave blank
  - d. **Host:** enter the Host Name or IP address of your RDS Host server.
  - e. **Port:** define the RDP port of your RDS host server (default is 3389)
  - f. **User:** enter the Username of the account that will connect via RDP to your RDS Host server and launch the PAM App Launcher published RemoteApp
  - g. **Password:** enter the valid password of this account
  - h. **Filter:** EAM Appliance Console, EAM Admin Console
  - i. **Remote App Platform:** select *Windows RDS* from the dropdown
  - j. **Enabled:** check the box.
3. Return to the container where you created this record and create a second record by selecting **Add Record > EAM Appliance Console**. This record will contain the information required to connect to your EAM Appliance web console. Create this record using the guidance provided below and click the **Save and Return** button when finished.
  - a. **Name:** (required) enter a name of your choosing for this EAM Appliance Console record
  - b. **Description:** (optional) enter a record description
  - c. **Reference Record:** leave blank
  - d. **Url:** enter the full web URL to your EAM Appliance Console's login page
  - e. **User:** enter the username of the account that can login to this web console
  - f. **Password:** enter the valid password of this account

**TIP:** If you plan to also support the EAM Admin Console, then repeat this section to create a third record using the **Add Record > EAM Admin Console** option. Please note when entering the User for your EAM Admin Console record, use the full account name like *user@domain.com*.

## Testing your Session Connections

Finally, it is time to try your EAM Appliance Console remote session.

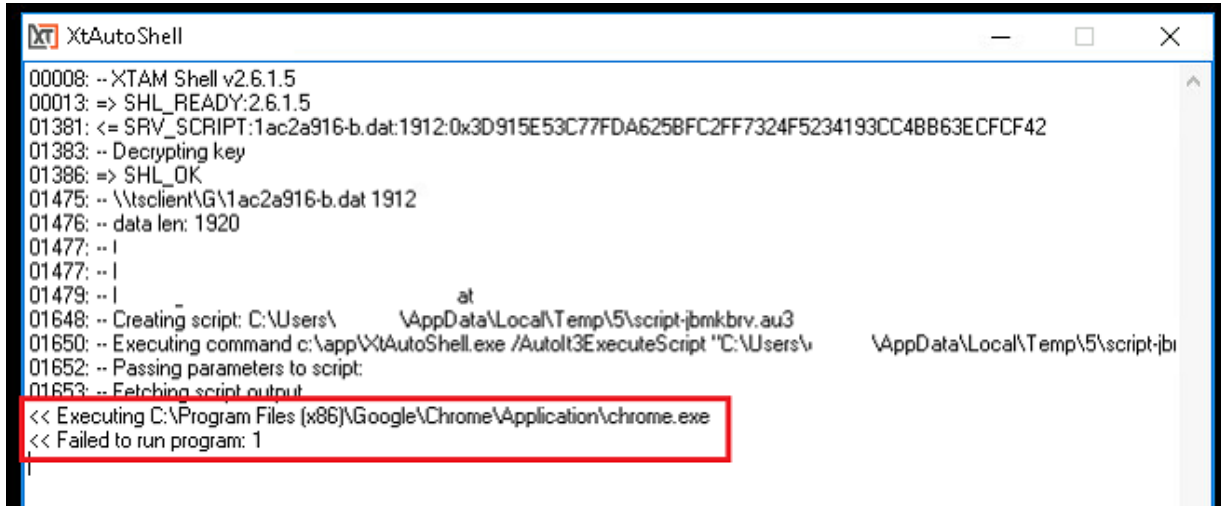
1. Open your EAM Appliance Console record and click the **Connect** or **Connect and Record** button.
2. A new session will begin. PAM will first establish an RDP connection to your RDS host server using your Remote App Host record.
3. Once this RDP session is successfully connected, the PAM App Launcher will automatically open and begin the process of launching the Chrome browser.
4. After the PAM App Launcher completes its operation, a Chrome browser will appear and PAM will begin the connection process. It will automatically enter the URL into the browser and after the login page loads, it will then enter the User, Password, and finally login to your EAM Appliance Console. The user cannot interact with the session until the automated process is complete.
5. You may now navigate the EAM Appliance Console using the credentials stored in the PAM vault. When you are finished, you can logout of the EAM Console and close the RDS Chrome browser to complete your PAM session.
6. If you selected the *Connect and Record* option, you may choose to review your recorded session now.

## *Troubleshooting and Tips*

Below you can find some common issues or tips that may help with this RemoteApp feature of PAM.

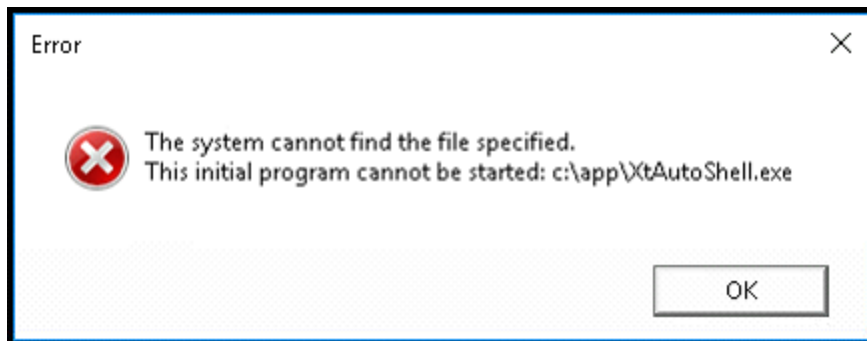
- The initial remote session to your RDS server fails with a session error 519 or 768.
  - This failure is usually caused by an incorrect host, port, or domain credentials stored in the record. Please verify that your User and Password are accurate and confirm with your RDS Administrator that the Host and Port are accurate. You should also make sure that RDP access to this host is available and this domain account is permitted to connect with this RDP session.
  - Additional information related to this [connection error](#).
- The initial remote session to your RDS server fails with a session error 771: Access Denied.
  - This failure typically occurs when the account defined in your Remote App Host record lacks the required permission in your RDS Collection to connect to the RD Session Host server and access published RemoteApp programs.
  - In your RDS Collection settings, open the *User Groups* section and add the account from your Remote App Host record.
- PAM App Launcher starts and executes the script, but quickly fails and my session completes.
  - This may be caused by an incorrect application path for the Chrome browser on your RDS Host server as defined in the PAM script. Please review the section above that discusses how to modify this path in the

PAM script.

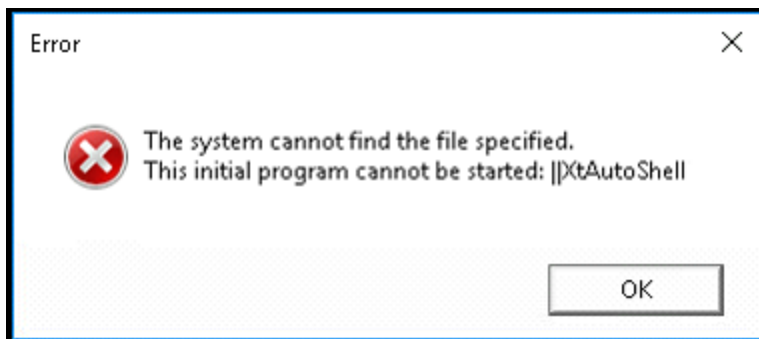


```
00008: --XTAM Shell v2.6.1.5
00013: => SHL_READY:2.6.1.5
01381: <= SRV_SCRIPT:1ac2a916-b.dat:1912:0x3D915E53C77FDA625BFC2FF7324F5234193CC48B63ECFCF42
01383: -- Decrypting key
01386: => SHL_OK
01475: -- \\tsclient\G\1ac2a916-b.dat 1912
01476: -- data len: 1920
01477: -- I
01477: -- I
01479: -- I
01648: -- Creating script: C:\Users\          \AppData\Local\Temp\5\script-jbmkbrv.au3
01650: -- Executing command c:\app\XtAutoShell.exe /Autolt3ExecuteScript "C:\Users\          \AppData\Local\Temp\5\script-jb
01652: -- Passing parameters to script:
01653: -- Fetching script output
<< Executing C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
<< Failed to run program: 1
```

- I receive the error message: Initial program cannot be started: <path\XtAutoShell.exe>



- XtAutoShell.exe was not found in the location defined in the RDS Published Remoteapp Program. Check this published RemoteApp in your RDS Collection and make any required changes to the RemoteApp program location.
- I receive the error message: Initial program cannot be started: XtAutoShell



- XtAutoShell was not published in your RDS collection. Check your RDS Collection and publish the XtAutoShell app as described earlier in this article.
- The automatic process of inputting the Url, User, or Password values into the login page of my console happens too fast or too slow.
  - Adjust the various *Sleep(n)* values in your script as needed. A Sleep value of 1000, measured in milliseconds, is equal to a 1-second pause in the execution of the script. We do not recommend overly

minimizing the Sleep pauses as a slowdown in application loading or web loading can lead to issues with the automated processing. It is better to have longer pauses to reduce the possibility of failures.

- Our EAM Admin Console has a Domain dropdown selector that prevents a successful login when passing just the User from the PAM record.
  - If your EAM Admin Console is integrated with 2+ Directories and a dropdown selector is required in the login form, then you must specify the User value in the PAM record using its full account name (UPN). For example, if the user is *bwilliams* and the domain is *contoso.com*, you would enter the User as *bwilliams@contoso.com* in the PAM record for your EAM Admin Console.
- The PAM RemoteApp session is starting successfully, however, Chrome is asking if the user wants to save the password. We don't want this to happen as it breaks the PAM autologin experience for RemoteApps.
  - We recommend you disable the Chrome Password Manager feature for this installation on your RDS Host server. Here is a link that offers guidance around Chrome Password Manager:  
<https://chromeenterprise.google/policies/#PasswordManagerEnabled>
- When a second user, UserB, starts a session the first user, UserA, is disconnected with the session error 521.
  - RDS is configured to allow only a single RDP session per user and since PAM is using the same account to connect to RDS (Remote Host App record), the second connection is taking over the first.
  - By default, Windows prevents a single user from establishing multiple sessions. As a workaround you may consider the following change on the RDS host server: from the Local Group Policy editor on the RDS Host server: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections > *Restrict Remote Desktop Services user to a single Remote Desktop Services session* > **Disabled**.
    - Consult with your Administrators before making any changes to the RDS Host server. Imprivata Support cannot help with Windows configuration.
- PAM App Launcher stuck on the "Waiting for window" message

Due to the limitations native to Google Chrome and most modern browsers, only a single session per user profile is permitted. As a result, when PAM starts a second session, using the same account from the Remote App Host record, Chrome is unable to launch and the App Launcher remains on this waiting message. This is a known limitation of Chrome and some workarounds are available that could be used to allow additional sessions per user profile as mentioned here:

<https://bugs.chromium.org/p/chromium/issues/detail?id=160676>

```
01349: -- Fetching script output
<< Executing C:\Program Files\Google\Chrome\Application\chrome.exe
<< Waiting for window
```

  - Consult with your Administrators before making any changes to the RDS Host server. Imprivata Support cannot help with Windows configuration.
- What is the expected behavior when PAM is configured to use a EAM Login (SAML) when the endpoint has a EAM agent installed and the EAM Extension is enabled in the browser?
  - If PAM is configured for EAM Login (SAML), and the endpoint has a EAM agent installed (with SSO enabled), and the web browser has the EAM Chromium extension installed, when the EAM Login button is clicked on the PAM webpage, the user is automatically logged using EAM SSO, without any prompt for



a username, password or MFA token.

- If EAM Single Sign-on is suspended in the EAM agent, the PAM system will prompt for the username, password and MFA token.

## Remote Apps with TSPlus

This guide is designed for System Administrators to learn about PAM Remote App Launchers using [TSplus](#) and to create a secure, high trust login to MS SQL Server Management Studio . Before you begin this guide, ensure you have the following pre-requisites:

1. Fully implemented, configured and working TSplus host. You will need access to the host to install our PAM Auto Shell program and to publish this application.
2. Updated instance of Privileged Access Management with a System Administrator login.
3. MS SQL Server Management Studio installed on this TSplus host in the location:

```
1 | C:\Program Files (x86)\Microsoft SQL
   | Server\140\Tools\Binn\ManagementStudio\Ssms.exe
```

4. Valid connection credentials for a MS SQL database connection (Server name, Login and Password).

### Guide topics:

**With the pre-requisites out of the way, this guide will cover the following topics:**

1. [Deploying and publishing the Auto Shell program](#)
2. [Configuring the Remote Apps record types](#)
3. [Creating your Remote App Host record](#)
4. [Creating your Remote App Launcher record](#)
5. [Testing your Remote App connection](#)

### Deploying and publishing

#### Step 1: Deploying and publishing the Auto Shell program on your TSplus Host

1. Copy the PAM Auto Shell program from your PAM host server to your TSplus host. The program is located at:

```
1 | $PAM_HOME\pkg\pam-app-launcher.zip
```

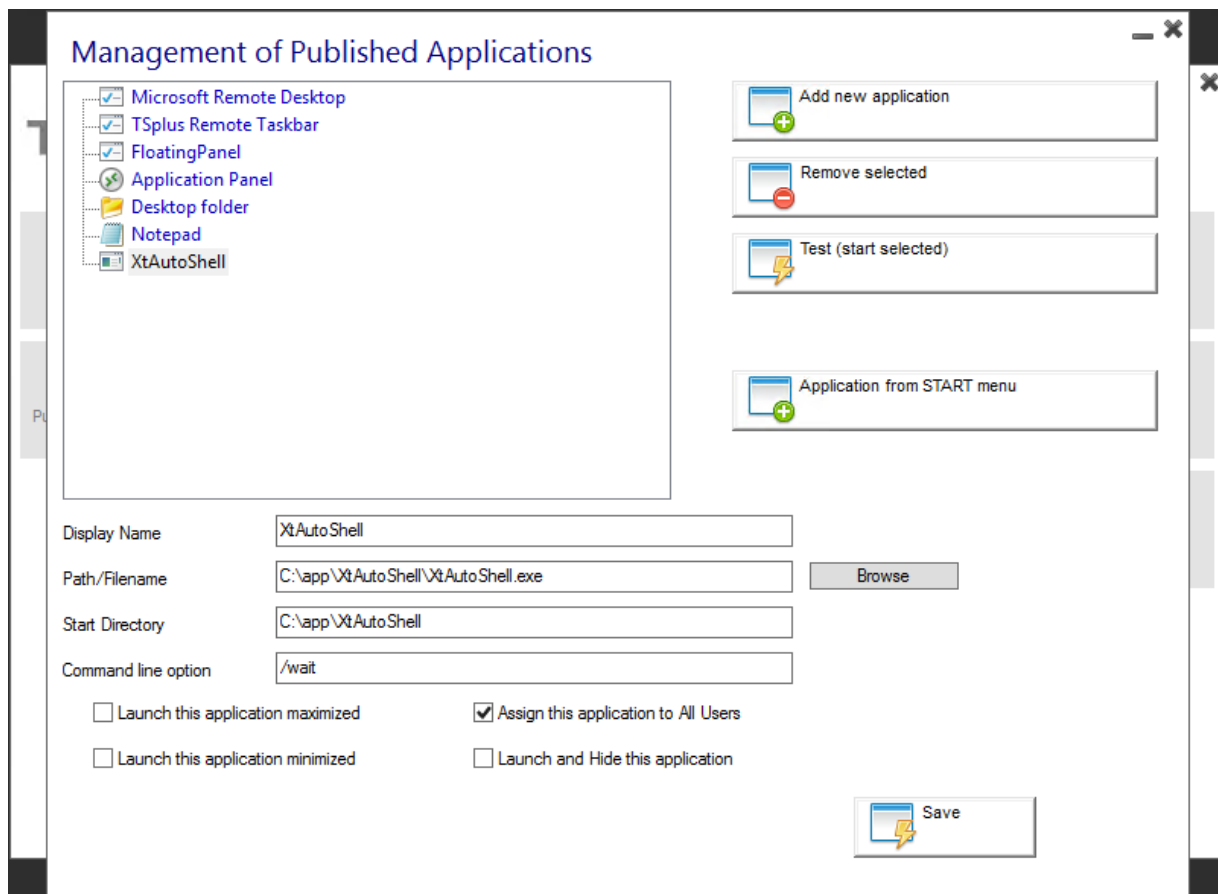
2. Login to your TSplus host.
3. On your TSplus host, extract our `pam-app-launcher.zip` to `C:\app`. The full program path should be:

```
1 | c:\app\XtAutoShell\XtAutoShell.exe
```

and an *Include* directory and `PamRemoteApp.jar` file will also be in this location.

4. In the TSplus Admin Tool, navigate to Applications > Application Publishing and add a new application for the **XtAutoShell** application using the following configuration:





```

1 | Display Name:  XtAutoShell
2 | Path/Filename: C:\app\XtAutoShell\XtAutoShell.exe
3 | Start Directory: C:\app\XtAutoShell
4 | Command Line Option: /wait
5 |
6 | Assign this application to All Users: Enabled/checked

```

5. Enable standard Remote Desktop access to this host server and enable permissions for the user account that you intend to define in your PAM Remote App Host record.

## Configuring Remote Apps record

### Step 2. Configuring the Remote Apps record types.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Record Types.
3. Locate the Record Type *Remote App Host* and click its **Edit** button.
4. Uncheck the option **Hidden** and then click **Save**.
5. Return to the Record Types page and repeat this process for the Record Type **MS SQL Studio**.

## 3. Remote App Host record

### Step 3. Creating your Remote App Host record.

This record will create the secure, remote connection to your TSplus server host.

1. Navigate to Records > All Records and (optionally) create a new folder.
2. Create a new Record using the type *Remote App Host*.
3. Enter a **Name** and **Description**.
4. Populate the following connection and configuration values:
  - **Host:** Enter the host name for the remote desktop connection to your Windows Remote Desktop Services server.
  - **Port:** Enter the port number for the remote desktop connection to your Windows Remote Desktop Services server.
  - **User:** Enter the user account that will establish the remote desktop connection and launch the published PAM Auto Shell program.
  - **Password:** Enter the password for this user account.
  - **Filter:** Enter the value MS SQL Studio. This defines which remote applications can be launched with the Remote App Host record. Empty value will permit any applications to be used.
  - **Remote App Platform:** Select TSplus from the dropdown menu.
  - **Enabled:** Check this box to enable this host for connection.
5. Click **Save and Return**.

#### 4. *Remote App Launcher record*

##### Step 4. Creating your Remote App Launcher record.

This record will be used by the PAM users to securely launch your MS SQL Server Management Studio remote application.

1. Create a new Record using the type *MS SQL Studio*.
2. Enter a **Name** and **Description**.
3. Populate the following connection and configuration values:
  - **Host:** Enter the server name for your MS SQL Database connection.
  - **User:** Enter the user account for your MS SQL Database connection.
  - **Password:** Enter the password for this user account.
4. Click **Save and Return**.

#### 5. *Testing your connection*

##### Step 5. Testing your Remote App connection.

1. Open the MS SQL Studio record that was created in the previous step.
2. Select the **Connect and Record** option to establish the connection with session recording enabled.
3. A new session will open. It will first establish a secure connection to your Remote App Host server and then it will launch the PAM Auto Shell script. Now, the PAM Auto Shell program will launch MS SQL Server Management Studio, populate the Server name, User and Password parameters automatically and open the database connection. Once the connection is made, keyboard and mouse controls will be returned to you.
4. Navigate through your MS SQL database and execute a few test SQL commands. Once satisfied, you may exit MS SQL Server Management Studio and then disconnect the secure remote session by closing this browser tab or window.

5. At this point, you may review the video and keystroke recordings by opening the **Sessions** tab for this record.

This completes the PAM Remote App Launcher using TSplus walkthrough.

For additional remote app topics and how-to guides, return to the **Remote App Launcher** main page and use the topics listed at the bottom to navigate the available articles.

[< Return to PAM Remote App Launcher](#)

## Windows RDS RemoteApp Launcher

PAM can be used to launch published RDS RemoteApps in a secure RDP session.

Using this feature, not only can it reduce the amount of effort one has to go through with traditional RemoteApp launching but it does so using the Privileged Session Management features of PAM to enable video and event recording, auditing, permissions, workflow approval and notifications.

If you are looking to preserve your native RemoteApp functionality but to do so in a more controlled and audited nature, then PAM is the solution for you.

For our Linux users, PAM also supports a similar feature where remote commands like connecting to a MySQL database can be automatically sent upon login. Read more about it [here](#).

Please note that while this guide uses MS SQL Server Management Studio as an example, credential injection via a script is a required step for all web-based applications. PAM provides pre-built scripts for certain applications; however, for other web applications, you must create a custom script tailored to their authentication process.

### *Cases and scenarios*

**The following use cases and scenarios are covered when configuring System to use your Windows RemoteApp infrastructure.**

- Provides end-users the ability to securely launch Remote Applications without having to use the traditional RDS Web Access portal.
- Easily capture video and keystroke recordings of all activity during their remote application sessions.
- Quickly share access using permissions and workflows to ensure users have access to the remote applications during the times when they need it the most.

### *Remote App Launcher Work*

**Remote App Launcher works with your existing Windows Desktop Services RemoteApp environment by:**

- Creating a secure connection to your Windows Desktop Services RemoteApp host.
- Launching the defined published RemoteApp without requiring additional user input or authentication.
- Once launched, enabling controls (mouse and keyboard) for the user so they can utilize the remote application.
- Recording keystrokes and (optionally) video of the user's session with the remote application.

- Retaining full support of native RDS Administrative Connections options including monitoring, Send Message, Shadow, Disconnect and Logout.

## Pre-requisites

To use the RDS RemoteApp Launcher, the following pre-requisites are required:

- Fully implemented, configured and working Windows Remote Desktop Services deployment. If you have not deployed a Windows Remote Desktop Services host yet, there are many online tutorials available with this one being an example: <http://www.concurrency.com/blog/w/rds8-quick-and-easy,-remoteapp-on-windows-server-2>
- The credentials entered into the System record must be included in the Collections properties as a member of User Group.
- The credentials entered into the System record must be able to connect to the RDS host server using RDP.
- The RemoteApp must be Published and the *RemoteApp program location* must be defined in the System record.
- This feature only works when connecting to a Windows RDS host server using Published RemoteApps.

## 1. Configure System to RemoteApps

To configure System to launch your published RemoteApps:

1. Login to the PAM with a System Administrator account.
2. Navigate to Administration > Record Types and click the **New Record Type** button.
3. Enter the following values to create your new record type:
  - **Name:** Windows Remote App or another name of your choosing
  - **Description:** (optional) Enter a description of this record type
  - **Session Manager:** RDP
  - **Parent Type:** Windows Host
4. Click the **Save** button to save your new record type.
5. Now click the **Add Field** button to create a custom field for this new record type. Use the following values for this new field:
  - **Field Type:** String
  - **Name:** Command
  - **Display Name:** RemoteApp Program Location or another name of your choosing
  - **Order:** 800
  - **Helper:** (optional) Enter the full path to the published RemoteApp on the RDS server
6. Click the **Save** button to save your new field.
7. Click the **Save** button to save your new record type.

Found 1 fields.

[Formula](#)
[Tasks](#)
[Commands](#)
[Save](#)
[Delete](#)
[Cancel](#)
[Reindex](#)
[↺](#)

**Name**

**Description**

**Session Manager**

**Parent Type**

**Hidden** ☐

**Personal Vault** ☐

[Add Field](#)

Field	Display Name	Field Type	Secured	Indexed	Helper	Actions
Command	RemoteApp Program Location	String				<a href="#">Edit</a>

Your record type is now ready to be used to create your Windows RemoteApp records.

## 2. Create a record

### To create a record used to launch your published RemoteApps:

1. Login to the PAM and navigate to the container where you will create your Windows Remote App record.
2. Click the **Add Record** button and select your new Record Type from the dropdown menu.
3. Create your record using the following values as guidance:
  - **Name:** Enter a name for your record
  - **Description:** (optional) Enter a description of your record
  - **Host:** Enter the host name or IP address of your Windows RDS host
  - **Port:** Enter the RDP port of your Windows RDS host (default is 3389)
  - **User:** Enter your domain user account. The same username you would use to login to the *RD Web Access* portal.
  - **Password:** Enter your domain password. The same password you would use to login to the *RD Web Access* portal.
  - **RemoteApp Program Location:** Enter the path of the published RemoteApp that will be launched on the RDS server from this record. For example, *C:\Windows\system32\calc.exe* or *%SYSTEMDRIVE%\Windows\system32\calc.exe*

Please consult with your Windows RDS Administrator if you need assistance with any of the values specific to your Remote App environment.

4. Click the **Save and Return** button to save your new record.

Windows RemoteApp Calculator Program

Name

Windows RemoteApp Calculator Program

Description

launch Calculator in a recorded RDS session

Host

10.0.0.134

Port

10024

User

xt\chrisk

Password

\*\*\*\*\*

RemoteApp Program Location

C:\Windows\system32\calc.exe

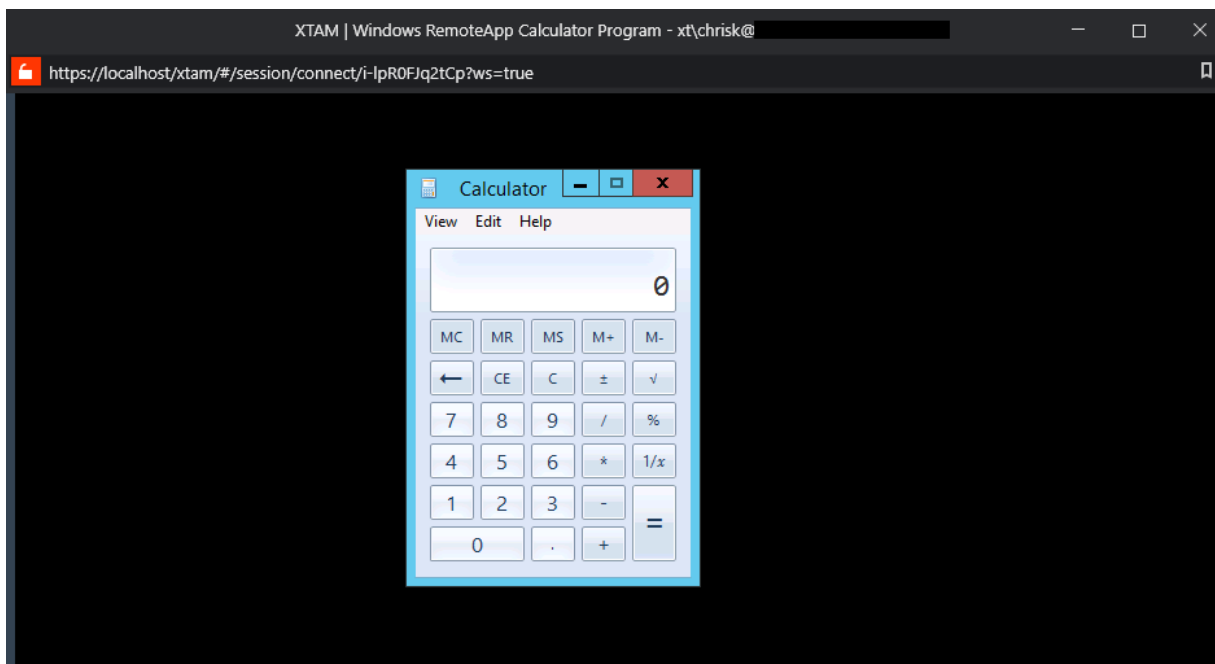
### 3. Testing Record

With the new record saved, you are ready to test your configuration. Return to this record’s View and click the **Connect** button to test this record’s function.

The expected result is that System will launch a remote RDP session to your RDS host, authenticating using the User and Password stored in the record.

Once the remote session is established, it will immediately launch the published RemoteApp that was defined in the RemoteApp Program Location field of the record.

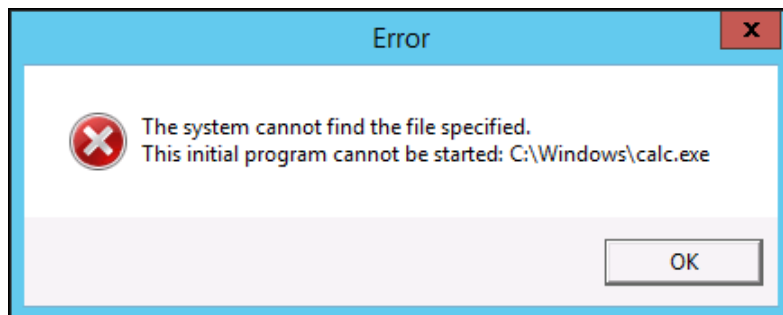
You can now use the RemoteApp and when finished, simply **Exit** or **Close the RemoteApp** and the System session will complete.



## Troubleshooting

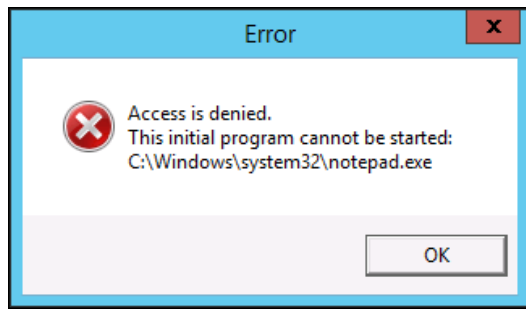
### Possible errors and decisions.

- **The remote session to your RDS server fails with connection error 519**
  - This failure is usually caused by an incorrect host, port or domain credentials stored in the record. Please verify that your User and Password are accurate and confirm with your RDS Administrator that the Host and Port are accurate. You should also make sure that RDP access to this host is available and your domain account is permitted to connect with this RDP session.
- **The remote session to your RDS server connects but the RemoteApp fails to launch with the error “The system cannot find the file specified. This initial program cannot be started:”**



This failure indicates that the path to the published Remote App in the System record is incorrect. Please verify this path and file name with your RDS Administrator to confirm its accuracy.

- **The remote session to your RDS server connects but the RemoteApp fails to launch with the error “Access is denied. This initial program cannot be started:”**



This failure indicates that the Remote App that you attempted to launch is not published.

Please verify that this Remote App is published with your RDS Administrator.

## Windows RDS MMC Snap-in Launcher (MSC)

PAM can be used to remotely launch MMC Snap-ins (MSC) in a secure RDP session. Using this feature, not only can it reduce the amount of effort one has to go through with traditional [RemoteApp](#) launching but it does so using the Privileged Session Management features of System to enable video and event recording, auditing, permissions, workflow approval and notifications.

If you are looking to provide users access to secured MSC console applications but do so in a more controlled and audited nature, then the PAM is the solution for you.

For our Linux users, the System also supports a similar feature where remote commands like connecting to a MySQL database can be automatically sent upon login. Read more about it [here](#).

To launch published application that are not MMC snap-ins, please see our RDS Launcher guide [here](#).

## Cases and scenarios

The following use cases and scenarios are covered when configuring the System to use your Windows RemoteApp infrastructure.

- Provides end-users the ability to securely launch MMC Snap-in consoles without providing direct access to the host server.
- Easily capture video and keystroke recordings of all activity during their remote MSC sessions.
- Quickly share access using permissions and workflows to ensure users have access to the remote applications during the times when they need it the most.

### MMC Launcher

System MMC Snap-in Launcher works with your existing Windows Desktop Services RemoteApp environment by:

- Creating a secure connection to your Windows Desktop Services RemoteApp host.
- Launching the defined MSC snap-in without requiring additional user input or authentication.
- Once launched, enabling controls (mouse and keyboard) for the user so they can utilize the MMC console.



- Recording keystrokes and (optionally) video of the user's session with the MMC console.
- Retaining support of native RDS Administrative Connections options.

## *Pre-requisites*

**To use the RDS MMC Snap-in Launcher, the following pre-requisites are required:**

- Fully implemented, configured and working Windows Remote Desktop Services deployment. If you have not deployed a Windows Remote Desktop Services host yet, there are many online tutorials available with this one being an example: <http://www.concurrency.com/blog/w/rds8-quick-and-easy,-remoteapp-on-windows-server-2>
- The credentials entered into the System record must be included in the Collections properties as a member of User Group.
- The credentials entered into the System record must be able to connect to the RDS host server using RDP.

## *1. System Configuration to Launch MMC Snap-ins*

**Step 1: To configure the System to launch your MMC Snap-ins:**

1. Login to the PAM with a System Administrator account.
2. Navigate to Administration > Record Types and click the **New Record Type** button.
3. Enter the following values to create your new record type:
  - **Name:** Windows MMC Snap-in Launcher or another name of your choosing.
  - **Description:** (optional) Enter a description of this record type
  - **Session Manager:** RDP
  - **Parent Type:** Windows Host
4. Click the **Save** button to save your new record type
5. Now click the **Add Field** button to create a custom field for this new record type. Use the following values for this new field:
  - **Field Type:** String
  - **Name:** RemoteApp
  - **Display Name:** MMC Snap-in Location or another name of your choosing
  - **Order:** 500
  - **Helper:** (optional) Enter the full path to the MSC snap-in file on the RDS server
  - **Default Value:** leave empty
6. Click the **Save** button to save your new field.
7. Click the **Save** button to save your new record type.

Record Type: Windows MMC Snap-in Launcher Extending [Windows Host](#)

Found 1 fields.

[Formula](#)
[Tasks](#)
[Commands](#)
[Edit Icon](#)
[Save](#)
[Delete](#)
[Cancel](#)
[Reindex](#)
[↺](#)

**Name**

**Description**

**Session Manager**

**Parent Type**

**Hidden** ☐

**Personal Vault** ☐

[Add Field](#)

Field	Display Name	Field Type	Default Value	Hidden	Secured	Indexed	Helper	Actions
Host	Host	String						Inherited
Port	Port	Number					3389	Inherited
User	User	String						Inherited
Password	Password	String			✓			Inherited
RemoteApp	MMC Snap-in Location	String						<a href="#">Edit</a>

Your record type is now ready to be used to create your MMC Snap-in Launcher record.

## 2. Create a record

### Step 2: To create a record used to launch your MMC Snap-in:

1. Login to the PAM and navigate to the container where you will create your *Windows MMC Snap-in Launcher* record.
2. Click the **Add Record** button and select your new *Record Type* from the dropdown menu.
3. Create your record using the following values as guidance:
  - **Name:** Enter a name for your record
  - **Description:** (optional) Enter a description of your record
  - **Host:** Enter the host name or IP address of your *Windows RDS host*
  - **Port:** Enter the *RDP port* of your Windows RDS host (default is 3389)
  - **User:** Enter a domain user account. This may be the same username you would use to login to the RD Web Access portal or a shared, privileged account with appropriate access to your *RDS Collection* and the snap-in to be launched.

- **Password:** Enter the User account's password.
- **MMC Snap-in Location:** Enter the path of the MSC snap-in that will be launched on the RDS server from this record. For example, `C:\Windows\System32\lusrmgr.msc` to launch the Local Users and Groups snap-in or `C:\Windows\System32\gpedit.msc` to launch the *Local Group Policy Editor* on the RDS host server.

On the RDS server, please add and publish as a RemoteApp the MMC Snap-in Location specified in the record. If app is not listed here by default select Add and find the location of the MSC snap in. See the example on the picture below.

**Publish RemoteApp Programs**

### Select RemoteApp programs

RemoteApp Programs  
Confirmation  
Publishing  
Completion

Select the RemoteApp programs to publish to the QuickSessionCollection collection. To add a RemoteApp program to the list, click Add.

The RemoteApp programs are populated from RDS-01.XTON.IMP.ENG.

RemoteApp Program	Location
<input type="checkbox"/> Steps Recorder	%SYSTEMDRIVE%\Windows\system32\psr.exe
<input type="checkbox"/> System Configuration	%SYSTEMDRIVE%\Windows\system32\msconfi...
<input type="checkbox"/> System Information	%SYSTEMDRIVE%\Windows\system32\msinfo3...
<input type="checkbox"/> Task Manager	%SYSTEMDRIVE%\Windows\system32\taskmgr....
<input type="checkbox"/> Windows Defender	%SYSTEMDRIVE%\Program Files\Windows Defe...
<input type="checkbox"/> Windows Media Player	%SYSTEMDRIVE%\Program Files (x86)\Windows...
<input type="checkbox"/> Windows Speech Recognition	%SYSTEMDRIVE%\Windows\Speech\Common\s...
<input type="checkbox"/> WordPad	%SYSTEMDRIVE%\Program Files\Windows NT\...
<input checked="" type="checkbox"/> lusrmgr	c:\Windows\System32\lusrmgr.msc

Add...

Verify that the program is installed on all the RD Session Host servers in the collection.

< Previous   Next >   Publish   Cancel

Please consult with your Windows RDS Administrator if you need assistance with any of the values specific to your Remote App environment.

4. Click the **Save and Return** button to save your new record.

## Local Users and Groups MMC Snap-in Launcher

**Name** Local Users and Groups MMC Snap-in Launcher

**Description**

**Host** 10.0.0.24

**Port** 10024

**User** xt\remoteappuser

**Password** \*\*\*\*\*

**MMC Snap-in Location** C:\Windows\system32\lusrmgr.msc

### 3. Testing Record

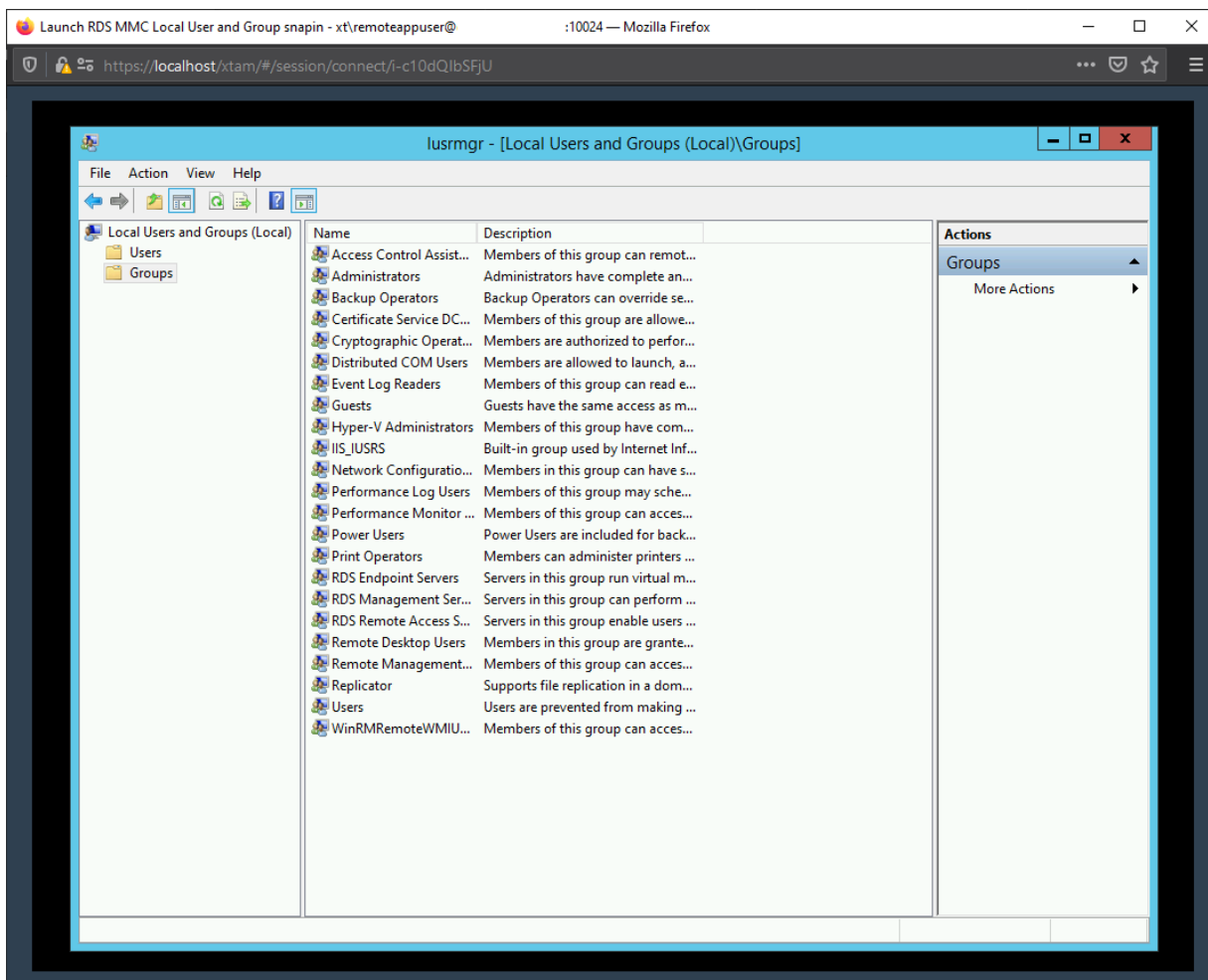
#### Step 3: Testing your Record

With the new record saved, you are ready to test your configuration. Return to this record's View and click the **Connect** button to test this record's function.

The expected result is that System will launch a remote RDP session to your RDS host, authenticating using the User and Password stored in the record.

Once the remote session is established, it will immediately launch the MMC Snap-in that was defined in the MMC Snap-in Location field of the record.

You can now use the MMC Snap-in and when finished, simply close the browser tab or window to complete your System session.



## Launching MMC snap-ins

Use the following String fields to customize the behavior of the launch of the Remote Application technology on the RDS server remote applications:

- **RemoteApp** – the name of the remote application to start
- **RemoteAppArgs** – optional parameters of the remote application
- **RemoteAppDir** – initial folder to launch remote application in

## Troubleshooting

### Possible errors and decisions.

- The remote session to your RDS server fails with connection error 519
  - This failure is usually caused by an incorrect host, port or domain credentials stored in the record. Please verify that your User and Password are accurate and confirm with your RDS Administrator that the Host and Port are accurate. You should also make sure that RDP access to this host is available and your domain account is permitted to connect with this RDP session.
- The remote session to your RDS server connects but the MMC Snap-in fails to launch.
  - This behavior may occur when the MMC console is not a published application on your remote host or this user does not have RDS permissions to launch the MMC console. Please check that both the MMC application is a published application and the User in the System record has permissions to use the published application.

# Additional-Topics

## Command Execution During SSH Login

Automatic Execution of Remote Commands for SSH Enabled or Unix Sessions.

When establishing a remote session to a SSH-enabled endpoint this ultimately leaves the user at the terminal prompt to execute or access anything they are permissioned to do.

Although this may be desirable for most endpoints, there are instances where you may wish to restrict a user's access to a single application.

This is where PAM's automatic command execution can be utilized.

Using an PAM Unix Host Command record type, it first creates the remote session and then immediately executes a command before handing over controls to the user, optionally providing a password retrieved from the record to be used by the command to access a specific resource.

This allows you to provide a secure remote session to your Unix endpoint but limits their activities to the command that was initially executed.

For example, you want your Administrator to connect on your Unix endpoint to manage your MySQL production database but you don't want them to have free-range on the endpoint to perform any other actions.

So you create the remote session using PAM which then immediately issues the command to connect to the MySQL database (without disclosing the password).

This keeps your Administrator within the boundaries of the MySQL prompt so they can perform their tasks.

Once finished, they can simply disconnect from MySQL and the remote session will end. Enable video and keystroke recording on this session for added security.

This is similar to the [Remote Application functionality](#) that is available for Windows sessions where specific applications are launched from a remote app host which sandboxes the user to work within this single, native application only.

*To configure Automatic Command Execution for Browser-based or Native SSH Client Use:*

1. Login to PAM as a System Administrator and navigate to Administration > Record Types.
2. Locate the Record Type **Unix Host Command** and click the **Edit** button.

<input checked="" type="checkbox"/>	Unix Host Command	Unix Host	SSH_EXEC	<input checked="" type="checkbox"/>	Edit
-------------------------------------	-------------------	-----------	----------	-------------------------------------	------

3. Uncheck the **Hidden** option and click **Save**.
4. Return to the Record List and create a new record using the type *Unix Host Command*.
5. Populate the values in the record as needed:

- a. **Name:** Enter a name for this new record.
- b. **Description:** Enter a description for this new record.
- c. **Host:** Enter the host name for your remote session.
- d. **Port:** Enter the port number for your remote session.
- e. **User:** Enter the user that will be used to create your remote session.
- f. **Password:** Enter the password for this user.
- g. **Remote Command:** Enter the remote command that will be automatically executed when the remote session is created. For example, to connect to a database using the MySQL client:  
mysql -u admin -p -h 10.0.0.33 Master.
- h. **Command Password:** If the remote command requires a password, enter this password to authorize this command. For example, the password for the *-u admin* in the previous Remote Command parameter.

Production Unix MySQL DB
Go to Parent
Connect...

Name	Production Unix MySQL DB		
Description	Use for MySQL db management only		
<hr/>			
Host	10.0.0.26		
Port	*****		
User	unix01		
Password	*****		
Remote Command	mysql -u admin -p -h 10.0.0.33 Master		
Command Password	*****		

6. Click **Save and Return** when finished.

With the record now created, test by establishing a browser-based session using the **Connect** option or use your native SSH client.

You should see that PAM creates the remote session and then automatically executes your Remote Command.

```
XTAM | Production Unix MySQL DB - unix01@10.0.0.26:*****
http://xtam/#/session/connect/1148106?rec=true
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.7.18-log MySQL Community Server (GPL)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from usr;
+-----+-----+-----+-----+-----+
| DIRECTORY_TYPE | FIRST_NAME | LAST_NAME | USER_TYPE | ID |
+-----+-----+-----+-----+-----+
| ApacheDS       | Service   | Service   | User      | 1  |
| ApacheDS       | Service   | Administrator | User      | 11 |
| ApacheDS       | 1         | 1         | User      | 115 |
+-----+-----+-----+-----+-----+
3 rows in set (0.00 sec)

mysql> 
```

Note that command execution can be used with any other Unix record type like *Unix Host with Key* by simply adding these two fields (*Command* and *CommandPassword*) to the record type or using record type inheritance. Please see our article [Creating Custom Record Types](#) for additional information.

## Custom Remote App Launcher Record Types

The following article will describe the process to create your own high trust remote application launcher in PAM.

PAM uses scripts written and developed for Autolt, so if you are not familiar with that application or its scripting language, it's a good time to learn more about it [here](#).

Now that you are familiar with Autolt, let's continue with the article.

### Autolt Record

1. Login to PAM using a System Administrator account.
2. Navigate to Administration > Scripts.
3. Click the **Create** button to create your new Remote App launcher script.
4. Enter a *Script Name*, *Description* and for *Job Execution Strategy* select the option **RemoteApp**.
5. Write or paste in your Autolt script in the **Custom Code** (Autolt) field. For an example script, click [here](#).
6. Click the **Save** button when you are finished.



7. With the script saved, navigate to Administration > Record Types and click the **New Record Type** button.
8. Enter a **Name, Description, Session Manager** select *RemoteApp* and finally for Remote App Script select *your new script name* from the previous step.
9. Create the rest of the [record type](#) as needed. For example, if you create a custom field named *URL*, then you can reference this value in your remote app script so that Autolt will automatically enter it during connection.
10. Click **Save** when you are finished.

Now you can navigate to Records > All Records and create a new record using this record type. Test the new record by clicking the **Connect** button to ensure it is working as expected before deploying to production.

Please note that while this guide uses MS SQL Server Management Studio as an example, credential injection via a script is a required step for all web-based applications. PAM provides pre-built scripts for certain applications; however, for other web applications, you must create a custom script tailored to their authentication process.

Remember, this procedure requires the prior deployment and configuration of [Windows Remote Desktop Services with RemoteApp](#) functionality, so if you have not configured your Remote App Host connection yet, it is recommended to review this [Getting Started Guide](#).

## PAM Autolt Script Examples

### MS SQL Server Management Studio Remote App Launcher Script

```

1  #include <XTAM.au3>
2
3  Local Const $SSMS_EXECUTABLE = "C:\Program Files (x86)\Microsoft SQL
  Server\140\Tools\Binn\ManagementStudio\Ssms.exe"
4  Local Const $SERVER_CLASS = "[CLASS:Edit; INSTANCE:1]"
5  Local Const $LOGIN_CLASS = "[CLASS:Edit; INSTANCE:2]"
6  Local Const $PASSWD_CLASS = "[NAME:password]"
7  Local Const $CONNECT_CLASS = "[NAME:connect]"
8  Local Const $AUTH_CLASS = "[NAME:comboBoxAuthentication]"
9  Local Const $WIN_MAIN = "[REGEXPTITLE:(?i)(.*Microsoft SQL Server Management
  Studio)]"
10
11 Local $hostname
12 Local $username
13 Local $password
14
15 $params = XtamGetProperties()
16
17 $len = Ubound($params)
18
19 For $i = 0 to $len - 1 Step 2
20     If $params[$i] = "Host_raw" Then
21         $hostname = $params[$i+1]
22     ElseIf $params[$i] = "User_raw" Then
23         $username = $params[$i+1]
24     ElseIf $params[$i] = "Password_raw" Then
25         $password = $params[$i+1]
26     EndIf
27 Next
  
```

```

28
29 ConsoleWrite("Executing " & $SSMS_EXECUTABLE & @CRLF)
30 $process = Run($SSMS_EXECUTABLE)
31
32 If @error Then
33     ConsoleWrite("Failed to run program: " & @error & @CRLF)
34     Exit
35 EndIf
36
37 ConsoleWrite("Waiting for window" & @CRLF)
38 WinWaitActive("Connect to Server", "", 10000)
39 $hwnd = WinGetHandle("Connect to Server")
40
41 ConsoleWrite("Input params" & @CRLF)
42 ControlSend($hwnd, "", $AUTH_CLASS, "S") ; select 'SQL Server
Authentication' type
43 ControlSetText($hwnd, "", $SERVER_CLASS, $hostname)
44 ControlSetText($hwnd, "", $LOGIN_CLASS, $username)
45 ControlSetText($hwnd, "", $PASSWD_CLASS, $password)
46 ControlSend($hwnd, "", $CONNECT_CLASS, "{ENTER}")
47
48 XtamSendDone()
49
50 ConsoleWrite("Waiting application close" & @CRLF)
51 WinWaitClose($WIN_MAIN)
52 ConsoleWrite("Exiting..." & @CRLF)
53
54 Shutdown(0) ; Logoff

```

## Dynamic Login Credentials

### Dynamically Use Stored Credentials to Login to a Remote Session.

Like Pass-Through configuration, Dynamic Login allows a record to be created without including a specific set of credentials (user and password) in your system record.

In addition to not including the credentials, Dynamic Login provides a search criteria where the System can dynamically use the credentials included in another record based on these search results.

Also, this Dynamic credential option provides the benefit of using different credentials to access remote servers for different users accessing the system.

The search criteria for this dynamic credential option is parametric and depends on user attributes (such as login name).

### Example

For example, you want to store user credentials in the System for your Admin accounts and you do not want to expose these credentials to the actual Administrators themselves.

So you create these login records in the System, assign a complex Password Rotation policy and then dynamically load these credentials when the Admins connect to the endpoint using another record, all without revealing the credentials to this user.

Cross-vault dynamic credentials search usage is not allowed. This means if you have dynamic credentials for a specific user finding a record from another vault then the user will fail to **Connect** with the audit log message **Failure** to activate dynamic credential to find a record from the same vault using criteria: **CRITERIA**.

The reason for this restriction is to prevent users from creating records in the place they can create them (personal vaults or vaults they can create records) using credentials stored in the vault with another role- or access-based restrictions.

You can disable this cross-vault blocker by adding the following line to your `$PAM_HOME/web/conf/catalina.properties` file and then restarting the pam management service:

```
1 | xtam.shadow.crossvault.disable=true
```

### To create Dynamically Loaded Login Records

1. Create a record that will contain the actual User and Password that will be dynamically loaded. If you wish to rotate this password, create the record using **Windows Host** or **Unix Host**. Otherwise, you can use any record type that contains the default User and Password fields.
2. In this record's **Name** or **Description**, enter a unique value that will be used in the search for your Host record. For example, put the User name like `user@domain.com` in the description so System search can locate it.

Windows Host Dynamic Login chrisk

Go to Parent

Connect...

Execute...

Name

Windows Host Dynamic Login chrisk

Description

Dynamic login for chrisk@DEMO-SERVER-WIN

Host

10.0.0.24

Port

10024

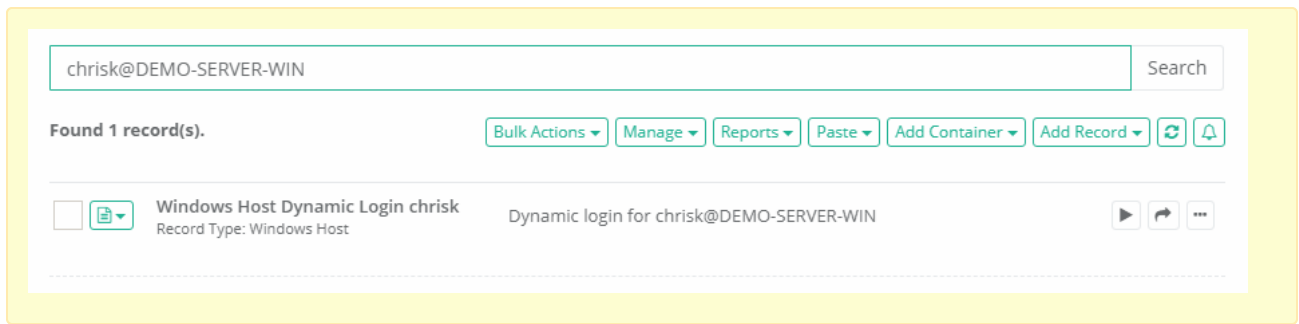
User

DEMO-SERVER-WIN\chrisk

Password

\*\*\*\*\*

Make sure this value is truly unique because system search can return only 1 record in order for dynamic login to work properly.



3. When finished, click the **Save and Return** button.
4. Now we are going to create the host record that will dynamically load the credentials from the previously created record. Create this host record using any record type that contains a User and Password fields.
5. Enter all information as needed. In the **User** field, we are going to create our search query that will locate our previous record. To create the query, use the following format: **\$search:{criteria}**

For example, to find our previous record your search criteria would look like this:

**\$search:user@domain.com**

Which uses the System search to find any records where the *Name*, *Description* or *Host* contains the value “user@domain.com”.

Alternatively, if your user logs in to System with the username “bwilliams”, then you could construct the query like this so that each user can have their own unique login credential:

**\$search:\$login@domain.com**

This query would then search for any records where the Name, Description or Host contains the value “bwilliams@domain.com”.

In addition to **\$login** placeholder for the currently logged in user account name, record owners might use **\$first-name** and **\$last-name** placeholders to base search criteria on first or on the last name of the currently logged in user.

**Name** Windows Host Dynamic Login

**Description** Dynamic login for Windows Host

**Host** 10.0.0.24

**Port** 10024

**User** \$search:\$login@DEMO-SERVER-WIN

**Password** \*\*\*\*\*



6. When finished, click the **Save and Return** button.

Now to test, simply login to the System with a user account that has the appropriate permissions on this endpoint and click the **Connect** button on its record.

The System will dynamically load the credentials from the first record which will then be used to authenticate and log in to the remote endpoint defined in this record.

To confirm, you can open the record's Audit Log and observe which account was dynamically loaded to the remote endpoint as shown below.

#### Windows Host Dynamic Login

Found 23 audit log records.



Show 50 entries

Search:  CSV PDF

Showing 1 to 23 of 23 entries

Time	User	IP	Category	Level	Event	Message
08/13/2018 10:06:56	Chris Kolodziejki (chrisk)		Operation	INFO	Connect	Activated dynamic credential with user: DEMO-SERVER-WIN\chrisk

Dynamic-login credentials support connections to remote sessions (Web and/or Proxy Sessions) as well as automation of execution of jobs/tasks in limited use cases. (Please be aware that combinations of any/all Pass-through place holders such as **\$login**, **\$user**, and **\$account** along with Dynamic-login credentials does **NOT** support the automation or execution of jobs/tasks).

## Pass-Through Login Credentials

Pass-through of login credentials will automatically use the currently logged in PAM user account to also authenticate against the remote session.

This provides the benefit of not having to define a specific shared account to be used with this record's connection and it will also provide a more seamless login experience for your users.

Also this pass-through credential option provides the benefit of being able to use your own login while auditing, recording and managing session access with workflows.

Please keep in mind that the pass-through credentials feature will only work with endpoints that support a User and Password login.

**To configure Remote Pass-Through on a record:**

1. Create a new record or Edit an existing record that connects to a remote endpoint using a User and Password authentication method. For example, a *Windows Host* record type.
2. In the User field, enter the value **\$forward** or **\$login**.

Windows Host Pass-Through Go to Parent Connect Execute... ▼

**Name**

Windows Host Pass-Through

**Description**

Pass-through XTAM credentials to login to remote endpoint

**Host**

10.0.0.24

**Port**


10024

**User**

\$login

**Password**

\*\*\*\*\*



3. Optionally, you may remove the *Password* value.
4. Click the **Save and Return** button when finished.

Now to test, simply login to PAM with a user account that has the appropriate permissions on this endpoint and click the **Connect** button on its record. PAM will pass-through the credentials used to login to it to the remote endpoint for session authentication.

To confirm, you can open the record's Audit Log and observe which account was passed through to the remote endpoint as shown below.

Found 32 audit log records.



Show 50 entries

Search:

CSV

PDF

Showing 1 to 32 of 32 entries

Time	User	IP	Category	Level	Event	Message
08/13/2018 11:36:58	IT Admin (itadmin)		Operation	INFO	Connect	Activated pass-through credential for user: itadmin

Use **\$user** placeholder instead of **\$login** one to make the system to use user name as the login of the current user while still using the password on record to connect.

Note that **\$user**, **\$login** or **\$search** placeholders might be used as a component of more complex pattern such as in this example: *admin-\$login*. In this case, the system will generate user name based on the login of the current user and the pattern provided.

If the system user is supported with a UPN format, use **\$account** placeholder instead of **\$login**. The system will use the current logged in users credentials to connect to the record. (The **\$account** placeholder will remove the "**@domain**" portion of the username, An example: *admininstrator@pam* will be replaced as *administrator*.)

Pass-through credentials only support connections to remote sessions (Web and/or Proxy Sessions). All Pass-through place holders such as **\$login**, **\$user**, and **\$account** do **NOT** support the automation or execution of jobs/tasks.

## Prompt for Credentials

User Prompt for Remote Connection Parameters.

When records to be used for Remote Sessions are typically created, the owner of the record defines the connection parameters including Host, Port, User and Password.

This allows the PAM user to easily connect to this remote session with a single click, while ensuring the record's are accurate.

However, there are valid reasons where the record Owner would like the PAM user to define their own host or user credentials during connection.

This includes, but is certainly not limited to, Network Administrators who are used to or are permitted to use their personal network credentials.

If you would like to configure this type of record, then please perform the following procedure in PAM and then share this record with your users.

The ability to prompt users for connection parameters currently supports the record parameters Host, Port, User and Password.

[To prompt a user for a host or port during connection](#)

[To prompt a user for user and password credentials during connection](#)

[To prompt a user for all parameters during connection](#)

[To prompt a user for a port using the SSH Proxy \(dynamic port\)](#)

[To prompt a user to select from a list of available hosts](#)

## Prompting Host or Port

To prompt a user for a Host or Port during connection:

1. Login to PAM as a user with the [permission to create a new record](#).
2. Create a new Record using the *Add Record* menu.
3. Select a Record Type that contains the parameters Host, Port, User and Password fields. For example, *Windows Host* or *Unix Host*.
4. Enter a **Name** for the new record (required).
5. Enter a **Description** for the new record (optional).
6. Enter a **User** for the new record.
7. Enter a **Password** to the User for the new record.

Define Remote Host

Name

Define Remote Host

Description

Use this record to connect to a Windows Host

Reference Record

Search reference record...

Type

Windows Host

Host

Port

3389

User

itadmin@xt.com

Password

.....

Save

Save and Return

Cancel

8. Click the **Save and Return** button to complete the record creation.



When a PAM user clicks the **Connect** button for this record, they will be required to populate the Host and/or Port number to establish the remote host.

The User and Password defined in the record will be used to connect.

### Connection Parameters

Host

Port

### *Prompting for User and Password credentials*

To prompt a user for User and Password credentials during connection:

1. Login to PAM as a user with the [permission to create a new record](#).
2. Create a new Record using the **Add Record** menu.
3. Select a Record Type that contains the parameters Host, Port, User and Password fields. For example, *Windows Host* or *Unix Host*.
4. Enter a **Name** for the new record (required).
5. Enter a **Description** for the new record (optional).
6. Enter a **Host** for the new record.
7. Enter a **Port** to the User for the new record.

## Define Login Credentials

Name	Define Login Credentials
Description	Use this record to connect to a Windows Host using your own login
Reference Record	Search reference record...

---

Type	Windows Host
Host	10.0.0.24
Port	10024
User	
Password	<input type="password"/>

---

SaveSave and ReturnCancel

8. Click the **Save and Return** button to complete the record creation.

When a PAM user clicks the **Connect** button for this record, they will be required to populate the User and Password to establish the connection to the remote Host and Port already defined.

### Connection Parameters

User

chrisk@xt.com

Password

.....

Cancel

Connect

### Prompting for All parameters


To prompt a user for All parameters during connection:

1. Login to PAM as a user with the [permission to create a new record](#).
2. Create a new Record using the **Add Record** menu.
3. Select a Record Type that contains the parameters Host, Port, User and Password fields. For example, *Windows Host* or *Unix Host*.
4. Enter a **Name** for the new record (required).
5. Enter a **Description** for the new record (optional).

## Define All

Name	Define All
Description	Use this record to connect to a Windows Host with your own credentials
Reference Record	Search reference record...

---

Type	Windows Host
Host	
Port	3389
User	
Password	<input type="password"/> 

---

Save Save and Return Cancel

6. Click the **Save and Return** button to complete the record creation.

When a PAM user clicks the **Connect** button for this record, they will be required to populate the Host, Port, User and Password to establish the remote connection. The Audit, Session and Recordings will be captured in the same manner as if all connection parameters were pre-defined in the record.

### Connection Parameters

#### Host

#### Port

#### User

#### Password

CancelConnect

## To prompt a user for a port using the SSH Proxy (dynamic port)

1. Login to PAM as a user with the [permission](#) to create a new record.
2. Create a new Record using the **Add Record** menu.
3. Select a Unix based Record Type that at least contains the parameters Host and Port fields. For example, *Unix Host* or *Unix Host with Key*.
4. Enter a **Name** for the new record (required).
5. Enter a **Description** for the new record (optional).
6. Enter a **Host** for the new record (required).
7. Enter a 0 (zero) in the **Port** for the new record (required).
8. Enter valid values for the remaining fields in the record (required).

### Prompt for Port Number

Name	Prompt for Port Number		
Description	Prompt the User to enter the valid port for the host connection		
Reference Record	Search reference record...		

---

Type	Unix Host		
Host	192.168.1.75		
Port	0		
User	root		
Password	<div>.....</div>		<div><div></div><div></div></div>

Password is Very Strong.

Save

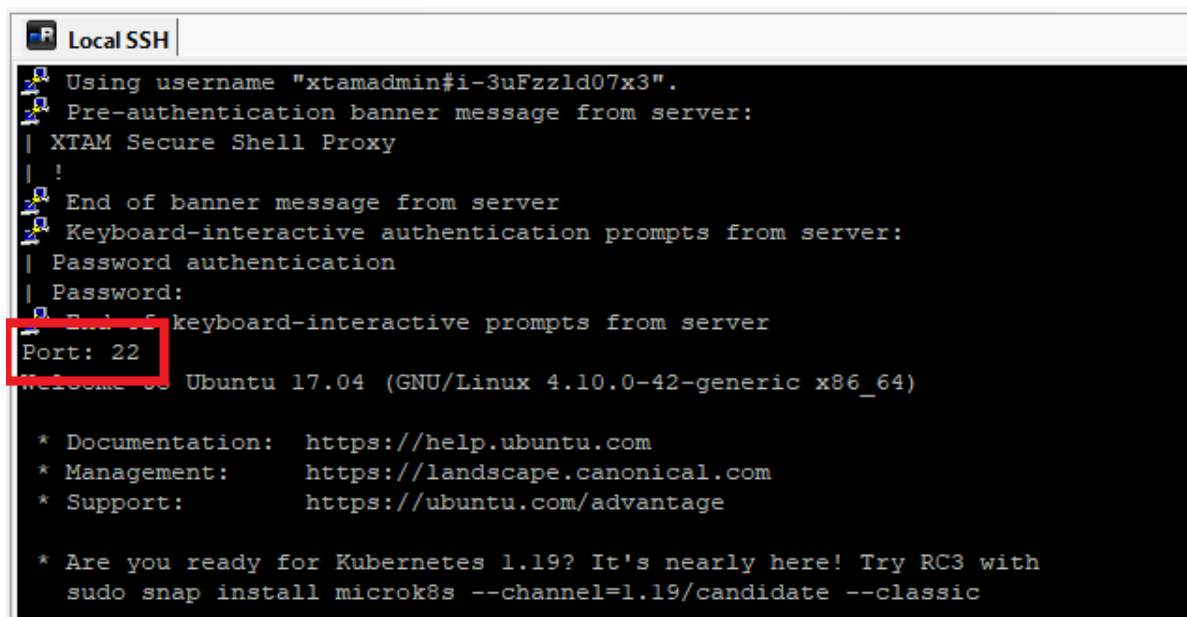
Save and Return

Cancel

9. Click the **Save and Return** button to complete the record creation.

When a PAM user connects with the SSH Proxy using this record, after authentication they will be required to enter the valid SSH port for this host to establish the remote connection.

The Audit, Session and Recordings will be captured in the same manner as if all connection parameters were pre-defined in the record.



```
Local SSH
Using username "xtamadmin#i-3uFzzld07x3".
Pre-authentication banner message from server:
| XTAM Secure Shell Proxy
| !
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password authentication
| Password:
| End of keyboard-interactive prompts from server
Port: 22
Welcome to Ubuntu 17.04 (GNU/Linux 4.10.0-42-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

* Are you ready for Kubernetes 1.19? It's nearly here! Try RC3 with
  sudo snap install microk8s --channel=1.19/candidate --classic
```

### *To prompt a user to select from a list of available Hosts*

A record may contain a predefined list of **whitelisted Host** or **Host:Post** values that will allow a user to select one for connection.

To configure this feature, you will need [to create a custom field](#) in your [Record Type](#) which will require [the System Administrator role](#).

To create this custom field:

1. **Login** to PAM with a System Administrator account.
2. Navigate to Administration > Record Types and click the **Edit** button for the record type in which you wish to enable this feature.
3. On the Record Type edit page, click the **Add Field** button and create your new field using these values:
  - Field Type: **Text**
  - Name: **Hosts**
  - Display Name: **Hosts**
4. Click **Save** when complete.

## Edit Field: Hosts

Field Type	<div>Text</div>
Name	<div>Hosts</div>
Display Name	<div>Hosts</div>
Hidden	<input checked="" type="checkbox"/>
Secured	<input type="checkbox"/>
Indexed	<input type="checkbox"/>
Order	<div>500</div>
Helper	<div></div>
Default Value	<div></div>

Once the new field has been created, return to an existing record that uses this type or create a new record of this record type.

1. Enter a **Name** for this new record (required).
2. Enter a **Description** for this new record (optional).
3. Enter a **User** for this new record.
4. Enter a **Password** to the User for the new record.
5. Enter a comma separated list of **whitelisted Host** or **Host:Port** values in the **Hosts** field.
6. If **Host** or **Port** fields are present, leave both empty.

Host Selector

Go to ParentConnect...Execute...

Name	Host Selector
Description	
User	localadmin
Password	*****
Hosts	10.0.0.1:3389,10.0.0.2:3389,10.0.0.158:1015,10.0.0.188,ZTWUIN122-XS08,10.0.0.3:3389,10.0.0.4:3389

Finally, when the user clicks the **Connect** option, they will be presented with a list of these predefined Hosts that they may select from to start their remote session.

Connection Parameters

Host

Filter

10.0.0.1:3389

10.0.0.2:3389

10.0.0.158:1015

10.0.0.188

ZTWUIN122-XS08

10.0.0.3:3389

10.0.0.4:3389

Cancel

Connect

## Setup SSH Tunnel Access

A common scenario we hear from our users is that they want to provide access to an internal resource (for example, a production database) without having to open access to it externally.

In addition, allowing their Admins and Developers to continue to use their native client tools is usually a must have requirement.

So how can you satisfy such a requirement while maintaining security?

The answer is simple; use PAM's privileged access management while employing SSH tunnels. Using a secure, password-less SSH session to the jump server, the user's traffic from their client is then tunneled to the desired endpoint.

Other common scenarios where SSH Tunnels are used:

- Ports cannot or should not be opened
- The service or system should only be accessible internally
- Firewall configurations
- Security architecture requires it

To enable the capturing of SQL statements to the PAM Session Event report, please read our [Capturing SQL Traffic](#) article.

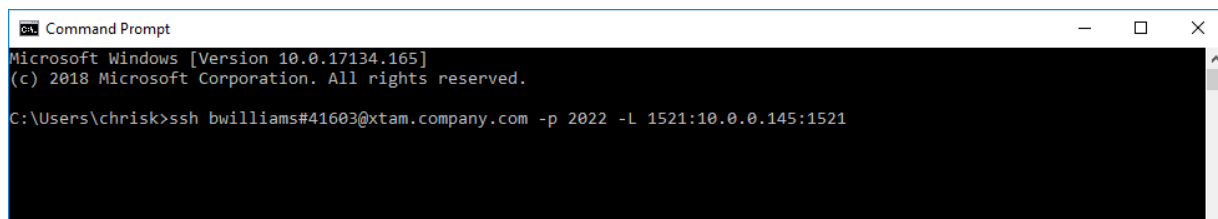
In the following example, we will demonstrate how PAM is configured to use a Unix jump server in order to provide a SSH tunnel from an external SQL Developer client to an internal Oracle database.

To make use of SSH tunneling, you first must enable the SSH Proxy feature in PAM. If you have not this feature yet, please first read our [SSH Proxy article](#) and then return here when complete.

1. Create a Unix record in PAM that will be used as the jump server for the ssh tunnel.
2. Open your preferred SSH client (our example is using the Windows 10 Command Prompt) and create your tunnel using the following syntax:

```
1 | ssh <your PAM userName>#<PAM record name or ID of the jump server>@<PAM host url>-p <PAM SSH Proxy port number> -L <local listening port>:<remote host>:<remote listening port>
```

For example:



```
Command Prompt
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\chris>ssh bwilliams#41603@xtam.company.com -p 2022 -L 1521:10.0.0.145:1521
```



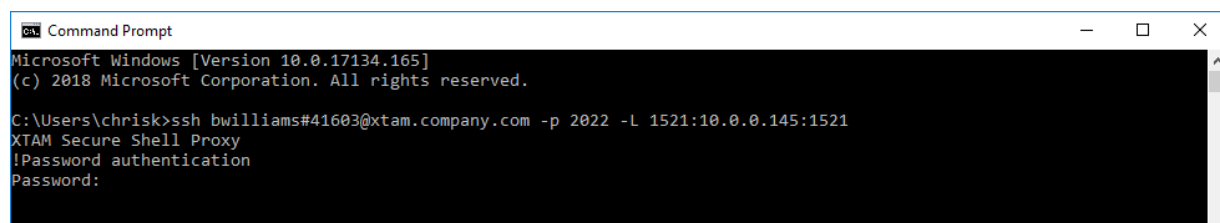
```
1 | ssh bwilliams#41603@xtam.company.com -p 2022 -L 1521:10.0.0.145:1521
```

- **bwilliams** – our PAM user
- **41603** – our PAM record ID for our Unix jump server. You can also use the PAM record Name, assuming it is unique.
- **xtam.company.com** – our PAM host URL
- **2022** – our PAM SSH Proxy port number
- **1521** – our local listening port (1521 is the default for Oracle)
- **10.0.0.145** – our Oracle database host IP
- **1521** – our remote listening port
- **-N** – (optional) to create the tunnel as a user with the “nologin” shell

On other operating systems, you may use other SSH products. For example, on Unix you can simply use the ssh command or on Windows you could use PuTTY.

Also, many applications like SQL Developer or MySQL Studio have their own SSH Tunnel configuration options which can be used instead of a separate SSH client.

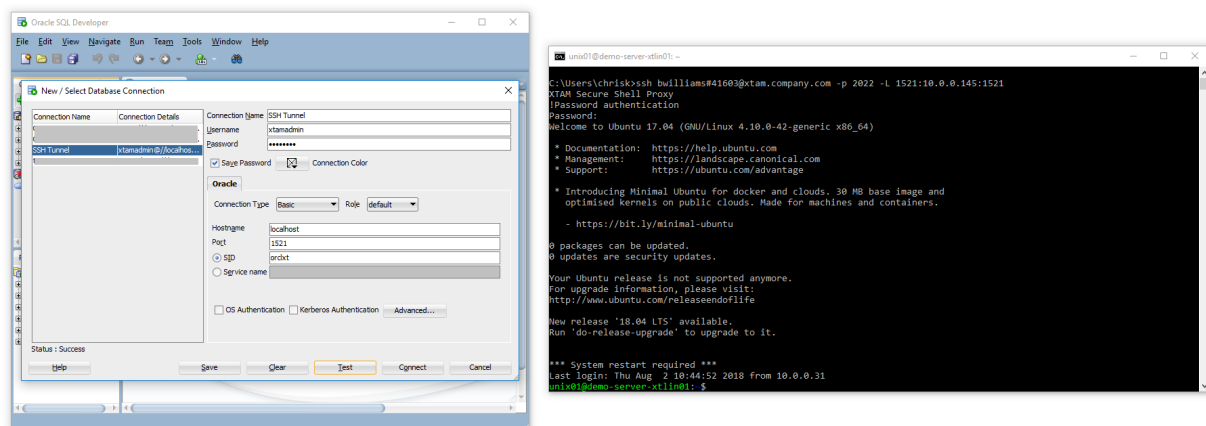
3. You should now see the display message PAM Secure Proxy Shell indicating that the traffic is being routed through PAM. At the password prompt, enter the PAM user’s password.



```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\chris>ssh bwilliams#41603@xtam.company.com -p 2022 -L 1521:10.0.0.145:1521
XTAM Secure Shell Proxy
!Password authentication
Password:
```

4. Once authenticated, the SSH tunnel is created. We can now connect to our internal Oracle database using localhost or 127.0.0.1 as the Hostname and port 1521. The traffic will be forwarded to the destination server behind our firewall.



5. When finished, you can close the tunnel.

```
Command Prompt
Password:
Welcome to Ubuntu 17.04 (GNU/Linux 4.10.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Introducing Minimal Ubuntu for docker and clouds. 30 MB base image and
   optimised kernels on public clouds. Made for machines and containers.
   - https://bit.ly/minimal-ubuntu

0 packages can be updated.
0 updates are security updates.

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

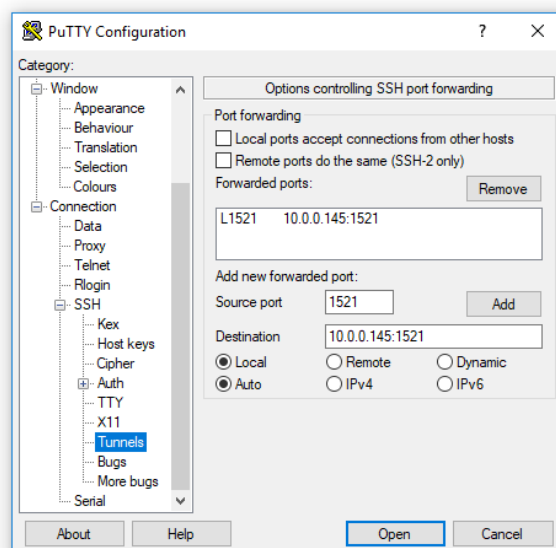
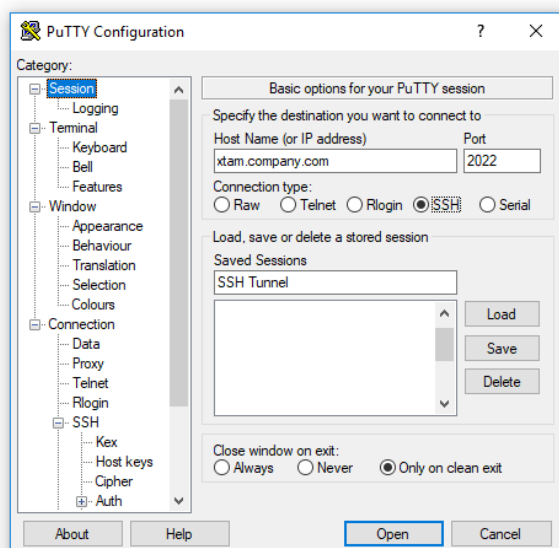
New release '18.04 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Thu Aug  2 11:11:38 2018 from 10.0.0.20
unix01@demo-server-xtlin01:~$ exit
logout
Connection to xtam.company.com closed.

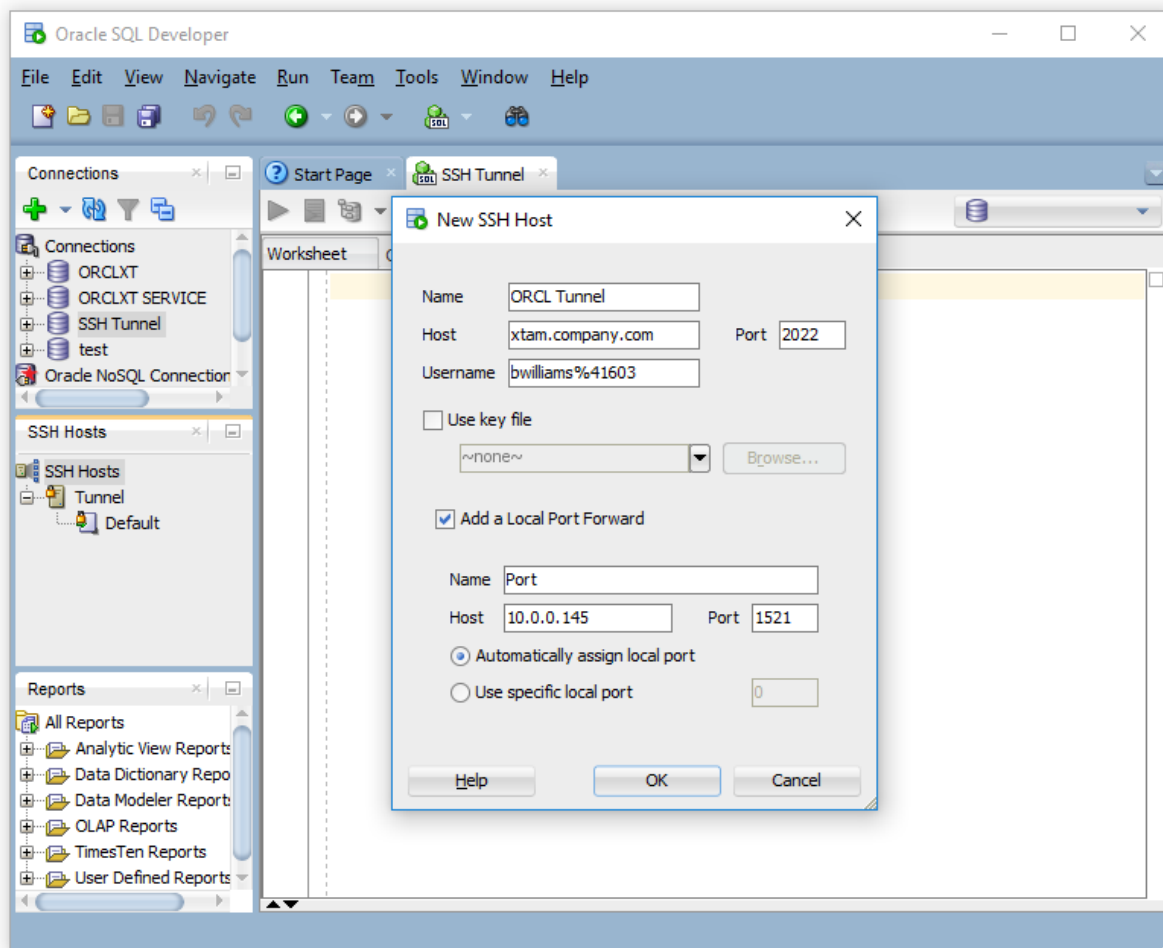
C:\Users\chris>
```

## Application SSH Tunnel Configuration Examples

### PuTTY



## Oracle SQL Developer



## SSH Sudo Execution or SU Utility Execution

Control Elevated Privilege in a SSH/SU session (sudo execution or directly executing su utility).

PAM includes the option to control the command to elevate privilege in a SSH/SU session to run through sudo execution or directly executing su utility.

With this option included, the system will use `exec sudo su – user` command to elevate user privilege instead of the default `exec su – user` command.

The option is controlled by a custom record-level field Type on *Unix with SU* record type or its inherited derivatives.

- **Field Type:** Checkbox
- **Name:** sudo
- **Display Name:** Use sudo
- **Order:** 620

## Record Type: Unix Host with SU Extending [Unix Host](#)

### Edit Field: sudo

Field Type	<input type="text" value="Checkbox"/>
Name	<input type="text" value="sudo"/>
Display Name	<input type="text" value="Use sudo"/>
Secured	<input type="checkbox"/>
Indexed	<input type="checkbox"/>
Order	<input type="text" value="620"/>

You will need to create this custom field within a Record Type. To learn about creating custom fields, please review [this article](#).

Now, within the record that uses the Record Type with this custom field, you will have a checkbox option named *Use sudo*.

## Unix Host with SU Session

<b>Name</b>	Unix Host with SU Session
<b>Description</b>	unix host session (external) with user + pass and SU

<b>Host</b>	10.0.0.26
-------------	-----------

<b>Port</b>	22
-------------	----

<b>User</b>	unix01
-------------	--------

<b>Password</b>	*****
-----------------	-------

<b>SU User</b>	unix02
----------------	--------

<b>SU Password</b>	*****
--------------------	-------

<b>Use sudo</b>	<input checked="" type="checkbox"/>
-----------------	-------------------------------------

- When **Use sudo** is enabled (checked), PAM will authenticate sudo su with the *User* password.

```
Last login: Tue Dec 17 10:44:02 2019 from 10.0.0.20
unix01@demo-server-xtlin01:~$
unix01@demo-server-xtlin01:~$ exec sudo su - unix02
[sudo] password for unix01:
unix02@demo-server-xtlin01:~$
```

- When **Use sudo** is disabled (unchecked), PAM will authenticate su with the *SU User* password.

```
Last login: Tue Dec 17 10:38:20 2019 from 10.0.0.20
unix01@demo-server-xtlin01:~$
unix01@demo-server-xtlin01:~$ exec su - unix02
Password:
unix02@demo-server-xtlin01:~$
```

## Sudo Session Persistence Control

PAM includes the *option to control* whether the sudo session in an SSH execution should persist or expire naturally after a timeout. This allows to decide if a password prompt is required each time a privileged command is executed, or if the session should remain authenticated during the entire SSH session.

- With this option enabled, the system will execute a temporary `sudo -v` to validate the session and maintain privilege elevation via a background command.
- When disabled, it defaults to standard Linux behavior where the password must be re-entered after the `sudo` timeout.

This feature is controlled by a custom record-level checkbox field added to the Unix with SU record type or its inherited derivatives.

- **Field Type:** Checkbox
- **Name:** `requirePasswordPrompt`
- **Display Name:** Require Password Prompt
- **Order:** 700

Record Type: Unix Host with SU Extending [Unix Host](#)

---

**Edit Field: `requirePasswordPrompt`**

<b>Field Type</b>	<div>Checkbox</div>
<b>Name</b>	<div>requirePasswordPrompt</div>
<b>Display Name</b>	<div>Require Password Prompt</div>
<b>Hidden</b>	<div><input type="checkbox"/></div>
<b>Secured</b>	<div><input type="checkbox"/></div>
<b>Indexed</b>	<div><input type="checkbox"/></div>
<b>Order</b>	<div>700</div>
<b>Default Value</b>	<div>Enabled</div>

Now, within the record that uses the *Record Type* with this custom field, you will have a checkbox option named *Require Password Prompt*.

## Unix Host with SU session

<b>Name</b>	Unix Host with SU session
<b>Description</b>	unix host session (external) with user + pass and SU

---

<b>Host</b>	100.0.26
<b>Port</b>	
<b>User</b>	unix01
<b>Password</b>	*****
<b>SU User</b>	unix02
<b>SU Password</b>	*****
<b>Require Password Prompt</b>	<input checked="" type="checkbox"/>

- When **Require Password Prompt** is enabled (checked), PAM will prompt for the sudo password each time the timeout expires, following standard Linux behavior.
- When **Require Password Prompt** is disabled (unchecked), PAM will keep the sudo session active in the background to avoid repeated password prompts and will automatically insert the password from the beginning.

## Cisco Devices

PAM provides Privileged Account and Session Management for your Cisco device including Password Rotation.

This article covers how to create a PAM record to manage your SSH enabled Cisco device, optionally with Enable mode, including secure, password-less connections with recording and automated polices for password reset and rotation.

```
Cisco_R1>enable
Password:
Cisco_R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cisco_R1(config)#
```

Do you also have [Juniper](#) or [Palo Alto Network](#) devices that you need to manage?

## Manage your Cisco device

### Creating an PAM record to Manage your Cisco device:

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Records Types.
3. Locate the Cisco record type in the list and click the **Edit** button to its right.
4. On the Cisco type edit page, locate the *Hidden* parameter and *disable/remove* the checked option. Click the **Save** button.
5. Navigate to Records > All Records.
6. From the **Add Record** dropdown menu, select **Cisco**.
7. Enter a **Name** (*required*) and a **Description** (*optional*)
8. Populate your Cisco device values into the **Host**, **Port**, **User** and **Password** fields.
9. (Optional) If you want to automatically switch to [Cisco's Enable mode](#) when a secure connection is established, enter a value for **Enable Password** and **Enable Level**.

To disable Enable Mode authentication, enter **-1** into the *Enable Level* field.

10. Click **Save and Return** to continue.

Your Cisco device is now under management in PAM. You may use the **Connect** button to test connectivity and if you wish to implement a Password Reset policy, continue to the next section of this article.

## Password for Cisco device

### Creating a policy to reset or rotate the Password for your Cisco device:

1. Open your Cisco record in PAM with a System Administrator or an account that has the [Manage permission for Task Control](#).
2. Within this record, open the **Manage** menu and select the **Tasks** option.
3. By default, both the *Check Status* and *Password Reset* scripts will applied.
4. Next to the *Password Reset* script, click the **Actions** menu and select **Edit Policy**.
5. Choose your required Policy by selecting from the list of available events.
6. Click the **Save** button when finished.

If you are managing several different Cisco devices and wish to apply the same policy for all records, perform the same steps above to the *Cisco Record Type* rather than each individual record.

Your password reset policy is now applied to the PAM record managing your Cisco device. *The password being reset will be the User password, not the Enable password.*



# Juniper Devices

PAM provides Privileged Account and Session Management for your Juniper device including Password Rotation.

This article covers how to create an PAM record to manage your SSH enabled Juniper network device, including secure, password-less remote connections with recording and automated password reset and rotation.

```
--- JUNOS 10.4R1.9 built 2010-12-04 09:20:43 UTC
junos@Juniper1> show version
Hostname: Juniper1
Model: olive
JUNOS Base OS boot [10.4R1.9]
JUNOS Base OS Software Suite [10.4R1.9]
JUNOS Kernel Software Suite [10.4R1.9]
JUNOS Packet Forwarding Engine Support (M/T Common) [10.4R1.9]
JUNOS Packet Forwarding Engine Support (M20/M40) [10.4R1.9]
JUNOS Online Documentation [10.4R1.9]
JUNOS Voice Services Container package [10.4R1.9]
JUNOS Border Gateway Function package [10.4R1.9]
JUNOS Services AACL Container package [10.4R1.9]
JUNOS Services LL-PDF Container package [10.4R1.9]
JUNOS Services PTSP Container package [10.4R1.9]
JUNOS Services Stateful Firewall [10.4R1.9]
JUNOS Services NAT [10.4R1.9]
JUNOS Services Application Level Gateways [10.4R1.9]
JUNOS Services Captive Portal and Content Delivery Container package [10.4R1.9]
JUNOS Services RPM [10.4R1.9]
JUNOS AppId Services [10.4R1.9]
JUNOS IDP Services [10.4R1.9]
JUNOS Runtime Software Suite [10.4R1.9]
JUNOS Routing Software Suite [10.4R1.9]

junos@Juniper1> █
```

Do you also have [Cisco](#) or [Palo Alto Network](#) devices that you need to manage?

## Manage Juniper device

### Creating an PAM record to Manage your Juniper device:

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Records Types.
3. Locate the Juniper record type in the list and click the **Edit** button to its right.
4. On the Juniper type edit page, locate the *Hidden* parameter and disable/remove the checked option. Click the **Save** button.
5. Navigate to Records > All Records.
6. From the *Add Record* dropdown menu, select **Juniper**.
7. Enter a **Name** (*required*) and a **Description** (*optional*).
8. Populate your Juniper network device values into the **Host**, **Port**, **User** and **Password** fields.
9. Click **Save** and **Return** to continue.

Your Juniper network device is now under management in PAM. You may use the **Connect** button to test connectivity and if you wish to implement a Password Reset policy, continue to the next section of this article.

## Password for Juniper network device

### Creating a policy to reset or rotate the Password for your Juniper network device:

1. Open your Juniper record in PAM with a System Administrator or an account that has the [Manage permission for Task Control](#).
2. Within this record, open the *Manage* menu and select the **Tasks** option.
3. By default, both the *Check Status* and *Password Reset* scripts will applied.
4. Next to the *Password Reset* script, click the **Actions** menu and select **Edit Policy**.
5. Choose your required Policy by selecting from the list of available events.
6. Click the **Save** button when finished.

If you are managing several different Juniper devices and wish to apply the same policy for all records, perform the same steps above to the *Juniper Record Type* rather than each individual record.

Your password reset policy is now applied to the PAM record managing your Juniper device.

## Palo Alto Devices

How to use PAM to provide Privileged Account and Session Management for your Palo Alto device including Password Rotation?

This article covers how to create an PAM record to manage your SSH enabled Palo Alto network device, including secure, password-less remote connections with recording and automated password reset and rotation.

Do you also have [Cisco](#) or [Juniper](#) devices that you need to manage?

## Manage Palo Alto device

### Creating an PAM record to Manage your Palo Alto device:

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Records Types.
3. Locate the *Palo Alto Networks* record type in the list and click the **Edit** button to its right.
4. On the *Palo Alto Networks* type edit page, locate the *Hidden* parameter and disable/remove the checked option. Click the **Save** button.
5. Navigate to Records > All Records.
6. From the *Add Record* dropdown menu, select **Palo Alto Networks**.
7. Enter a **Name** (*required*) and a **Description** (*optional*).
8. Populate your Palo Alto Networks device values into the **Host**, **Port**, **User** and **Password** fields.
9. Click **Save and Return** to continue.

Your Palo Alto Networks device is now under management in PAM. You may use the **Connect** button to test connectivity and if you wish to implement a Password Reset policy, continue to the next section of this article.

## Password for Palo Alto Networks device

### Creating a policy to reset or rotate the Password for your Palo Alto Networks device:

1. Open your Palo Alto Networks record in PAM with a System Administrator or an account that has the [Manage permission for Task Control](#).

2. Within this record, open the *Manage* menu and select the **Tasks** option.
3. By default, both the *Check Status* and *Password Reset* scripts will applied.
4. Next to the *Password Reset* script, click the **Actions** menu and select **Edit Policy**.
5. Choose your required Policy by selecting from the list of available events.
6. Click the **Save** button when finished.

If you are managing several different Palo Alto Networks devices and wish to apply the same policy for all records, perform the same steps above to the Palo Alto Networks *Record Type* rather than each individual record.

Your password reset policy is now applied to the PAM record managing your Palo Alto Networks device.

## MacOS Endpoints

Manage Privileged Access, Sessions and Tasks for Apple (Mac) Hosts.

Much like Windows, Unix/Linux, Cisco, Juniper and other systems, PAM can also be used to manage the access, sessions and tasks (like Password Rotation) on Apple endpoints.

This can be configured to support graphical connections using the VNC protocol or terminal based using the SSH protocol.

Regardless of the protocol used, the same features available for other supported record types, including permissions, workflows, command control, recording and auditing, are also supported when the host is an Apple system.

To manage an Apple endpoint, simply use one of the existing **Unix Host** or **VNC Host** record types and enter your connections parameters as needed.

The default port for VNC is 5900 and for SSH it is 22.

Mac SSH

Go to ParentConnect...Execute...

Name

Mac SSH

Description

Host

Port

22

User

chris

Password

\*\*\*\*\*

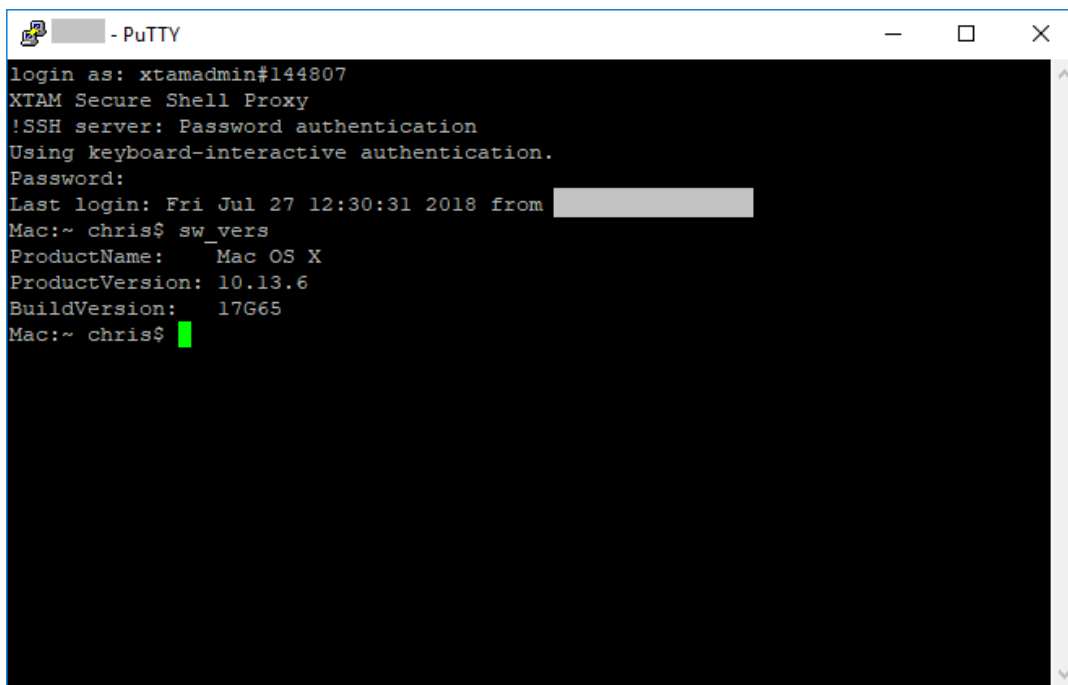
If you want to create your own custom Apple or Mac named record type, please review our [Creating Custom Record Types](#) for additional information.

XTAM | Mac SSH - chris@

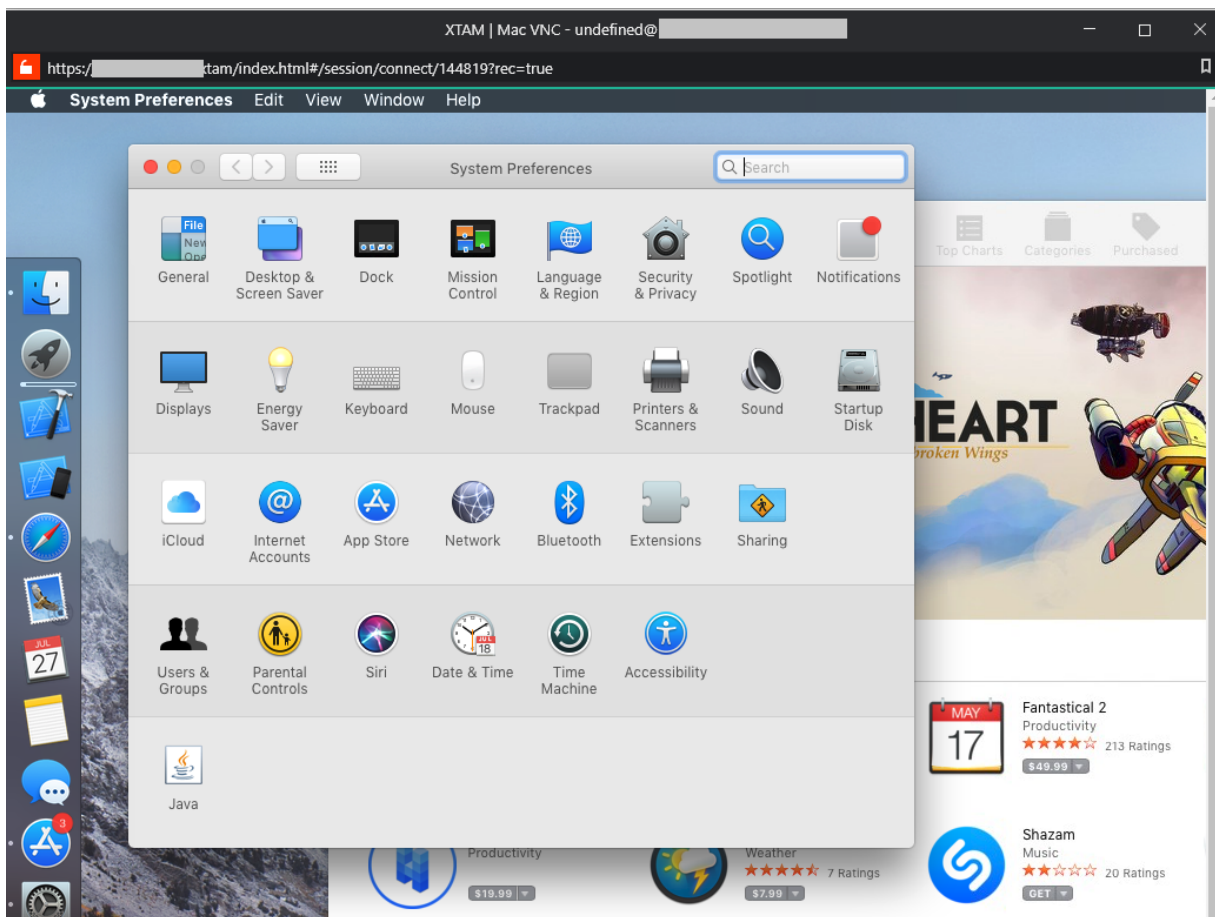
https://xtam/index.html#/session/connect/144807?rec=true

Last login: Fri Jul 27 12:16:36 2018  
Mac:~ chris\$ sw\_vers  
ProductName: Mac OS X  
ProductVersion: 10.13.6  
BuildVersion: 17G65  
Mac:~ chris\$

PAM – Secure SSH (browser) Session



PAM – Secure SSH (PuTTY client) Session



PAM – Secure VNC (browser) Session

# Tasks

A task or job is an object that is configured to run a command or script against the managed host that is executed based on a policy.

These tasks can allow for elevated job execution by securely sharing this record (but not the password) with a user that would typically not be permitted to run such a command.

For example, allow a least privileged user the ability to reset a password without providing them direct **Administrative** or **Root access** or the password required for each.

Alternatively, a task can be configured to automatically rotate a password every set time period or based on a user action like **Unlock** or **Check-in**.

Tasks can be unique to record types (i.e. a different task for Windows vs Unix endpoints) or it can be unique to records themselves (i.e. a different task for each Windows endpoint).

To define your tasks on a record type, you will need to have the System Administrator role.

Once logged in with your System Administrator account, navigate to Administration > Record Types and then click the **Edit** button next to the record type you wish to update.

Next, click the **Tasks** button to open its configuration page. Make the required changes to the tasks list and then click the **Save** button to finalize the update.

To define your tasks on a record, you will need to have the Task Control: Manage role for this record. Once logged in, view the record, select the Manage > Tasks option and then the **Make Unique** button on its configuration page to break the Task inheritance from the record type.

Make the required changes to the tasks and then click the **Save** button to finalize the update.

Tasks consist of several components and all can be configured as required.

## Creating Tasks

To Add a new task to either a Record Type or a uniquely tasked [Record](#):

1. Open the Record Type's Task menu (**Task** button) or the Record's Task menu (Manage > Tasks) and click the **Add Task** button.
2. Select the script that will be executed against the record when the task is executed. For example, the script *Password Reset Remote Windows* will reset the password of the User defined in this record using the Host.
3. Check one or more [Policy Event](#) options. The Event options define when the task's Script will be executed. For example, selecting *Every Sunday* means the script will be executed against the record every Sunday (once a week).
4. Click the **Save** button to complete the task creation process.

## Edit or Remove Tasks

To Edit or Remove an existing task on either a [Record Type](#) or a uniquely tasked [Record](#):

1. Open the Record Type's Task menu (**Task** button) or the Record's Task menu (Manage > Tasks).
2. For the task that needs to be edited, select the required option from its Actions menu.

Edit Policy	Use this option to select a different script or to update the selected Events.
Edit Script	Use this option to edit the script.
Remove Task	Use this option to remove the task entirely from this object.

3. Click the **Save** button afterwards to complete your edit.

## Target Record

Target Record parameter defines which record should be used to schedule a job with the selected script for this task.

Possible values are:

- **Record Itself** - the job will be scheduled for the record itself. This is the most typical choice for the majority of situations.

Note that for the password reset jobs if the record references another record then the referenced record password will be updated after successful job execution.

- **Referenced Record** - the job will be scheduled for the referenced record if it exists in this record definition. The scheduling process will select the task in the referenced record by the name of the script. If the task does not exist the job will be scheduled for the record itself. This option could be used to support the case when the task should be triggered following events that occur with the main record. However, the job should be executed using the configuration and environment of the referenced record.
- **Shadow Record** - the job will be scheduled for the shadow record if it exists in the task list. The scheduling process will select the task in the referenced record by the name of the script. If the task does not exist the job will be scheduled for the record itself.

## Policy Events

A Task's [Policy Event](#) determines when the script will be executed. For example, if you want to rotate a password every time a user Checks-in a record or simply every Friday, then that Check-In action or Every Friday time period is the policy event that triggers the password rotation.

The following is a list of available Policy Events that can be configured for Task execution:

After Approval	This event is triggered after the applied record is approved by a user or system administrator.
After creating or updating a record	This event is triggered after the applied record is initially created or after it is updated, either by a user or system interaction.
After Expire	This event is triggered after the approved workflow time expires on this record.
After Check-In	This event is triggered after the approved workflow is checked in on this record.

After Session	This event is triggered after an active session on this record is completed.
Check to defer execution until completion of the last active session	<p>When enabled (checked), the event will only trigger when the last active session is completed.</p> <p>This includes all concurrent sessions on this single record or any other record if it is configured to use a Reference Record.</p> <p>In the case of reference records, the logic will check all records that use this reference and only trigger the policy when the last of all possible sessions has completed.</p>
<i>n</i> minutes after unlock	<p>Enter a numerical value for this event defined in minutes.</p> <p>The event is triggered this many minutes after a record's secured field is unlocked.</p> <p>For example, 60 minutes after the password field is unlocked, it will be queued for rotation.</p>
Every <i>nth</i> day of each month	<p>Enter a numerical value for this event defined by the day of the month.</p> <p>This event is triggered on this day each month.</p> <p>For example, the 20th day of every month the password will be queued for rotation.</p>
Every <i>&lt;selected day&gt;</i>	<p>Select a day of the week.</p> <p>This event is triggered on this selected day every week.</p> <p>For example, every Sunday the password will be queued for rotation.</p>
On Demand	This task will be made available in the record's <b>Execute</b> menu and can be initiated when needed by a user with the required permissions.
Every <i>nth</i> day	<p>Enter a numerical value for this event.</p> <p>This event is triggered every n number of days.</p> <p>For example, every 1 day (i.e. every day), the password will be queued for rotation.</p>
Every <i>x</i> to <i>y</i> days	<p>Enter a numerical value for the start and end day of this event.</p> <p>This event is triggered on a random day between your two defined values.</p> <p>For example, for every 15 to 30 days, the password will be queued for rotation on a random day between the 15th and 30th day of each interval.</p>

## Shadow Account

A [Shadow Account](#) is a secondary account used to connect to the remote computer on behalf of the primary record account to perform the designated tasks.



A common scenario is that a user cannot reset a password however the Admin or root account can, so that will be used instead.

Normally the record account is used to connect to the remote computer to execute scripts.

When a shadow account is specified for the task the script is executed under the shadow account privileges although it still has access to the main record account.

Shadow Account credentials are stored in a separate record, so when configuring your [Shadow Account](#) to be used in a Task list you must select this other record.

## Time Window

The Time Window allows you to confine Task or Job executions to a specific time window.

For example, this option can be used to limit periodic job executions to off-peak hours as to not interfere with the main function of the remote devices (i.e. maintenance windows).

The time window is specified using the popular CRON format, but it also includes a visual builder for CRON expressions if you are unsure of how to write this format yourself.

## Reviewing Job Results

A [Job History report](#) is provided so that the results of all jobs can be reviewed and actioned. This Job History report will include all jobs that are scheduled or have previously executed, including their events, timestamps, results, state, actions and details.

The Job History report can be accessed on an individual record by clicking the **Job History** button so that only jobs that pertain to this record are included. It can also be accessed globally (Reports > Job History) so that all jobs across all records can be reviewed on a single report.

On the Job History report, additional Actions can be executed:

Run	For <i>Scheduled</i> jobs configured to run on the local node only (i.e. not deferred to a remote worker node), click the <b>Run</b> button to send this job to the queue. If the job is configured to run on a remote worker node, the <b>Run</b> button will result in an error message indicating this remote node configuration and the task will not be executed.
Cancel	For <i>Scheduled</i> jobs only, click the <b>Cancel</b> button to cancel the execution of this job by removing it from the queue.
Details	For <i>Completed</i> or <i>Error</i> state reported jobs, click the <b>Details</b> button to see the detailed results of this executed job.

## Fallback Jobs

Fallback execution can be enabled globally which instructs the Job Engine to repeat previously failed jobs. System Administrators define both the frequency and total cycles of the fallback processing for the entire system.

Jobs that are reprocessed due to this fallback mechanism will be shown in the [Job History report](#) with the type **Fallback**.

NOTE: If a user overwrites a job in its fallback reprocessing cycle (**Cancel** or **Run** the job manually), the fallback reprocessing mechanism itself will be canceled for this record.

More information about [Fallback Jobs](#) and configuration options.

## Configuration

Privileged Access Management provides the ability to associate and execute one or more Tasks on records. This can allow for elevated job execution by securely sharing this record (but not the password) with a user that would typically not be permitted to run such a command.

A Task is a combination of a [Script](#) (**what** is executed against the record) and a [Policy](#) (**when** it is executed against the record).

The principal may execute or review task results as well as view the task list. To include the ability to *Add/Remove* tasks and edit *Task Policies*, the user should be assigned both *Record Control: Owner* and *Task Control: Manage* permissions.

## To configure and execute a script associated to a record

1. Open your record and click the Manage > **Tasks** button along the bottom.

Unix Service Command Defined

Go to Parent Connect... Execute...

**Name** Unix Service Command Defined

**Description** Execute a Unix strategy

**Host** demo-server-xtlin014

**Port** 10026

**User** pamadmin

**Password** \*\*\*\*\*

Record Type: Unix Host  
ID: i-2QztqHd2SfR  
ID-CAP: L-15RKZFKYHMOF  
Created By: Service Administrator (pamadmin)  
/Local @ 12/15/2021 10:46  
Last Modified By: Service Administrator (pamadmin)  
/Local @ 12/15/2021 10:46

Job Queue: (click to refresh)  
● 12/15/2021 10:48, After Update, Check Status Remote SSH, schedule

Command Controls  
Formula  
Permissions  
**Tasks**  
Workflows  
Archive

Audit Log Change History Sessions Job History

Manage Edit

2. Once in the Task view, click the **Make Unique** button and then **OK** on the confirmation dialog.

If you do not want to make tasks unique to this record, you can click the name of the Record Type that it inherits located along the top portion of this frame. Then from the Record Type page, you may then click its Task button to add or modify tasks that will then automatically inherit back down to this and all records that use this record type.



3. Click the **Add Task** button.



4. On the Task page, select your Script from the dropdown menu. The scripts that appear in this selection menu are stored in the System Scripts library. If you would like to create a new custom script or modify an existing script, navigate to Administration > Scripts and click the **Create** or **Edit** buttons.
5. Assign a Policy Event for when the Script should be executed.

Note that adding the *On Demand* option will allow a user to execute this Task by simply clicking the **Execute** button on this record. This is the recommended Event for testing scripts before deploying to production records.

[Save](#)
[Cancel](#)
[↺](#)

**Script** Access SMS Code ⌵

**Target Record** Record Itself ⌵ ?

**Event**

<input type="checkbox"/>	After Approval
<input type="checkbox"/>	After creating or updating a record
<input type="checkbox"/>	After Expire
<input type="checkbox"/>	After Check-In
<input type="checkbox"/>	After Session <input type="checkbox"/> Check to defer execution until completion of the last active session
<input type="checkbox"/>	<input style="width: 50px;" type="text"/> minutes after unlock
<input type="checkbox"/>	Every <input style="width: 50px;" type="text"/> th day of each month
<input type="checkbox"/>	Every <span style="border: 1px solid black; padding: 2px;">⌵</span>
<input checked="" type="checkbox"/>	On Demand
<input type="checkbox"/>	Every <input style="width: 50px;" type="text"/> th day
<input type="checkbox"/>	Every <input style="width: 50px;" type="text"/> to <input style="width: 50px;" type="text"/> days

6. Click the **Save** button when you are finished configuring your Task.
7. You may now add an additional Task or you can return to your Record View by clicking on the breadcrumb.

Tasks ?

Root Folder / Unix Service Command Defined / Tasks

8. From the Record view, click the **Execute** button and then select your Script from the dropdown menu.

Go to Parent ⌵
Connect... ⌵
Execute... ⌵

Password Reset Remote SSH

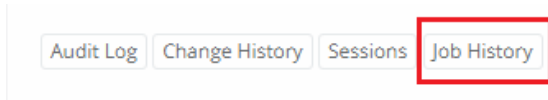
Restart Unix Service

9. This Script will now be added to the *Job Queue*.

Job Queue: [\(click to refresh\)](#)

● 12/15/2021 11:35, On Demand, ready

10. When the Job is processed, it will be removed from the Queue. Depending on your System configuration settings and the current system activity, this may take anywhere from a few seconds or minutes to complete.
11. To view the current status of any Job, click the **Job History** button.



12. The Job History view will display all scripts that have been executed with this record. The most recent will be sorted to the top. If necessary, click the **Refresh** button until the State changes to Completed.

Job History (Unix Service Command Defined)

Found 2 job records.

Columns Bulk Actions

Show 50 entries Search:

CSV PDF TXT XLSX CSV Protected PDF Protected TXT Protected XLSX Protected

Showing 1 to 5 of 5 entries

	Time	Type	Object	Host	Task	Processed	State	
<input type="checkbox"/>	12/15/2021 11:35:07	On Demand	Unix Service Command Defined	demo-server-xtlin014	Check Status Remote SSH	12/15/2021 11:35:27	Ready	Details

First Previous 1 Next Last

13. When the State is either Completed or Error, click the **Details** to view the response that was returned when the strategy was executed.

State	
Completed	Details

Created	12/15/2021 11:35
Scheduled	12/15/2021 11:35
Processed	12/15/2021 11:35
Type	OnDemand
State	Completed
Result	
Response	<pre>1 8-- cron.service - Regular background program processing daemon 2   Loaded: loaded (/lib/systemd/system/cron.service; enabled; vendor preset: enabled) 3   Active: active (running) since Wed 2021-12-15 11:35:07 EDT; 1min 3s ago 4     Docs: man:cron(8) 5   Main PID: 27903 (cron) 6     Tasks: 1 (limit: 9830) 7   Memory: 500.0K 8      CPU: 9ms 9   CGroup: /system.slice/cron.service 10          └─8"8"27903 /usr/sbin/cron -f 11 12 Dec 15 11:35:07 demo-server-xtlin01 systemd[1]: Started Regular background program processing daemon. 13 Dec 15 11:35:07 demo-server-xtlin01 cron[27903]: (CRON) INFO (pidfile fd = 3) 14 Dec 15 11:35:07 demo-server-xtlin01 cron[27903]: (CRON) INFO (Skipping @reboot jobs -- not system startup) 15 Results: 16 Usage: grep [OPTION]... PATTERN [FILE]...</pre>

Cancel

# Task Policy Events

A Task's *Policy Event* determines when the script will be executed.

For example, if you want to rotate a password every time a user Checks In a record or simply every Friday, then that Check In or Every Friday is the policy event that triggers the password rotation (i.e. the script).

The following is a list of available Policy Events:

- **After creating or updating a record** – This event is triggered after the applied record is initially created or after it is updated, either by a user or system interaction.
- **After creating a record** – This event is triggered after the applied record is initially created or imported into the system.
- **After Expire** – This event is triggered after the approved workflow expires on this record.
- **After Session** – This event is triggered after an active session on this record is completed.
  - Check to defer execution to enabled (checked).

In order to select **Check to defer execution until completion of the last active session** checkbox first need select **After Session** checkbox otherwise will be js error on save.

- **After Check-In** – This event is triggered after the approved workflow is checked in on this record.
  - **Check to defer execution until completion of the last active session** – When enabled (checked), the event will only trigger when the last active session is completed. This includes all concurrent sessions on this single record or any other record if it is configured to use a Reference Record. In the case of reference records, the logic will check all records that use this reference and only trigger the policy when the last of all possible sessions has completed.
- **n minutes after unlock** – Enter a numerical value for this event defined in minutes. This event is triggered this many minutes after a record's secured field is unlocked. For example, 60 minutes after the password field is unlocked, it will be queued for rotation.
- **Every nth day of each month** – Enter a numerical value for this event defined by the day of the month. This event is triggered on this day each month. For example, the 20th day of every month the password will be queued for rotation.
- **Every <selected day>** – Select a day of the week. This event is triggered on this selected day every week. For example, every Sunday the password will be queued for rotation.
- **On Demand** – This task will be made available in the record's Task menu and can be initiated when needed by an appropriately permission-ed user.
- **Every nth day** – Enter a numerical value for this event. This event is triggered every n number of days. For example, every 1 day (i.e. everyday), the password will be queued for rotation.
- **Every x to y days** – Enter a numerical value for the start and end day of this event. This event is triggered on a random day between your two defined values. For example, for every 15 to 30 days, the password will be queued for rotation on a random day between the 15th and 30th day of each interval.

## Task Control

Task Control provides access to Tasks associated to Records in the System.

- **None**

The principal may **not** execute, review or manage tasks.

- **Execute**

The principal may execute tasks.

- **Review**

The principal may execute or review task results.

- **Manage**

The principal may execute or review task results as well as view the task list. To include the ability to *Add/Remove* tasks and edit *Task Policies*, the user should be assigned both *Record Control: Owner* and *Task Control: Manage* permissions.

### Grant Access

**Principal ?**

developers

Add

**Selected Principals**

John Williams ▾

**Record Control ?**

Viewer ▾

**Session Control ?**

Connect (Always Recording) ▾

**Task Control ?**

Review ▾

Cancel

Select

Found 2 entries.

[Bulk Actions](#) [Grant Permission](#) [Revoke Permission](#) [Inherit from Parent](#) [Access Report](#) [Refresh](#)

Principal	Type	Record Control	Session Control	Task Control	Actions
<input type="checkbox"/> IT Department /Local	Group	Viewer	None	None	<a href="#">Edit</a>
<input type="checkbox"/> Service Administrator (pamadmin) /Local	User	Owner	Connect (Optionally Recording with Session Events)	Manage	<a href="#">Edit</a>

## Shadow Account

A Shadow Account is a secondary account used to connect to the remote computer on behalf of the primary record account to perform the designated tasks.

Shadow Accounts cannot be used to rotate SSH keys.

A common scenario is that a user cannot reset a password however the Admin or root account can so that will be used instead.

Normally the record account is used to connect to the remote computer to execute scripts.

When a Shadow Account is specified for the task the script is executed under the Shadow Account privileges although it still has access to the main record account.

Cross-vault shadow account usage is not allowed. This means if you have a task running on a record in Vault A, it cannot be configured to use a *Shadow Account record from Vault B*.

The reason for this restriction is to prevent users from creating tasks in the place they can create them (personal vaults or vaults they can create records) to reset passwords that could be executed using powerful domain or root shadow accounts these users otherwise could not use.

You can modify the cross-vault blocker by adding/updating the following line to your `$PAM_HOME/web/conf/catalina.properties` file and then restarting the pam management service:

```
1 | xtam.shadow.crossvault.disable=true #default is true
```

**For example**, you configure a Windows Host record with the user `ituser@company.com` to use in order establish secure remote sessions; however `ituser@company.com` does not have full permissions on the remote host to execute specific commands.

In this situation, when you would use this account to execute your tasks they would ultimately end up failing due to lack of permissions, but this is where Shadow Accounts can help.

You can leave the limited user `ituser@company.com` as the primary record account used for session connectivity and add a second Shadow Account `itadmin@company.com` which does have permissions to execute scripts on the remote host.

This gives you the ability to control the amount of permissions granted during a remote session while not limiting your ability to execute tasks and scripts with the proper permissions.



Shadow Account can be added directly to *Record Types* (i.e. Windows Host) so that they inherit down to all *Records* created from them or they can be added directly to *Records* that have unique Tasks configured.

Shadow Account used to execute the associated Script:

Inherit from Parent

Add Task

Save

Shadow Account

IT Admin use for task execution only \

Time Window

\*\* 10-18 ? 1-12

Script	Policy	Actions
Password Reset Remote SSH	On demand	...

## Additional topics

### Generate, Save and Share Virtual MFA TOTP Tokens

The benefits of enforcing the use of *Multi-factor Authentication* (MFA) tokens or *One-Time Passwords* (OTP) are obvious with personal accounts, but what if you could extend these security benefits to your shared accounts too?

For example, when using a Imprivata Privileged Access Management (PAM) solution, you can securely save and share the login credentials of your various shared administrative accounts.

However, if you were to enforce the use of MFA with this shared account, then it reverts to more of a personal experience where someone would need to be in the possession of the device that generates and displays the token.

Now with PAM, a user can safely store the Virtual TOTP Secret Key in an record, share this record with others and with a click of their mouse, PAM will generate them a valid OTP token.

And because this Secret Key is stored in a secured record, the existing system features including role-based permissions, approval workflows and auditing trails can be used to control, limit or report access.

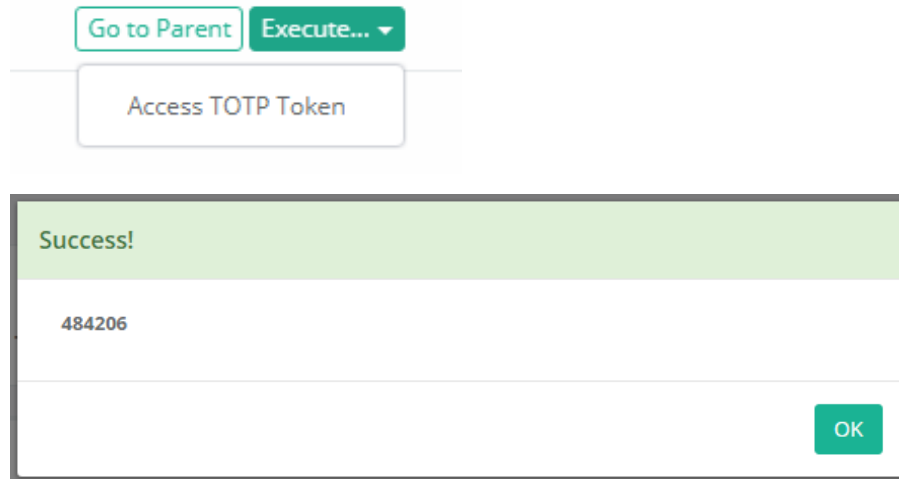
In summary, using PAM you can now enforce the use of MFA when logging into the product and you can provide the ability to generate Virtual TOTP tokens for those shared accounts that are being managed for “just in time” access.

Additionally, it could be a great way to backup your Virtual TOTP secret key(s) in case your device is lost or broken.

#### *To Generate Virtual TOTP MFA Tokens in PAM*

1. Login to PAM with a System Administrator account
2. Navigate to Administration > Record Types, locate the type named **Virtual TOTP MFA** and click its **Edit** button.

3. Uncheck the **Hidden** checkbox and click **Save**.
4. Return to the System Record List, click the **Add Record** button and select this **Virtual TOTP MFA** type.
5. Create your new record as needed:
  - **Name:** enter a record name.
  - **Description:** enter a record description.
  - **Secret Key:** enter the Virtual TOTP Secret Key assigned to the managed account.
6. Click **Save and Return** when complete.
7. After the record is saved, now you can use the Execute > **Access TOTP Token** option to generate your TOTP token. Tokens have a 30 second expiration period so if it does expire prior to use, simply click the Access TOTP Token option again for the new token.



## Heartbeat Checks

When a Windows or Unix record is either created or updated, the PAM [Job Engine](#) will automatically queue a heartbeat or status job to ensure that the provided parameters (host, port, user and password) are accurate. To continue ensuring the record's status, this heartbeat status will be queued again after every *Connection* or *Update* to this record, either performed manually by a user or automatically by a scheduled task like [Password Reset](#).

A record's heartbeat looks like the screenshots below and provides the following information:

- **Last Action:** Indicates the time of the last attempt to validate the record's parameters using the heartbeat's **Check Status** task.
- **Last Success:** Indicates the time of the last successful validation or heartbeat of this record. Green means the most recent attempt was successful, while red means this most recent attempt was unsuccessful.
- **Job Queue:** Displays the Check Status queue state in the PAM Job Engine.

[Job Queue: \(click to refresh\)](#)

● 01/26/2018 10:37, AfterCheckin, Check Status Remote Windows, scheduled

### Heartbeat Queue

Last Action: Execute @ 01/26/2018 10:37  
Last Success: **Execute @ 01/26/2018 10:37**  
Job Queue: [\(click to refresh\)](#)

### Heartbeat Succeeded

Last Action: Execute @ 01/26/2018 10:42  
Last Success: **Execute @ 01/26/2018 10:37**  
Job Queue: [\(click to refresh\)](#)

### Heartbeat Failed

The actual verification heartbeat is a rather simply **echo SUCCESS** task that can be applied to any other supported records using PAM’s [Script Library](#) and [Record Task configuration](#).

Tasks for Windows Host (internal)

Refresh

Inherit from Parent

Add Task

Save

Shadow Account

Search records...

?

Script	Policy	Actions
Check Status Remote Windows	After Check-in,On demand	...

You may also execute an *on-demand* heartbeat check at anytime by simply selecting the **Check Status** task from the **Execute** menu.

Windows Host (internal)

Go to Parent

Connect...

Execute...

Name	Windows Host (internal)
Description	windows host session (internal) with non-domain account

Password Reset Remote Windows

Check Status Remote Windows

### Job Details Error Responses

Below is a list of possible errors reported in the Job Details page.

Click the Job Error Response Message or code below to skip down to its section where further explanation and possible resolutions are located.

If your specific error is not found or the resolutions are still not working as expected, please contact our Support Team <https://support.imprivata.com/communitylogin> for further assistance.

#### Job Error Responses:

- [401](#)
- [Cannot perform this operation at this time](#)
- [The user or administrator has not consented to use the application with ID](#)
- [Verification Error: Exception calling "ChangePassword"](#)
- [Exception calling "SetPassword" ... "Access is denied."](#)
- [Error resetting password: Failure to update AD certificate](#)
- [Error resetting password. Cannot find user domain\user or cannot connect to AD ldaps://yourADServer:3269](#)
- [StrategyDirectory: Error resetting password. PamException: The WS-Management service cannot process the request. The maximum number of concurrent shells for this user has been exceeded.](#)

### *Response error: 401*

The 401 error response is usually associated to an Unauthorized response from the remote host. The following reasons may be the root cause for this error:

1. The User or Password associated to the record (or shadow account) is either incorrect or does not have the permissions to connect to the remote host. To troubleshoot, attempt to establish a Secure Connection using this record to the remote host. If that fails, then Edit the record, modify the User or Password and then try again. For Windows tasks, try using the format **DOMAIN\user** or **user@domain.com** for the User parameter in the record.
2. The user or shadow account used for this Task does not have the Windows permission to execute a remote PowerShell command. To troubleshoot, ensure this user or shadow account is a member of the local Windows group "Remote Management Users" on your remote host and then try again. Some scripts may require additional permissions, so adding this account to the "Administrators" group may also help to resolve the error.
3. Remote Windows tasks are sometimes executed using the [Windows Remote Management protocol](#) and this needs to be enabled on the host. To do so, run the following command on this Windows host: *Winrm quickconfig*. WinRM, by default, uses the ports 5985/5986 so these must be open between the PAM host server and your endpoint.

*To troubleshoot a 401 response error, consider trying the following:*

1. From the PAM host server itself, open a PowerShell session (run as administrator) and execute the following command. Replace the bolded values with those from your PAM record.

```
Invoke-Command -ComputerName remote-host -Credential domain\user -ScriptBlock {dir \}
```

If the above command executes successfully, meaning PowerShell does not return any error messages, then it will display a list of directories in the root drive of the remote host.

If the above command does not execute successfully, then that may indicate an issue with the network's Windows Remote Management (WinRM) configuration. Try to understand and troubleshoot the error message that PowerShell returns. If you are stuck, consider trying the following:

2. From the PAM host server itself, open a [PowerShell](#) session (run as administrator) and execute the following command. Replace the bolded values with those from your PAM record.

```
1 | Set-Item -Path WSMan:\localhost\Client\TrustedHosts -Value 'remote-host'
```

This command will add your remote-host computer to the trusted hosts list in the server's WinRM configuration. After this command is executed successfully, try executing your record's [Task](#) in PAM again.

### *Response error: Cannot perform this operation at this time*

When attempting to reset the password on an AS400 host, this message may appear if the Password policy does not allow for the password to be updated at this time.

To troubleshoot, either wait until the policy on the AS400 host allows for the password to be updated or modify the policy to allow more frequent updates and then try again.

### *Response error: The user or administrator has not consented to use the application with ID*

When attempting to reset the password on an Azure or Office 365 Administrative account, the operation fails because permissions have not been fully granted to the Application.

To troubleshoot, login to your Azure Portal (as an Administrator), open our PAM App you created earlier, click All Settings > Required Permissions > Grant Permissions and then **Yes** to confirm. Once complete, try the password reset again.

### *Response error: Verification Error: Exception calling "ChangePassword"*

This can commonly be the error response when attempting to a change password in a Windows domain where the new password does not meet the requirements of your Local or Domain Security policy.

For example, this could be the password age (resetting too frequently) or complexity (formula not strict enough).

To troubleshoot, log in to this Remote host and attempt to manually change the password.

If it fails to update manually, check the [Password Policy](#) on this Local computer or the [Domain Controller](#) to ensure the new password meets its minimum requirements.

Of particular importance, if your Password Policy has the policy **Password must meet complexity requirements** set to Enabled, then you must configure your [PAM formula](#) to comply with this policy. This means that your formula must meet at least 3 out of the following 4 requirements:

- Minimum Number of Upper Case Characters: 1 or greater
- Minimum Number of Lower Case Characters: 1 or greater
- Minimum Number of Numeric Characters: 1 or greater
- Minimum Number of Special Characters: 1 or greater

You also want to be aware that most password policies do not allow a password to be changed often (minimum password age), this may mean that you are only allowed to change the password once a day or less often.

While this is an important policy for production account security, it can prove to be problematic during testing where you may need to or want to change an account's password with more frequency.

### *Exception calling "SetPassword" ... "Access is denied."*

This can commonly be the error response when attempting to set a password (script: Password Set Remote Windows with Service Dependencies) using a non-domain, local account as the PAM [Shadow Account](#).

Due to native Windows permissions, the local account used as the Shadow Account needs additional privileges beyond the usual WinRM requirements. To progress beyond this error, you can use the following options:

- Rather than a local account, use a domain account that has sufficient privileges to Set another user's password. This usually means being in the local Administrators group on this target server.
- Modify the registry of your target server to support this function. Please read the "Let me fix it myself" section of this Microsoft support document for more information. <https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows>

### *Task: Password Reset LDAP, State: error, Message: StrategyDirectory: Error resetting password. PamException: Failure to update AD certificate*

This can commonly be the error response when attempting to a reset an Active Directory password when PAM was integrated with AD not using LDAPS.

If you are using the Password Reset LDAP script, as shown in the above error message, then in order to reset an AD domain password through a native LDAP connection in PAM, your AD integration must be configured using LDAPS.

Microsoft requires any such AD passwords to be updated only through a secure port using your AD's SSL certificate.

With this in mind, the first thing to check is that your PAM AD integration (Administration > Settings > AD) should be using LDAPS and a secure port which is usually either 636 or 3269.

For example, in your Server parameter your connection should begin with `ldaps://` and end with the required port 636 or 3269.

If you are not configured with LDAPS, then you will need to change it as required and once the integration is successful, you will need to then restart the PAM service (**PamManagement** or **pammanager**).

During this restart, PAM will attempt to import your AD's SSL certificate so that the connection is secured over the defined port which then allows for the password change.

As an alternative approach, you can try using the *Windows Host* record type to rotate your password. When created, this record type will connect to the Host machine defined in the record and attempt to reset the AD account's password through this host itself.

This method does not use a direct LDAP connection, so LDAPS is not required in this case.

*Task: Password Reset LDAP, State: error, Message: StrategyDirectory: Error resetting password. PamException: Cannot find user domain\user or cannot connect to AD ldaps://yourADServer:3269.*

This can commonly be the error response for a few possible reasons.

- The most obvious reason is that either the displayed user account was not found in this AD or the connection to this AD failed. Confirm that the user does exist with this exact account name, take note that if you are logging into PAM using UPN accounts, then the User in this record should be in the same format (user@domain.com). Also ensure that PAM can still connect to your [Active Directory](#) using the displayed server and port.
- If your AD integration limits the scope of user logins based on OU configuration or AD Group membership, then the account in this record should be included in this OU or the defined AD Group. Make the necessary adjustments and retry your password reset task.
  - However, if you do not want to modify your AD integration parameters, consider using additional options in PAM to manage Active Directory accounts not relying on your integration. For more information, please read this [article](#).

*(Partial) Message: StrategyDirectory: Error resetting password. PamException: The WS-Management service cannot process the request. The maximum number of concurrent shells for this user has been exceeded.*

Microsoft Server limits the maximum number of concurrent users connected to the WinRM session to five and the maximum number of shells per user to five also. This could present issues when multiple connections, using WinRM, are connected to the host.

If you wish to resolve this issue by increasing the maximum number of allowed user or shells per user, you can use this procedure on the host:

1. On the host, open command prompt using the Run as Administrator option.
2. Execute the following command to retrieve the host's current configuration:

```
1 | winrm get winrm/config/winrs
```

3. To increase limits, the following commands may be used if needed (note these changes are permanent unless changed later):

```
1 | winrm set winrm/config/winrs @{MaxConcurrentUsers="20"}
```

```
1 | winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
```

```
1 | winrm set winrm/config/winrs @{MaxMemoryPerShellMB="512"}
```

For additional information about these limits, please review: <https://docs.microsoft.com/en-us/windows/win32/winrm/quotas>

## Reconciliation Account

A reconciliation account can be used to reset the password of the User account if it becomes out of sync with the host.

A reconciliation account differs from the use of a [Shadow Account](#) in that it could be a unique account for each host.

The reconciliation account will be used automatically to reset the User account password on this host when a *Check Status* job fails.

A *Check Status* failure indicates that the User account in the record is no longer valid possibly due to a password change that occurred outside of PAM or during a remote session.

Reconciliation account passwords can also be periodically reset using the *Password Reset Reconcile* script with the desired policy event.

To create a record with a reconciliation account, select the record type **Unix Host with Reconcile Account**.

Please note that this record type is *hidden* by default, so you may need to unhide it before it becomes available.

In the record, you will see two additional fields; *Reconcile Account User* and *Reconcile Account Password*.

In these fields, enter your reconciliation user and password. Both fields are hidden, so you will only see them when you create or edit the record.

Type	Unix Host with Reconcile Account	▼
Host	168.192.1.88	
Port	22	
User	useraccount	
Password	●●●●●●●●●●	👁️ 🔍
Password is Very Strong.		
Reconcile Account User	reconaccount	
Reconcile Account Password	●●●●●●●●●●	👁️
Password is Very Strong.		



This reconciliation account will be automatically used when the Check Status job fails on this record.

No additional configuration is required, but you may configure the *Check Status* task by navigating to Manage > Tasks and updating it as needed.

Time	Type	Task	Processed	State	
12/30/2020 08:44:20	Fallback	Password Reset Remote SSH		Scheduled	<button>Cancel</button> <button>Run</button>
12/30/2020 08:44:02	On Demand	Check Status Remote SSH	12/30/2020 08:44:20	Error	<button>Details</button>

Additionally, if you wish to reset the Reconcile Account Password, you can configure the *Password Reset Reconcile SSH* task policy on this record as needed.

For *Switch User* records, you can extend this same functionality by creating two new fields in the record type; *ReconcileUserSU* and *ReconcilePasswordSU* and entering the reconcile credentials in each field that will be used to reset the password of the SU User account if its Check Status job fails.

The screenshot shows a configuration interface for a record. At the top right, there are buttons: 'Inherit from Parent', 'Add Task', 'Save', and a refresh icon. Below these, there is a 'Shadow Account' section with a search bar labeled 'Search records...'. Underneath is a 'Time Window' section with a dropdown menu and two small icons. The main part of the interface is a table with three columns: 'Script', 'Policy', and 'Actions'. The table contains three rows: 1. 'Check Status Remote SSH' with policy 'After Session:-1, On demand' and an 'Actions' button. 2. 'Password Reset Reconcile SSH' with policy 'On demand' and an 'Actions' button. 3. 'Password Reset Remote SSH' with policy 'On demand' and an 'Actions' button. A context menu is open over the third row, showing options: 'Edit Policy', 'Edit Script', and 'Remove Task'.

If you want to add this Reconciliation Account function to an existing record, you can create the fields *Reconcile Account User* and *Reconcile Account Password* manually in your record type.

After, you can add the *Password Reset Reconcile* task to the record as well to support the option to reset the Reconciliation Account Password.

## Rerun Failed Jobs (Fallback)

Automatically Rerun Failed Jobs or Tasks.

PAM can be configured to automatically rerun periodic jobs or tasks that have resulted in a failure.

This option improves the chances to reach computers that often appear outside of the corporate network, offline or shutdown frequently to reset password, check password status, manage local administrators group or maintain valid service credentials.

The configuration for this option is driven by two system parameters both of which allow time interval specifications in seconds, minutes, hours or days: *Rerun Failed Job Window* defines for how long the job should be repeated and *Rerun Failed Job Interval* defines how frequently the fall back job should be scheduled.

## To configure these rerun options

1. Login to PAM with a System Administrator account
2. Navigate to Administration > Settings > Parameters
3. Locate or search for the parameters **Rerun Failed Job Interval** and **Rerun Failed Job Window**
  - **Rerun Failed Job Interval:** The system will reschedule failed periodic, monthly or weekly jobs several times with the specified interval during the specified time window or until the job will succeed.

Note that non-zero time interval should be smaller than the rerun failed job time window.

- **Rerun Failed Job Window:** The system will reschedule failed periodic, monthly or weekly jobs several times during the specified time window or until the job will succeed.
4. For each parameter, enter the desired value in a space or colon separated list of tokens, each token is a number plus time unit, defined in seconds (s), minutes (m), hours (h) or days (d). For example:
    - **1d 12h** — means 1 day and 12 hours
    - **45m** — means 45 minutes
    - **0d** or **0h** or **0m** or **0** — means zero
  5. Click the **Save** button next to each value when finished.

### Jobs

Rerun Failed Job Interval	<input type="text" value="6h"/>		Save
Rerun Failed Job Window	<input type="text" value="2d"/>		Save

Attempted periodic job reruns will appear in the Job History report as the Type *Fallback*, as shown in the screenshot below.

### Job History

Found 2 job records.

Time: Last Day ▼ State: Any ▼ Columns

Show  entries Search:  CSV PDF TXT XLSX CSV Protected PDF Protected TXT Protected XLSX Protected

Showing 1 to 2 of 2 entries

Time	Type	User	Host	Task	Processed	Result	State	
06/14/2021 07:04:36	Fallback	Service Service (pamservice) /Local		Check Status LDAP	06/14/2021 07:04:48		Error	<a href="#">Details</a>
06/14/2021 07:04:36	Fallback	Service Service (pamservice) /Local		Check Status LDAP	06/14/2021 07:04:48		Error	<a href="#">Details</a>

First Previous 1 Next Last

## SSH Key Management

SSH Key Management and Automated Rotation.

With increasing popularity of Unix and Linux systems in the enterprise space, it is becoming a growing concern to Security personnel as they are not typically accessed like a Windows-based server.

In many instances, Unix and Linux endpoints are secured not with a traditional username and password, but rather they are accessed via SSH using a *private/public* keypair. And much to the disapproval of Security professionals, these keys can sometimes be made to work across multiple servers and are rarely, if ever, updated. This means if a threat gains access to one of your SSH keys, they can potentially access areas of your enterprise infrastructure without warning or consent.

With Imprivata Privileged Access Management software, one can easily and safely store any number of SSH keys with the additional benefit of secure sharing with others, auditing usage of the keys and providing remote access to these Unix endpoints without giving user’s the key itself.

Even if the key itself is never shared with another human again, PAM also provides the ability to automatically rotate the SSH key based on configured policies (scheduled or on-demand), ensuring no one can ever again gain access without your knowledge or approval.

To begin implementing SSH Key Management in your PAM deployment today, simply create a record using either the **Unix Host with Key** or **Unix Host with Protected Key** [record types](#) (or create your own [custom record type](#) using the [File field](#)) and save your key into PAM’s secured Identity Vault.

Next, configure your **Public Key Update Remote SSH** rotation policy and finally share access to it with your authorized users.

Tasks for AWS Production

Inherit from ParentAdd TaskSave↺

Shadow Account

Search records...

?

Script	Policy	Actions
Check Status Remote SSH	On demand,After Update	...
Public Key Update Remote SSH	On demand,After Check-in,Every (n)th day of a week	...

For your SSH keys, PAM will:

- Safely store your SSH key(s) in a centralized location.
- Prevent unauthorized access to both them and the corresponding endpoint.
- Automatically rotate the key(s) based on a schedule or on-demand.
- Provide an easy means to share access to the key with employees and outside contractors, but not the key itself.
- Audit, report and alert all interactions and activities associated with the key.
- Generate Request and Approval Workflows so Senior level or Managers can grant access to these keys.
- Establish a recorded remote [SSH session](#) (client or browser) to this protected endpoint.

# Dual Account Control

Dual Account Control allows for PAM to manage more than one account that can be used with a single API call to return valid privileged credentials.

With single account management there can be times, no matter how short, where the credentials would be invalid during events like password rotations.

By implementing Dual Account Control, PAM can return another set of credentials while the first are in the process of being rotated so there is no point in time when the API would return credentials that may be invalid at that moment.

Dual Account Control should only be used for highly available business continuity systems that require valid credentials to be always returned by the API call. For the majority scenarios, using the standard single account record with password rotation is still recommended.

## Enable Dual Account Control

Dual Account Control is disabled by default, please follow the steps below to enable this feature.

1. Log in to PAM using a System Administrator account.
2. Navigate to Administration > Settings > Parameters > Dual Account Support, switch this parameter to *Enabled* and click **Save**.

## Creating Dual Account Control Records

The following will describe how to create and link dual account records.

1. Navigate to the container where the records will be stored and use the **Add New Record** button to create your first record. This will become the primary record of your dual account configuration. You may use the record type that best conforms to your requirements like Active Directory User, Windows Host, Linux Host, etc.

With your first record, enter the values as needed. For the username and password fields, be sure the credentials entered are valid. When complete, **Save** this new record.

Name	Domain Admin 1
Description	
<hr/>	
User	<input type="text" value="contoso\dadmin1"/>
Password	<input type="password" value="*****"/>

2.

Create your second record using the same method above, including a second set of valid credentials. This will become a secondary record in your dual account configuration.

**Name** Domain Admin 2

**Description**

---

**User** contoso\dadmin2

**Password** \*\*\*\*\*

3.

Return to your first record (primary record) and use the **Edit** button. On the Edit Record page, find the *Reference Record* parameter, change it from Reference to *Dual Account* and enter your second record in the field provided. A valid record is needed for this field and as you type the name, it should appear in the dropdown below that you can use for selection. When complete, **Save** this updated record.

**Name** Domain Admin 1

**Description**

**Reference Record** Dual Account ▾ Domain Admin 2 (Paths: /Dual Account)

4.

Both records are now created, and the primary record is linked to the secondary record, so the next step will be to set up a suitable password reset policy for each.

If you want to support more than two records, you can create more records and link them to the primary using the same steps above. Be sure the primary record is updated to link each Dual Account record you wish to include in the configuration.

## Configuring Dual Password Rest Policies

To support this feature, each record must have the same password reset script in its task list (i.e., Password Reset LDAP, Remote Windows Password Reset, etc.) and each record's task must be scheduled for non-overlapping times (i.e., record 1 every Monday and record 2 every Thursday).

If both records are scheduled for password reset during the same period, then no valid records will be returned by the API until one of the tasks has been completed. This result should be avoided to minimize potential problems.

1. In record 1, open Manage > Tasks, click **Make Unique** and select the **Edit Task** action for the Password Reset script listed.

On the Edit Task page, scroll down to the Every event and select **Sunday** from the dropdown menu. Click **Save** to update this task.

☐ Every th day of each month

☒ Every

2.

☐ On Demand

3. In record 2, open Manage > Tasks, click **Make Unique** and select the **Edit Task** action for the Password Reset script listed.

On the Edit Task page, scroll down to the *Every event* and select **Thursday** from the dropdown menu. Click **Save** to update this task.

A screenshot of a web interface showing a dropdown menu. The dropdown is open, displaying 'Friday' as the selected option. To the left of the dropdown is a green checkmark icon. The text 'Every' is visible to the left of the dropdown box.

4. 

## Using the API to Retrieve Valid Credentials

Now that both records have been configured, you can use the API to retrieve a currently valid set of credentials between those that have been linked.

When calling the API, it will return the credentials from the record that is not presently scheduled for a password reset. Since both records in our example have been assigned non-overlapping task policies, the record's credentials returned at any given time will be valid (i.e., not in the process of being reset).

The credentials used to authenticate to PAM to make the API call require that the permission on each linked record is Record Control: Unlock or higher for this account. If permissions on the linked records are insufficient, then the API call will return an error.

1. Use the **API /xtam/rest/dual/unlock/[recordID]** to perform the call where [recordID] is the ID of the primary record, record 1.
2. The response returned of a successful call to the primary record will be one of the following results:
  - The record metadata and credentials from record 1 (primary record) because record 2 is in process of a password reset or no linked accounts are in the process of a password reset.
  - The record metadata and credentials from record 2 (secondary record) because record 1 is in process of a password reset.
  - An error response with the message "No active dual accounts found" indicating that all linked accounts (primary and secondary) are currently in process of a password reset operation.


## Reports

Dual Account Control has its own unique report named *Dual Account Log Report* available in the Report Center when enabled. This report will include only those Unlock actions that are performed using the Dual Account API to retrieve credentials. By isolating these Dual Account Unlock events to their own report, it allows for easier review and auditing of this feature.

Unlock events in the Dual Account Log Report are automatically grouped by time ranges and include a unique *Count* column to show the total number of Unlock events that occurred within that given range.

The Dual Account Audit Log report provides a list of all audit events captured throughout the operation of the dual account API.

Found 11 audit log records.

Time: Last Week Category: Any Level: Any Columns   

Show 50 entries

Search:  CSV PDF XLSX PDF Protected CSV Protected XLSX Protected

Showing 1 to 11 of 11 entries

Time	User	IP	Object	Category	Level	Event	Count	Message
05/24/2024 13:46:56 - 05/24/2024 13:46:56	Service Administrator (pamadmin) /Local	0:0:0:0:0:0:1	Domain Admin 2	Data	INFO	Unlock	1	
05/24/2024 13:46:41 - 05/24/2024 13:46:41	Service Administrator (pamadmin) /Local	0:0:0:0:0:0:1	Domain Admin 1	Data	INFO	Unlock	1	
05/24/2024 13:16:49 - 05/24/2024 13:17:07	Service Administrator (pamadmin) /Local	0:0:0:0:0:0:1	Domain Admin 1	Data	INFO	Unlock	2	
05/24/2024 13:15:40 - 05/24/2024 13:15:52	Service Administrator (pamadmin) /Local	0:0:0:0:0:0:1	Domain Admin 1	Data	INFO	Unlock	2	

## Alternate Dual Account Control Configuration

Another configuration possibility is to add a standalone primary record for which the API request will be submitted for three (or more) records; one primary and two or more secondary. There is no added functionality available in this configuration, but it does allow for a primary record without credentials to be used for API requests.

To configure a three-record setup with two linked dual accounts:

1. Create a primary record with any required values in each field. This primary record should not include any credentials. No task policies are needed on this primary record.
2. Create each of your secondary records (two or more are supported), each with valid credentials. Configure the password reset task policies as described in the earlier section.
3. Return to your primary record and in the Reference Record parameter, select the Dual Account option and reference all your secondary records. Use the + button to add multiple Dual Account references.
4. When calling the API, use the record ID of this standalone primary record. When a successful API call is made to this primary record, the following response will be returned:
  - The record metadata and credentials from any secondary record that is not currently in the process of a password reset. The credentials returned may come from secondary record 1, 2, 3, etc.
  - An error response with the message “No active dual accounts found” indicating that all linked secondary records are currently in process of a password reset operation.

## Verification API

To verify that the record being called is configured as part of a Dual Account, you can call the following API:

1. Use the **API /xtam/rest/dual/related/[recordID]** to perform the call where [recordID] is the ID of the primary or a secondary record.
2. The response returned of a successful call to the record will be one of the following results:
  - **True** will be returned if the record is part of a Dual Account configuration. This record may be the primary or secondary record.
  - **False** will be returned if the record is not part of a Dual Account configuration.

## Performance Optimization

If the API is being called often, every second or many times a second, you can adjust the *Record Cache TTL* to better support the application load caused by this high frequency of unlock actions.

The application caches record information to optimize retrieval of frequently accessed records. The smaller this value, the more frequently the application will query the record data from the database. The larger the value, the memory usage will increase. Set this value to 0 (zero) to disable this cache.

To adjust the Record Cache TTL parameter:

1. Log in to PAM using a System Administrator account.
2. Navigate to Administration > Settings > Parameters and find the parameter labeled **Record Cache TTL**.
3. Adjust this value (increase the value measured in minutes to increase the cache time) as needed and click **Save** when done.

## Host Queries for Mass Script Execution

Host Queries to Configure and Execute Tasks across many Endpoints.

Say you are looking to executing a task like [Local Admin Group Cleanup](#) or [Windows Service Password Reset](#) across a series of computers.

What is the best way to configure this scenario in PAM?

One method would be to create a record for each endpoint with its specific host, port, username and password, then apply the task to this record and setup your automated policy.

A couple of steps are required, but certainly not terribly difficult to implement unless you have thousands or hundreds of thousands of assets to manage.

With that many endpoints, now you are looking into [Import](#) options. I could create a CSV file that lists all the endpoints or import them from my current session management solution like Remote Desktop Manager or mRemote.

This would decrease the amount of implementation time needed to populate PAM and get you up and running more easily, but now you have hundreds or thousands of records in PAM that are not needed outside of task execution policies.

What if there was an easier way?

What if you could execute your task like *Local Admin Group Cleanup* script against all your endpoints using a single [PAM record](#)?

You create a single record, you share a single record, you review and monitor a single record, but in reality that single record is executing your task against hundreds or thousands of your managed endpoints.

If this sounds promising, then let's talk about PAM's Host Query records.

A traditional endpoint record in PAM defines a specific host that is used to connect to the asset. In our host query record, you define all your hosts to be inputting a query to find your host rather than a host name, for instance an Active Directory query to locate your web servers.

PAM will execute your query and for every endpoint that is returned, it will queue, execute and report your configured task(s).



Managing tasks for many like endpoints just got a lot easier.

## Using PAM Host Query Records


1. Login to PAM and create a new record using the type **AD Query**. If you do not see this type in the drop-down, navigate to Administration > Record Types, locate this AD Query type, click **Edit**, uncheck the Hidden option and finally click **Save**.
2. Enter a **Name** (*required*) and **Description** (*optional*) for your new record.
3. For the **User** and **Password** field, enter credentials that are will be valid for all your potential endpoints. Consider using a Domain Administrator account to avoid connection issues.
4. Finally, in the **AD Query** field, enter an Active Directory query that will return a list of computer hosts that you want to execute tasks against.

Here is an AD Query example to return every computer in Active Directory that contains DEV: (&(objectclass=computer)(objectcategory=computer)(cn=DEV\*))

### Local Admin Group Cleanup AD Query

Name	Local Admin Group Cleanup AD Query		
Description	AD Query host to execute cleanup task against all development computers.		
Reference Record	Search reference record...		

---

Type	AD Query		
User	domainAdmin@company.com		
Password	.....		
AD Query	(&(objectclass=computer)(objectcategory=computer)(cn=DEV*))		

---

SaveSave and ReturnCancel

5. Click the **Save and Return** button when finished.
6. With the record saved, you can now [apply your task\(s\)](#).
7. Click the **Execute** dropdown and then select your task from the list to execute. If you want to test the query first, select the preconfigured task *Query Sample Data*. This task will display a list of hosts returned from the query without executing any scripts against them. If you do not want to test the query, proceed to the next step.

## Sample Data

Name	Host
CN=DEV-EXTQA01,CN=Computers	dev-extqa01.xt.com
CN=DEV-MARIADB,CN=Computers	dev-mariadb.xt.com
CN=DEV-MYSQL5,CN=Computers	dev-mysql5.xt.com
CN=DEV-ORACLE12,CN=Computers	dev-oracle12.xt.com
CN=DEV-POSTGRES9,CN=Computers	dev-postgresql9.xt.com
CN=DEV-SERVER-ALT,CN=Computers	dev-server-alt.xt.com
CN=DEV-SERVER-MARK,CN=Computers	dev-server-mark.xt.com
CN=DEV-SQL16,CN=Computers	dev-sql16.xt.com
CN=DEV-WIN10ENT,CN=Computers	dev-win10ent.xt.com
CN=DEV-WIN2003R2E,CN=Computers	dev-win2003r2e.xt.com

8. When executing your task like Windows Local Administrator Group Cleanup, select it from the dropdown list and then you will be presented with a new dialog. In this new dialog, enter a value into the **Query Sample Data Size** field. This is how you determine how many endpoints to execute against. If you only want to test a subset, then enter a value like 5 which will mean only the first five returned query results will be used or enter the value -1 or *All* to execute the task against all query results.

Note: When tasks are executed automatically, the AD Query will return and ultimately process all of the results. This *Query Sample Data Size* parameter is only available for On-Demand policy execution.

### Script Parameters

#### Query Sample Data Size

9. Once the task is executed, it will first generate a list of all endpoints and add them as queued jobs. You will see all these jobs listed in [Job History](#) with a status of Ready.

Time	Type	User	Object	Host	Task	Result	State	
02/23/2018 15:42:12	OnDemand	Chris Kolodziejwski (chrisk)	<a href="#">Local Admin Group Cleanup AD Query</a>	DEV-WIN2008R2E.xt.com	Windows Local Admin Group Membership		Ready	<button>Cancel</button>
02/23/2018 15:42:12	OnDemand	Chris Kolodziejwski (chrisk)	<a href="#">Local Admin Group Cleanup AD Query</a>	dev-mariadb.xt.com	Windows Local Admin Group Membership		Ready	<button>Cancel</button>
02/23/2018 15:42:12	OnDemand	Chris Kolodziejwski (chrisk)	<a href="#">Local Admin Group Cleanup AD Query</a>	dev-win2003r2e.xt.com	Windows Local Admin Group Membership		Ready	<button>Cancel</button>
02/23/2018 15:42:12	OnDemand	Chris Kolodziejwski (chrisk)	<a href="#">Local Admin Group Cleanup AD Query</a>	dev-win10ent.xt.com	Windows Local Admin Group Membership		Ready	<button>Cancel</button>
02/23/2018 15:42:12	OnDemand	Chris Kolodziejwski (chrisk)	<a href="#">Local Admin Group Cleanup AD Query</a>	dev-extqa01.xt.com	Windows Local Admin Group Membership		Ready	<button>Cancel</button>
02/23/2018 15:42:12	OnDemand	Chris Kolodziejwski (chrisk)	<a href="#">Local Admin Group Cleanup AD Query</a>	dev-sql16.xt.com	Windows Local Admin Group Membership		Ready	<button>Cancel</button>
02/23/2018 15:42:12	OnDemand	Chris Kolodziejwski (chrisk)	<a href="#">Local Admin Group Cleanup AD Query</a>	dev-postgresql9.xt.com	Windows Local Admin Group Membership		Ready	<button>Cancel</button>

10. As the jobs execute, their status will update and you can review their results in the [Job History](#) or [Job Summary reports](#).

Over time, as your query returns new host results, the record will dynamically load each of these new hosts which will ensure this host query record adapts to your changing environment.

## Windows Local Admin Group Cleanup

Any users who are members of a Windows local Administrators group have elevated permissions on this computer, including the ability to install programs, change IP addresses and potentially cause havoc within your business, and because of this it is crucial for Network, Domain and Security Administrators to be able to easily monitor and manage this group's membership across all Windows endpoints. In a nutshell, users should not have unnecessary administrative privileges; this is bad practice.

If you simply want to report on local Administrators group membership (or any group for that matter), this can be accomplished quite simply with an PAM task.

And if you want to go one step further and cleanup the group's membership (remove all users except those specified), that too can be easily accomplished.

In this article, we are going to detail the process for cleaning up the Administrator group's membership.

Before we begin, it's important to understand the ramifications to this action. Cleaning up Windows local Administrators group membership is good and highly recommended, it may come as a surprise to those users who are "cleaned".

Things and tasks that they could do yesterday may no longer be possible, so if necessary run reports first so you can alert your "cleaned" users ahead of time to minimize their potential objections.

**When you are ready to begin, perform this procedure in PAM.**

We recommend running this on a few Windows test hosts before you run it against all your managed Windows endpoints.

1. Create a new or use an existing **Windows Host** record.
2. Open the record's Task menu by selecting Manage > Tasks.
3. Add the Task *Windows Local Administrators Group Cleanup* to this record by using one of these two procedures:
  - a. Add the Task directly to the record's Record Type and allow inheritance to apply it to this record.
  - b. Make this record's Task unique by clicking the **Make Unique** button and adding the task directly to this record.
4. Once the task is applied, configure the task's Policy to include the On Demand execution. In this example, we are going to manually execute the reset, however you can configure any additional policies including automated reset as you need.
5. If the user already associated to this record is not also a member of the host's local Administrator's group, then you will need to add a [Shadow Account](#) to the task that contains a user account that is a member.

Our default task removes everyone except the local "Administrator" account and the "Domain Admins" group account. If the record's user is not one of these two accounts, then it too will be removed when executing this task and will subsequently fail during the next execution due to a lack of permissions.

If you want to modify the task to exclude additional accounts from removal or specify a different group to maintain all together, click [here](#) for more information.

Tasks for Windows Admin Group Cleanup

Inherit from Parent Add Task Save ↺

Shadow Account

Script	Policy	Actions
Check Status Remote Windows	After Check-in,On demand	⋮
Password Reset Remote Windows	On demand	⋮
Windows Local Admin Group Cleanup	Every (n) days:1,On demand	⋮

6. Click the **Save** button.

7. Return to the record, active the Execute dropdown and select our **Windows Local Administrators Group Cleanup** task.

Windows Admin Group Cleanup

Go to Parent ▼

Connect... ▼

Execute... ▼

**Name**

Windows Admin Group Cleanup

**Description**

Use this record to clean the local Admin group membership

Check Status Remote Windows

Password Reset Remote Windows

Windows Local Admin Group Cleanup

8. When the task executes, open the **Job History** tab and check the state. When the State is Complete, open the Details to review all users that were removed from this host’s local Administrators group.

Job Detail for Record: Windows Admin Group Cleanup

**Created**

02/16/2018 11:23

**Scheduled**

02/16/2018 11:23

**Type**

Periodic

**State**

Completed

**Response**

1 Removed: XT\\ref01

2 Removed: XT\\psenescu

3 Removed: XT\\itadmin

4 Removed: XT\\alt

5 Removed: XT\\admin

6 Removed: DEMO-SERVER-XTW\\mkloc

7 Removed: DEMO-SERVER-XTW\\local01

8 Removed: DEMO-SERVER-XTW\\john

9 XTAM Index:Processed

10 XTAM Success

When reviewing the *Job History*, you will notice two Result states for Completed tasks. The Result “Processed” indicates that the task was run successfully and it found and removed at least one account from the host’s group. The Result “Compliant” indicates that the task was run successfully, however there were no additional accounts found to be removed from the host’s group so it is deemed in compliance with the policy.

Found 37 job records.



Show 50 entries

Search:

Copy

CSV

Excel

PDF

Print

Showing 1 to 37 of 37 entries

Time	Type	User	Object	Task	Result	State	
02/16/2018 12:25:30	OnDemand	Chris Kolodziejcki (chrisk)	<a href="#">Windows Admin Group Cleanup</a>	Windows Local Admin Group Cleanup	Compliant	Completed	<a href="#">Details</a>
02/16/2018 12:24:11	OnDemand	Chris Kolodziejcki (chrisk)	<a href="#">Windows Admin Group Cleanup</a>	Windows Local Admin Group Cleanup	Compliant	Completed	<a href="#">Details</a>
02/16/2018 12:23:18	OnDemand	Chris Kolodziejcki (chrisk)	<a href="#">Windows Admin Group Cleanup</a>	Windows Local Admin Group Cleanup	Compliant	Completed	<a href="#">Details</a>
02/16/2018 11:23:39	Periodic	Service Service (pamservice)	<a href="#">Windows Admin Group Cleanup</a>	Windows Local Admin Group Cleanup	Processed	Completed	<a href="#">Details</a>

Now that this task was executed successfully and the results confirmed, you may return to the *Task* and update the policy so that this process can be automated and add it to additional records so you can begin your enforcement across your enterprise.

### Bulk Task Execution

You can also execute this or any task against several records by simply selecting the checkbox option for the records in their folder location then choosing the Bulk Actions > **Execute** menu option.

Next, check the box next to the task name and then finally the **Select** button to execute this task against the chosen records.

Found 8 record(s) and 1 folder(s).

<input type="checkbox"/>	Expired Certificates		<input type="button" value="Request Access"/> <input type="button" value="Request Execute"/> <input type="button" value="Share"/> <input type="button" value="More"/>
<input type="checkbox"/>	Network Web Server Account Record Type: Active Directory	Authenticate to the internal network	<input type="button" value="Request Access"/> <input type="button" value="Request Execute"/> <input type="button" value="Share"/> <input type="button" value="More"/>
<input checked="" type="checkbox"/>	Production Record Type: Windows Host		<input type="button" value="Select All"/> <input type="button" value="Select Records"/> <input type="button" value="Unselect All"/> <input type="button" value="Play"/> <input type="button" value="Share"/> <input type="button" value="More"/>
<input type="checkbox"/>	Production Web Server (A) SSL Certificate Record Type: Certificate	... - Expires December 2018	<input type="button" value="Request Access"/> <input type="button" value="Request Execute"/> <input type="button" value="Share"/> <input type="button" value="More"/>
<input type="checkbox"/>	Production Web Server (B) SSL Certificate Record Type: Certificate	... - Expires December 2018	<input type="button" value="Request Access"/> <input type="button" value="Request Execute"/> <input type="button" value="Share"/> <input type="button" value="More"/>
<input checked="" type="checkbox"/>	Web Server - Development Record Type: Windows Host	...ment and testing only (internal)	<input type="button" value="Select All"/> <input type="button" value="Select Records"/> <input type="button" value="Unselect All"/> <input type="button" value="Play"/> <input type="button" value="Share"/> <input type="button" value="More"/>
<input checked="" type="checkbox"/>	Web Server - Production A Record Type: Windows Host	Production web server (prodA)	<input type="button" value="Copy"/> <input type="button" value="Cut"/> <input type="button" value="Delete"/> <input type="button" value="Play"/> <input type="button" value="Share"/> <input type="button" value="More"/>
<input checked="" type="checkbox"/>	Web Server - Production B Record Type: Windows Host	Production web server (prodB)	<input type="button" value="Copy"/> <input type="button" value="Cut"/> <input type="button" value="Delete"/> <input type="button" value="Play"/> <input type="button" value="Share"/> <input type="button" value="More"/>
<input type="checkbox"/>	Web Server - Staging Record Type: Windows Host	Staging web server. Used for pre-deployment testing before release	<input type="button" value="Copy"/> <input type="button" value="Cut"/> <input type="button" value="Delete"/> <input type="button" value="Play"/> <input type="button" value="Share"/> <input type="button" value="More"/>

## Modifying the task

### Modifying the task to exclude additional users or to target a different group.

1. Login to PAM with a System Administrator account.
2. Navigate to Administration > Scripts.
3. Locate the script named *Windows Local Administrators Group Cleanup* and click its **Edit** button.
4. In the **Custom Code** field, take note of the first two lines:

Script Windows Local Administrators Group Cleanup

Script Name	Windows Local Administrators Group Cleanup
Description	A Windows script to remove all users from the host's local Administrators group except for the Local Administrator and Domain Administrator accounts.
Job Execution Strategy	Windows Remote
Custom Code (PowerShell)	<pre> 1 \$LocalGroupName = 'Administrators' 2 \$LocalAdmins = 'Administrator,Domain Admins' 3 \$computerName = '.' 4 </pre>

- The first line targets the script to the host's group named Administrators. If you want to target another group change the value between the single quote marks. For example, 'Guests'
- The second line specifies the accounts to exclude from cleanup or removal. If you want to include additional users, add their name to this comma separated list, between the single quote marks. For example, 'Administrator,Domain Admins,jwilliams'.

5. Click the **Save** button when done.

Once saved, the changes made to this script will automatically be applied to all tasks that are associated to it.

We would recommend you test the change before automating it across your enterprise.

## Setting Windows Passwords

PAM to reset or rotate a Windows password without knowing the current password.

There may be times when you want to bring under management a Windows account that you currently do not know the password to.

Such examples may be Windows accounts that are used for Service Log Ons, Application Pools or Installation and Administrative accounts that were created long before you were an employee of your business.

And of course, it can be used in that unfortunate situation where the password was lost or forgotten.

PAM provides tasks that will assist in managing and rotating passwords for Windows account in both scenarios; one where you have the full account credentials (task: *Password Reset Remote Windows*) and the other where you do not possess the account's password (task: *Password Set Remote Windows*). To put it into simple terms, think of them like this:

- Password **Reset** Remote Windows will reset a Windows account password by a method that first specifies the current password and then issues a new password. Much like a user would do during a Windows Change Password exercise.
- *Password Set Remote Windows* will reset a Windows local account password by issuing a new password without first supplying the current one. This replicates the process that an Administrator would take to reset a password on behalf of another account and is precisely why it can only be done with an Administrator account.

If this account is being used for a Windows Service Log On account, please review our article about the [Reset Password on Service Dependencies task](#) before executing this task.

If you find yourself in this situation and need to automate the rotation of an account without the password, then follow through this procedure to configure your task in PAM.

1. Create a new PAM record using the **Windows Host** or any custom type you have that inherits from Windows Host.
2. Enter a Name, Description (optionally), Host and Port for the Windows host where this account is a valid user.
3. In the **User** field, enter the account name.
4. Leave the **Password** field empty.



User

localuser

Password

- Click the **Save and Return** button.
- Open the record’s Task menu by selecting Manage > Tasks.
- Add the Task **Password Set Remote Windows** to this record by using one of these two procedures:
  - Add the Task directly to the record’s Record Type and allow inheritance to apply it to this record. *This is the recommended approach.*
  - Make this record’s Task unique by clicking the **Make Unique** button and adding the task directly to this record.
- Once the task is applied, configure the task’s Policy to include the **On Demand** execution. In this example, we are going to manually execute the reset, however you can configure any additional policies including automated events as you need.
- Add a [Shadow Account](#) that contains a user that is the member of this Windows host’s local Administrator group.

Tasks for Set without Current Password

Inherit from Parent

Add Task

Save

Shadow Account

Windows Local Admin Group Members (script to display list of Windows local Administrators)

Script	Policy	Actions
Check Status Remote Windows	On demand,After Check-in	...
Password Set Remote Windows	On demand	...

- Click the **Save** button.
- Return to the record, active the **Execute** dropdown and select our **Password Set Remote Windows** task.

Set without Current Password

Go to Parent

Connect...

Execute...

Name

Set without Current Password

Description

Windows password set without current password

Check Status Remote Windows

Password Set Remote Windows

- On the next page, accept the current or generate a new password and then click the **Schedule Job** button to begin.

Password

.....



Validate

Generate

13. When the task executes, open the **Job History** tab and check the state. When the State is *Complete*, open the *Details* to ensure the operation completed successfully.

Job Detail for Record: Set without Current Password

Created

02/16/2018 11:14

Scheduled

02/16/2018 11:14

Type

OnDemand

State

Completed

Response

1 XTAM Success

14. Return back to the Record's page and observe that the password field now contains a valid password which is being managed by PAM.

User

localuser

Password

(3Q1gld9jY+#X&lt;0!2BIHt2pe@JNm2Ck JWZ1[0wy)%lm4EwUp=A

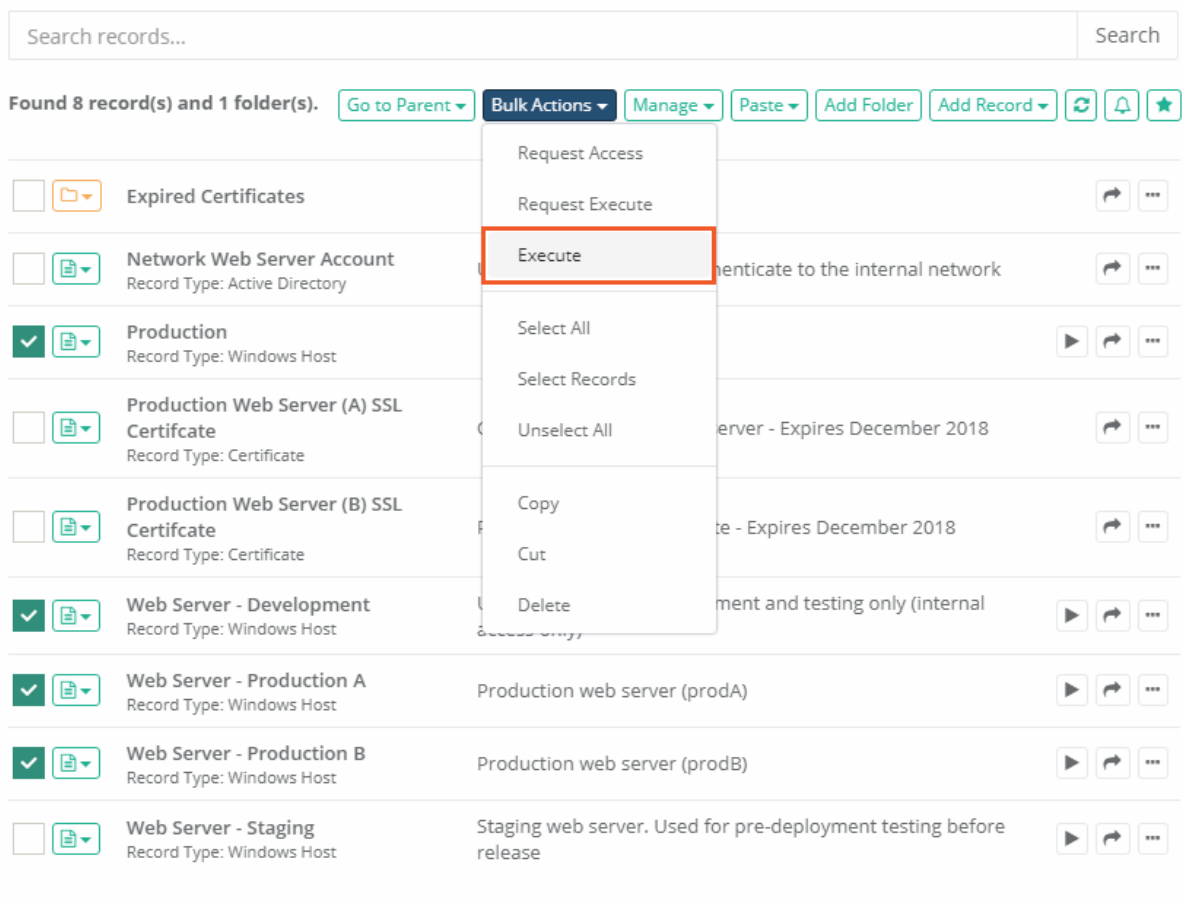


Now that we have successfully set the password for this account, you may return to the Task and update the policy so that this process can be automated.

### Bulk Task Execution

You can also execute this or any task against several records by simply selecting the checkbox option for the records in their folder location then choosing the Bulk Actions > **Execute** menu option.

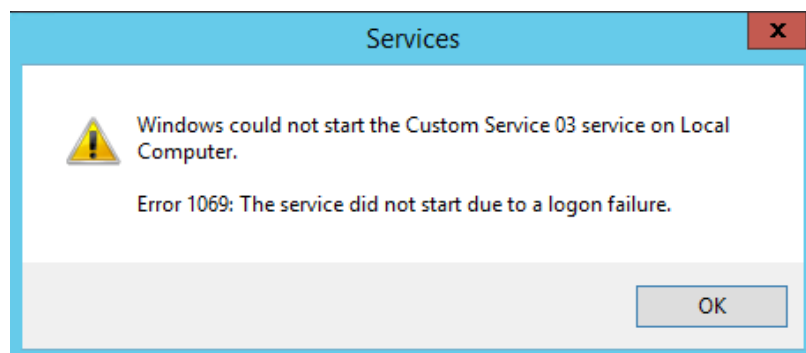
Next, check the box next to the task name and then finally the **Select** button to execute this task against the chosen records.



## Rotating Domain Passwords used for Services

Any services that run in a Windows environment have an associated Log On account that is used to start this service.

When this account is a Domain Account and the associated password is changed, you need to ensure that the new password is also updated in the service configuration on every endpoint where it is used or else the service will fail to properly start.



With PAM, Domain Accounts can be easily managed which allows for automated password rotations using extremely complex and randomized strings.

Once this managed password is reset, PAM will then process each included endpoint where this Domain Account is being used as a Log On service account and also update the service with this new password.

Once setup, this process is entirely automated so you can schedule the operation to take place as often as required or needed.

The remaining portion of this article will describe how to properly setup this process.

We will outline the entire process including several steps that may be optional in your deployments.

Although the inclusion of all steps will make the page longer, it will accurately detail all possible scenarios in order to present the full picture.

## Setup

First, we will create a new Folder (or Vault) **Domain Service Account Management** to more easily organize all the components.

This step is optional, but we would recommend creating a container per Domain Account that you would like to manage for this scenario.

Our folder will contain the following records:

1. Domain Administration account to be used as the Shadow Account for the password reset.
  - This record will be created using the type *Active Directory User* and will contain the credentials for a Domain Administrator. This will be used as the [Shadow Account](#) to rotate the password on the Domain Service Account.
  - If the Domain Account can change its own password, this record is not required. We use the Domain Admin as the shadow account in our example to eliminate any possible security issues in AD.
2. Domain Account that is the account that is the Service Log On As account.
  - This record will be created using the type *Active Directory User* and will contain the credentials of the Domain Service Account.
3. A Windows Host that will be used to reset the password of the Domain Account.
  - This record will be created using the type *Windows Host* and will be used as the host where the Domain Service Account password will be reset.
  - If you are using the **Password Reset LDAP** task on the Domain Account record, then this record is not needed. We are using a separate *Windows Host* record in our scenario to further illustrate the entire process but understand that its inclusion is optional.
4. A *Windows Host* record for each endpoint that contains a Service that is configured with the Domain Account. Our example will contain two Windows Host records, but your scenario may contain more or less.






If you are unsure or do not want to manually create records for each Windows Host, you can use the Discovery feature to automatically create records where a Service is found using this account. Please review the [Discovery](#) article for additional information and make note of the parameter **Auto-Import Filter** located in the Auto-Import section to implement this feature.

## Record List

Home / Records / Domain Service Account Management

Search ?

Found 5 record(s). Go to Parent Bulk Actions ▾ Manage ▾ Reports ▾ Paste ▾ Add Folder Add Record ▾ ↺ 🔔

<input type="checkbox"/>		<b>Domain Admin</b> ID: 3699991, Record Type: Active Directory Account	Used as shadow account to reset the domain service account password	<span>↺</span> <span>⋮</span>
<input type="checkbox"/>		<b>Domain Service Account</b> ID: 3699996, Record Type: Active Directory Account	Domain account that is the Log On As account for local services across the domain	<span>↺</span> <span>⋮</span>
<input type="checkbox"/>		<b>Windows Host used for Password Reset</b> ID: 3700021, Record Type: Windows Host	The Domain Service Account password will be changed using this Windows Host	<span>▶</span> <span>↺</span> <span>⋮</span>
<input type="checkbox"/>		<b>Windows Host with Service Dependencies (01)</b> ID: 3700031, Record Type: Windows Host	This Windows Host contains the local service that are using the Domain Service Account as the Log On As account	<span>▶</span> <span>↺</span> <span>⋮</span>
<input type="checkbox"/>		<b>Windows Host with Service Dependencies (02)</b> ID: 3700058, Record Type: Windows Host	This Windows Host contains the local service that are using the Domain Service Account as the Log On As account	<span>▶</span> <span>↺</span> <span>⋮</span>

### Step by Step Configuration Example

1. Login to PAM with a System Administrator account.
2. Navigate to Administration > Scripts and click the **Create** button
3. For this new script, enter the following values:
  - **Script Name:** Password Reset Remote Windows Trigger (or a name of your choosing)
  - **Description:** Windows password reset script that also triggers update on dependent service accounts (or a description of your choosing)
  - **Job Execution Strategy:** Windows Remote

- **Custom Code (Powershell):**

```
1 | ${ResetPassword}
2 | #XTAM TRIGGER REF Windows Remote Reset Dependent Services
```

#### Script

Home / Scripts / Password Reset Remote Windows Trigger

Script Password Reset Remote Windows Trigger

Save Factory Default Cancel ↺

**Script Name** Password Reset Remote Windows Trigger

**Description** Windows password reset script that also triggers update on dependent service accounts

**Job Execution Strategy** Windows Remote

**Custom Code (PowerShell)**

```
1 | ${ResetPassword}
2 | # PAM TRIGGER REF Windows Remote Reset Dependent Services
```

4. Click **Save** to complete the creation of this new script.
5. Navigate to Records > All Records and determine a parent location to create your new folder.
6. In this parent create a new folder named **Domain Service Account Management**.
7. In this folder create a new *Active Directory User* record named **Domain Admin** and input your AD Domain Administrator credentials.
8. In this folder create a new *Active Directory User* record named **Domain Service Account** and input your AD Domain Service Account credentials.
9. In this folder create a new *Windows Host* record and enter the following values:
  - **Name:** Windows Host used for Password Reset (or a name of your choosing)
  - **Description:** The Domain Service Account password will be changed using this Windows Host (or a description of your choosing)
  - **Reference Record:** select your Domain Service Account record created in step 8.
  - **Host:** your host name

- **Port:** your host's port

Windows Host used for Password Reset

Name

Windows Host used for Password Reset

Description

The Domain Service Account password will be changed using this Windows Host

Reference Record

Domain Service Account

Type

Windows Host

Host

10.0.0.24

Port

10024

User

dservice@xt.com

Password

.....

Save

Save and Return

Cancel

10. Open the record's Task menu by selecting **Manage > Tasks** and click the **Make Unique** button.
11. Now click the **Add Task** button to configure the new task for this record.
12. On the Add Task page, select your new script from step 3 *Password Reset Remote Windows Trigger* and then choose at least one Event. We will select the *On Demand* event, but you may decide to use one of the automated options.
13. Click the **Save** button to complete the configuration.
14. Back on this record's Task page, in the **Shadow Account** field, select your Domain Admin record from step 7 and again click the **Save** button to complete the configuration.

Tasks for Windows Host used for Password Reset

Inherit from Parent

Add Task

Save

Shadow Account

Domain Admin (Used as shadow account to reset the domain service account password)

?

Script

Policy

Actions

Password Reset Remote Windows Trigger

On demand

...

15. Return to your new folder and create a new *Windows Host* record for the host that contains a service configured with your Domain Service Account as a Log On As account. For the record, be sure the

following is configured:

- **Reference Record:** select your Domain Service Account record created in step 8.
- **Shadow Account (for the Tasks):** select your Domain Admin record created in step 7.
- **Script:** select the default Script *Windows Remote Reset Dependent Services* with the *Event On Demand*.

Tasks for Windows Host with Service Dependencies (01)

Inherit from Parent Add Task Save ↺

Shadow Account Domain Admin (Used as shadow account to reset the domain service account password) ⓘ

Script	Policy	Actions
Windows Remote Reset Dependent Services	On demand	+

16. Ensure everything is saved between each step and repeat step 15 for each new endpoint that you wish to add.

Please note that you can setup this task on the Record Type itself and take advantage of task inheritance so you do not have to repeat some steps for each record.

That completes the configuration.

Please continue to the next section to understand how this can be triggered and how the process flows from initiation to success completion of each task.

## Process Flow

The following summarizes how to initiate the process (manually) and what happens when it is triggered.

- To initiate the process manually, execute the task **Password Reset Remote Windows Trigger** on your record Windows Host user for Password Reset.
- PAM will use the Shadow Account on this host to reset the password of the Domain Service Account.
- When the password is reset successfully, PAM then executes the trigger *#XTAM TRIGGER REF Windows Remote Reset Dependent Services* that is contained in your new script. This trigger specifically looks for all records that contains the Reference Record of your Domain Service Account.
- On these found records, PAM will now schedule each record's associated task *Windows Remote Reset Dependent Services*. This task is designed to connect to the specified host, find each service that has the Log On As account defined in its User field and update it with the new password. Because this User and Password are referenced back to the original, it will always contain the most recent password.
- Finally, the PAM Job Engine will process all dependent records and create a Job History entry for each. These Job History events will detail the successfully completion of the task and list all the services (by Name) that were updated.



Job History

Found 8123 job records.

Time: All Jobs State: Any

Show 50 entries

Search:

CSV PDF

Showing 1 to 50 of 8,123 entries

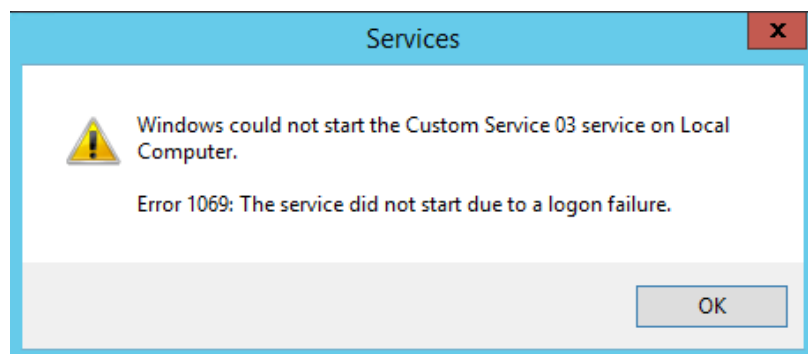
Time	Type	User	Object	Host	Task	Result	State	
12/24/2018 09:27:03	On Demand	Service Service (pamservice)	<a href="#">Windows Host with Service Dependencies (02)</a>	10.0.0.60	Windows Remote Reset Dependent Services		Completed	<a href="#">Details</a>
12/24/2018 09:27:03	On Demand	Service Service (pamservice)	<a href="#">Windows Host with Service Dependencies (01)</a>	10.0.0.23	Windows Remote Reset Dependent Services		Completed	<a href="#">Details</a>
12/24/2018 09:26:52	On Demand	Chris Kolodziejewski (chrisk)	<a href="#">Windows Host used for Password Reset</a>	10.0.0.24	Password Reset Remote Windows Trigger		Completed	<a href="#">Details</a>
12/24/2018 09:19:18	Once a Week	Service Service (pamservice)	<a href="#">MS SQL Studio Login</a>	dev-sql16	Password Reset MS SQL Server		Completed	<a href="#">Details</a>
12/24/2018 09:16:50	Once a Month	Service Service (pamservice)	<a href="#">Script Strategy Execution (Windows)</a>	10.0.0.23	Script Strategy Execution (Windows)		Completed	<a href="#">Details</a>

## Rotating Local Passwords used by Services

Any services that run in a Windows environment have an associated Log On account that is used to start this service.

When the password for this account is rotated, you need to ensure that the password is also updated in the service configuration or else it will no longer be able to start.

This also applies to any task scheduled in Windows Task Scheduler that includes a saved password.



### Windows Service Failed to Start – Incorrect Log On Password

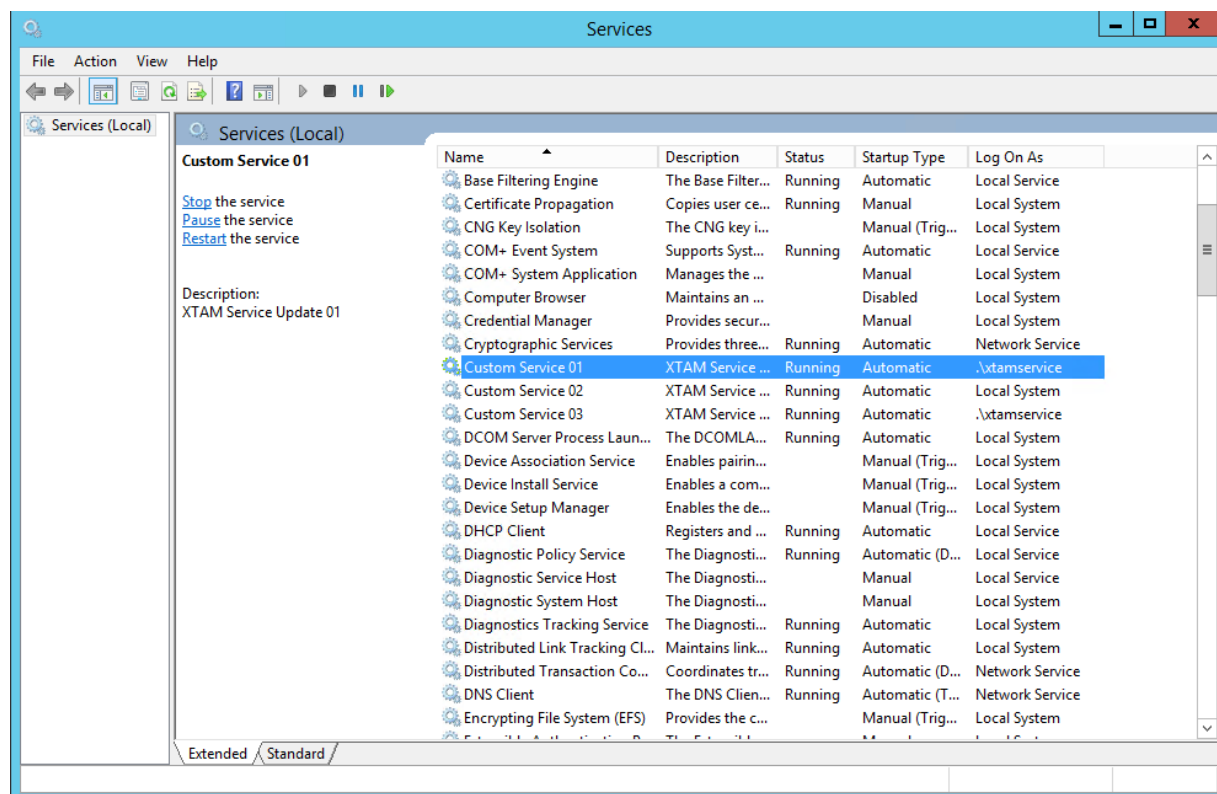
PAM supports the password rotation for Windows Local and Domain accounts and it also can check for and update passwords associated with any Services Log On account or Windows Task Scheduler tasks as well.

If you want to rotate password for accounts associated to services or tasks, then please continue reading.

Before we show the procedure, let's first set the stage. In my environment, I have created three custom services, all set to run Automatically, with two configured with a Log On account *xtamservice* and one using the traditional Local System.

This walk through will describe the scenario where you want to rotate the password on the *xtamservice* account and subsequently update the Service's Log On account with the newly rotated password.

At the end, the password will rotate on the *xtamservice* account, its Service dependencies will be found by PAM, Log On account password will be updated with the new password and the service will remain Running (it can also be restarted without error).



1. Create a new PAM record using the **Windows Host** or any custom type you have that inherits from Windows Host
2. Enter a Name, Description (optionally), Host and Port for the Windows host that has this Service running.
3. In the User and Password fields, enter the User and Password that you wish to rotate which has Service dependencies. In our example, this is the account *xtamservice* and its corresponding password.

User xtamservice

Password \*\*\*\*\*

If you do not know the account's password, please review our article for the [Set Windows Password task](#).

4. Click the **Save and Return** button.

- 5. Open the record’s Task menu by selecting Manage > Tasks.
- 6. Add the Task *Password Reset Remote Windows with Service Dependencies* to this record by using one of these two procedures:
  - a. Add the Task directly to the record’s [Record Type](#) and allow inheritance to apply it to this record. *This is the recommended approach.*
  - b. Make this record’s Task unique by clicking the **Make Unique** button and adding the task directly to this record.
- 7. Once the task is applied, configure the task’s Policy to include the On Demand execution. In this example, we are going to manually execute the reset, however you can configure any additional policies including automated reset as you need.
- 8. In our scenario, our Service account *xtamservice* is not an account that has any Administrative nor remote execution permissions on this host, so we will need to configure a [Shadow Account](#) that does have these permissions to execute this task. *If your service account also have Administrative rights then you can skip this step.*

Tasks for Service Account

Inherit from Parent

Add Task

Save

Shadow Account

Windows Local Admin Group

Script	Policy	Actions
Check Status Remote Windows	On demand,After Check-in	
Password Reset Remote Windows	On demand	
Password Reset Remote Windows with Service Dependencies	On demand	

- 9. Click the **Save** button.
- 10. Return to the record, active the Execute dropdown and select our **Password Reset Remote Windows with Service Dependencies** task.

Service Account

Go to Parent

Connect...

Execute...

Name	Service Account
Description	Account that runs our custom services

Check Status Remote Windows

Password Reset Remote Windows

Password Reset Remote Windows with Service Dependencies

- 11. On the next page, accept the current or generate a new password and then click the **Schedule Job** button to begin.

Password

#### Formula Rules

- Lowercase : 15
- Max : 50
- Min : 50
- Numbers : 10
- SpecialCharacters : 10
- Uppercase : 15
- Username : 1

12. When the task executes, open the **Job History** tab and check the state. When the State is **Complete**, open the **Details** to ensure the Services that used this account as its Log On were updated.

#### Job Detail for Record: Service Account

Created	02/15/2018 16:59
Scheduled	02/15/2018 16:59
Type	OnDemand
State	Completed
Response	1 Updated: Custom Service 01 2 Updated: Custom Service 03 3 Updated: XtonUserTest 4 XTAM Success

13. Optionally, connect to this host and manually restart one of the services to verify that it completes successfully.

Now that we have successfully configured, executed and tested that the password was reset and the service is still functionally, you may return to the Task and update the policy so that this process can be automated.

## Autologon Domain Account Management (Windows Kiosk Mode)

This article describes the Autologon Domain Account Management feature provided by Imprivata PAM.

Windows *Kiosk Mode* is used across many organizations to provide a single or multi-application-controlled environment. In retail, this could be used to display digital signs through a PowerPoint presentation or in a hospital setting, for shared workstations at a nursing station or patient exam room. Kiosk mode, native to Windows, is useful for many business applications.

Configuration of Kiosk mode can be done using a Windows Autologon account defined on the Kiosk workstation itself. What becomes common in such enterprise-wide deployments is the password of each autologon account is identical, opening the possibility of a security breach or a potential discovery during an audit.

Using Imprivata PAM (Privileged Access Management), you can manage the domain autologon accounts of Kiosk mode enabled workstations, including the option to perform an on-demand or automated password

rotation. Automated password rotation ensures that you can maintain strong, unique passwords across all domain Autologon accounts and periodic password resets to maintain security and risk compliance.

## Pre-requisites

Before we begin, there are some prerequisites that are required for this operation to be successful.

1. Windows 10/11 Kiosk Mode is supported only. Windows 7 or any other version is not supported.
2. Unique domain Autologon accounts per workstation are supported by this feature only. Local Autologon accounts are not supported.
3. *The autologon password is set to the encrypted area of the Windows registry (Sysinternals).*

To be successful in this, we recommend to use a [Shadow Account](#), that is a member of the local Administrators group on the Windows Kiosk workstation.

4. *WinRM must be enabled and configured on each Kiosk workstation* where the Autologon account is being managed. WinRM is used to remotely execute the script by PAM. Use powershell to check WinRM:
  - Open PowerShell from any Windows Server
  - Test-WSMan -<kioskname>
5. PAM must be integrated with the AD (Active Directory) where the Kiosk Autologon accounts are enabled users.
6. After task execution has been completed successfully, *a restart of the Kiosk workstation may be required*, depending on the applications that are running on this workstation.

*By default, PAM will not restart the Kiosk workstation; however, there is a small modification that can be manually made to the script to enable a restart.*

7. This feature is tested and verified with the latest [Imprivata EAM](#) type 2 agent running on a *Windows 10 Kiosk mode enabled workstation* to ensure it is not negatively affected.

Please note that other agents, applications or hardware on the workstation are not verified, so please plan and test the Autologon Domain Account Management accordingly in your environment as required.

## Configuration

To configure this feature, please follow these steps.

### Step 1. Create a new Script

1. Login to PAM with a System Administrator's account.
2. Navigate to Administration > Scripts and click **Create**, add the required fields:
  - **Script Name:** Password Reset for Autologon Account with Shadow Account
  - **Description:** *Optional value of your choosing*

- **Job Execution Strategy:** Windows Remote
- **Custom Code:** echo

3. Click **Save**.
4. After the script is saved, click the **Factory Default** button to load the new script.
5. Click **Save** again to save the new script that was loaded.

## Step 2. Create a new Record Type

1. Navigate to Administration > Record Types and click **New Record Type** and create a new *Record Type*, add the required fields, and **Save** this new record:
  - **Name:** Windows Autologon or a name of your choosing
  - **Description:** Optional value of your choosing
  - **Session Manager:** empty
  - **Parent Type:** empty
  - **Hidden:** unchecked
  - **Personal Vault:** unchecked

After the new Record Type is saved, a new section will appear that is used to create fields.

## Step 3. Create new Fields

1. Click **Add Field** to create a new field, the first of three total.  
Use the guidance below:

### First Field:

- Field Type: **String**
- Name: **Host**
- Display Name: **Host**
- Hidden: *unchecked*
- Secured: *unchecked*
- Indexed: *unchecked*
- Order: **100**
- Helper: *empty*
- Default Value: *empty*

### Second Field:

- Field Type: **String**
- Name: **User**
- Display Name: **User**
- Hidden: *unchecked*
- Secured: *unchecked*

- Indexed: *unchecked*
- Order: **200**
- Helper: *empty*
- Default Value: *empty*

### Third field:

- Field Type: **String**
- Name: **Password**
- Display Name: **Password**
- Hidden: *unchecked*
- Secured: *checked*
- Indexed: *unchecked*
- Order: **300**
- Helper: *empty*
- Default Value: *empty*

2. Click the **Save** button on this page.

The three needed fields have been created.

## Step 4. Set the Password Complexity formula

1. Navigate to Administration > *Record Types* page and click the **Formula** button.
2. Set the *Password Complexity formula* in PAM to meet or exceed the requirements of your *Domain Password Policy*.
3. Click the **Save** button and then return to the *Record Type* page.

Note: When testing, it is typical to run the password reset task several times in a short amount of time which may result in errors due to the *Minimum Password Age* requirement defined in your Domain Password Policy. If the *Minimum Password Age* is set to 1 (or higher), then you may only run this task once a day as the domain policy will fail additional attempts.

## Step 5. Set the Tasks configuration

1. Navigate to Administration > *Record Types* page and click the **Tasks** button.
2. On this *Tasks* page, click the **Add Task** button, select the following:
  - Script: **Password Reset for Autologon Account with Shadow Account**
  - Target Record: **Record itself**
  - Event: **On Demand**
3. Click **Save** when completed.

We will return to this page later to finalize the Tasks configuration.

## Step 6. Create a record

1. Navigate to Records > All Records and click Add Container > **Add Vault**.
2. Create a new vault with the *Name* and *Description* of your choice.
3. Open the created vault, click the **Add Record** button and select *Active Directory User* from the dropdown menu.

Note: This record will contain an Active Directory account that will be used to reset the AD password of your Autologon account(s) and to update the registry on each Kiosk workstation. To accomplish both tasks this account is *required to have the necessary permission in Active Directory* to reset the password of another account and to be a member of the local Administrators group on every Kiosk workstation where the Autologon account is managed. If this AD account lacks these permission requirements, the task will fail to execute properly.

4. For this new record, enter the values:
  - **Name:** **Autologon Shadow Account** or a name of your choosing
  - **Description:** *Optional value of your choosing*
  - **Reference Record:** *leave empty*
  - **Type:** **Active Directory User**
  - **User:** *Active Directory login name in the form of **domain\user***
  - **Password:** *Active Directory account password*
5. Click **Save and Return** when complete.

## Step 7. Associate a new Record with the Task as a Shadow Account

1. Navigate to Administration > Record Types,
2. Locate and **Edit** your type *Windows Autologon*.
3. Click the **Tasks** button and in the [Shadow Account](#) field, **type** the record name of your Active Directory User you previously created to assign it to this field.
4. After the [Shadow Account](#) displays your [Active Directory](#) User record, click the **Save** button.
5. Navigate to your Vault to continue.
6. In the Vault, click the **Add Record** button and select the *Record Type* from the dropdown that was created earlier named *Windows Autologon*. For this new record, enter the values:

Note: This record will contain the values of a Kiosk workstation and Autologon account that you wish to manage.

- **Name:** **Kiosk Workstation 1** or a name of your choosing
- **Description:** *Optional value of your choosing*
- **Reference Record:** *leave empty*
- **Host:** The hostname of the Kiosk machine in either a fully qualified domain hostname or IP address.



- **User:** The name of the domain Autologon account in the form **domain\user**
- **Password:** The current, valid password of this domain Autologon account.

7. Click **Save and Return** when complete.

If you wish to manage additional Autologon accounts, then you can repeat the previous Step 6 to create a new record for each individual Kiosk workstation.

## Testing

To perform testing, we will execute the Task on the record that was created to manage the Autologon account on a Kiosk Workstation.

1. Open or View your Kiosk Autologon account record and click the **Execute** > *Password Reset for Autologon Account with a Shadow Account* button.
2. On the Schedule Job page, use the automatically generated random password that is provided and click the **Schedule Job** button. This will place the job into the PAM queue for execution.

Depending on the number of jobs currently in the queue, the task may be executed immediately, or it may take a few minutes to process.

3. To check the status and future results of the task execution, navigate back to the Record > **Job History** button. On the *Job History* page, it will display your current Task and its status. You may use the **Refresh** button to update the page until it is completed.

## How it Works

This feature is designed to perform two functions:

- To reset the password of the Autologon account in its domain.
- To update the registry, in the encrypted location, on the Host with this new password.

When the *Password Reset for Autologon Account with Shadow Account* task is executed the following occurs within the PAM Job Engine:

1. PAM connects to the Kiosk workstation to reset the password of the Autologon account contained within your Kiosk Autologon record. The script is executed by the Shadow Account assigned to this task.
    - If the password reset fails, then the task ends and reports an *Error as the State*.
    - If the password reset is successful, then the *task continues*.
  2. PAM connects to the Kiosk workstation (as defined by the Host in this record) using WinRM to update the registry with this new password. The registry update is performed by the Shadow Account assigned to this task.
- If the task execution against the Host fails, then the task ends and reports an *Error as the State*.

Depending on the condition of the failure, additional details may be available by clicking the **Details** button for this task.

- If the registry update fails, then the task ends as **Completed with Failed: Result Code: 1 as the Result**.

Depending on the condition of the failure, additional details may be available by clicking the **Details** button for this task.

- If the registry update is successful, then the task ends as

**Completed with Success:** *Result Code: 0 as the Result.*

- If you enabled the *Restart* command in the script, the Kiosk workstation will be immediately restarted upon this successful completion.

## Script configuration to enable the restart command

Enable the PAM script to restart the Kiosk workstation after a successful task execution.

In the script's default configuration, a Kiosk workstation restart is not performed; however, if it is required in your environment, then a simple modification to the script can be made to enable an automatic restart of the workstation. This restart will only occur if the task is completed successfully, as a last step.

1. Navigate to Administration > Scripts, locate and click **Edit** for the script named *Password Reset for Autologon Account with Shadow Account*.
2. Within this script, locate the below line using your browser's search and make the modification as noted, removing the **#** before the line (uncommenting):

```
1 | Restart-Computer -Force
```

3. Click the **Save** button to finish the modification.

## Rotating Domain Service Account Passwords in Additional Domains using LDAP Server and LDAP User Records

This article describes an example configuration that can be used to reset a password of domain service accounts in non-primary Active Directory domains.

Non-primary domain refers to a domain that is not used for [Active Directory integration](#) with PAM.

1. Login to PAM with a System Administrator account.
2. Navigate to Administration > Records Types.
3. Locate and select the Record Types **LDAP Server** and **LDAP User**, then click the **Bulk Actions** dropdown and choose **Enable**.
4. This will make both Record Types available to be used as Records in PAM.
5. Create the following folder structure. Note these folders are used as an illustrative example and it is not required to create them for the password reset operation to be successful.
  - LDAP
    - ADUsers
    - ADAdmins
    - DomainControllers
    - ServiceAccounts

6. In the *ADAdmins* folder, create a record using the Active Directory User type and, in this record, enter your Domain Admin account credentials.
7. In the *DomainControllers* folder, create a record using the **LDAP Server** type that is used to connect to this non-primary domain. Specify the LDAP URL for this domain controller and for credentials use the *Reference Record* field to reference the Active Directory User record created in the previous step. Note that the LDAP URL must use a secure LDAPS connection like this example:  
ldaps://dc.somedomain.com:636.

Name	Domain Controller	
Description	Record to manage Domain Controller	
Reference Record	Domain Admin; Doman Admin account credentials (Paths: /)	

---

Type	LDAP Server	▼
LDAP URL	ldaps://dc.contoso.com:636	
User	domainAdmin@contoso.com	?
Password	.....	

Password is Very Strong.

8. In the *ADUsers* folder create a record using the **LDAP User** type. This record will contain the LDAP account which will have the password rotated. Specify the LDAP account using UPN format like this example: username@somedomain.com. Additionally, in this record, navigate to Manage > Tasks, click the **Make Unique** button and in the *Shadow Account* field, select the LDAP Server record that was created in a previous step in the *DomainControllers* folder. Finally, click the **Save** button.

Tasks for AD User Account	
Inherit from Parent Add Task Save ↺	
Shadow Account	Domain Controller; Record to manage Domain Controller /ldaps://dc.contoso.com:636 (Pat ?)
Time Window	ⓘ ⓘ

9. Next, we will create the script that processes the password reset operation. Navigate to Administration > Scripts and click the **Create** button. On the script create page, enter the following values and **Save** when

complete:

- Script Name: LDAP password reset with dependent service accounts
- Strategy: LDAP
- Custom Code:
  - `\${ResetPassword}
  - #PAM TRIGGER REF Windows Remote Reset Dependent Services

Now, we will return to the records and continue our configuration.

Save

Factory Default

Cancel

Script Name

LDAP password reset with dependent service accounts

Description

Job Execution Strategy

LDAP

Custom Code (shell)

```
1 `${ResetPassword}
2 #PAM TRIGGER REF Windows Remote Reset Dependent Services
```

10. In the *ServiceAccounts* folder create a record using the **LDAP User** type. This record will contain the LDAP credentials of the service account that is being managed. After this record is saved, navigate in it to Manage > Tasks and click the **Make Unique** button. Add the LDAP Server record created in an earlier step as the Shadow Account and click **Save**. Then, click the **Add Task** button, select the custom script *LDAP password reset with dependent service accounts* that was previously created, check the *On Demand* event option and finally the **Save** button.

Inherit from Parent

Add Task

Save

Shadow Account

Domain Controller; Record to manage Domain Controller /ldaps://dc.contoso.com:636 (Pat ?)

Time Window

Script	Policy	Actions
LDAP password reset with dependent service accounts	On demand	...

11. Return to the *ServiceAccounts* folder and create a record using the **Windows Host** type. This record(s) will represent the host(s) where the Service Account is present and where the service itself is running from that is being managed. In this Windows Host record, set the *Reference Record* field to be the LDAP User record that was created in the previous step in this same folder. Enter the appropriate value in the *Host* field (hostname, FQDN or IP address) and then click **Save and Return**.

## Windows Server

<b>Name</b>	Windows Server
<b>Description</b>	
<b>Reference Record</b>	Service Account; Managed service account (Paths: /)

---

<b>Type</b>	Windows Host
<b>Host</b>	10.0.0.25
<b>Port</b>	3389
<b>User</b>	APMservice@contoso.com
<b>Password</b>	.....

Password is Very Strong.

- From within this new record, navigate to Manage > Tasks and click **Make Unique**, then in the *Shadow Account* field select the *AD Admin account* from the record created earlier in the *ADAdmins* folder. Finally, click the **Add Task** button, select the script *Windows Remote Reset Dependent Services*, check the *On Demand* event option and finally the **Save** button.

## Tasks for Windows Server

[Inherit from Parent](#)
[Add Task](#)
[Save](#)
[Refresh](#)

<b>Shadow Account</b>	Domain Admin; Doman Admin account credentials (Paths: /)
<b>Time Window</b>	

---

Script	Policy	Actions
Windows Remote Reset Dependent Services	On demand	...

- This completes the configuration and we can now test the process. To execute the operation, open the LDAP User record created in the ServiceAccounts folder and execute the on-demand script *LDAP password reset with dependent service accounts*. After this password is successfully changed, the Service Accounts update will be triggered on each Windows Host record where this service account was set as

the reference record.

## Hostname DNS Verification

To prevent potential abuse, PAM records can now perform hostname verification prior to executing tasks.

This can potentially reduce the ability to alter DNS in order to gain access to a managed Windows endpoint.

### *To implement hostname verification*

1. Login to PAM with a System Administrator account.
2. Navigate to Administration > Record Types.
3. Locate the [Record Type](#) that you wish to enforce this verification on and click its **Edit** button.

We recommend, but do not require, creating a custom record type and inheriting from the Windows Host (or another) parent type rather than modifying any default types. For more information about *Custom Record Types*, please read [this](#) article.

4. On the Record Type's page, scroll down and click the **Add Field** button. Configure the following values:
  - **Field Type:** Checkbox
  - **Name:** HostNameDNS
  - **Display Name:** *Disable Hostname Verification (or another value of your choosing)*
  - *The remaining values can be configured to your requirements*
5. Click the **Save** button on this *Add Record Type Field* page.
6. PAM will return you to the [Record Type](#) page, click this **Save** button to complete the configuration.

Found 1 fields.

[Formula](#) [Tasks](#) [Commands](#) [Save](#) [Delete](#) [Cancel](#) [↺](#)**Name** Windows Host with Verification**Description** Windows Host that enforces hostname verification**Session Manager** RDP ▼**Parent Type** Windows Host ▼**Hidden** ☐**Personal Vault** ☐[Add Field](#)

Field	Display Name	Field Type	Secured	Indexed	Helper	Actions
HostNameDNS	Disable Hostname Verification	Checkbox				<a href="#">Edit</a>

To test hostname verification, please perform the following steps:

1. Create a new record or reuse an existing record that utilizes the [Record Type](#) that was updated in the previous section.
2. On this new **Disable Hostname Verification** field, do not check this box. *Unchecked/disabled* means the hostname will be verified, while *Checked/enabled* means that verification will be skipped.
3. Execute a task against this record. Ensure that the hostname in the record will fail verification prior to executing this task.

When the task is executed, it will first verify the hostname defined in the record and in this scenario, this verification will fail. This will prevent the task from executing and it will therefore report a Status of *Error*

and the details of this error will be reported as such:

1

Failure to verify host name hostname from the record, detected hostname detected on the endpoint.

Job Detail for Record: Windows Host Verification

Host	dev.x
Task	Check Status Remote Windows
Created	01/11/2019 14:23
Scheduled	01/11/2019 14:23
Type	OnDemand
State	Error ( <a href="#">click here for additional information</a> )
Result	
Response	<div>1 Failure to verify host name dev.x, detected dev-se. Original:</div>

Of course, if the verification is successful, then the task will be executed as expected.

Job Detail for Record: Windows Host Verification

Host	dev.x
Task	Check Status Remote Windows
Created	01/11/2019 14:15
Scheduled	01/11/2019 14:15
Type	OnDemand
State	Completed
Result	
Response	<div>1 Success 2 XTAM Success 3 Script execution verified by result code</div>

## Automated Password Rotation for Multiple AD Servers

Password Reset for Multiple or Uniquely Configured [Active Directory](#) Servers.

The following guide describes the configuration process to automate the password reset or rotation of user and administrator accounts in multiple [Active Directory](#) servers or those requiring unique configuration compared to integration.



## Assumptions

This guide assumes the following environment:

1. Network includes several Active Directory servers or your Active Directory server under management has different configuration properties as compared to your AD Integration.
2. PAM server is deployed and operates successfully in the network
3. Network configuration allows PAM server to directly connect to all Active Directory domain controllers involved in the configuration
4. It is not required for PAM server to integrate with any of the Active Directory servers for authentication purposes
5. The goal of the guide is to configure PAM server to manage accounts (rotate or set passwords based on specified policies) in Active Directory servers.

## Concepts

To support the scenario described in the Assumptions section of this guide, the PAM System Admin first has to create a record of the record type *LDAP Server* to represent each Active Directory domain controller.

This *LDAP Server* record contains three vital properties: LDAP host, admin user and password of the admin user.

When PAM needs to reset a password for an Active Directory account, it connects to this AD using the host, user and password defined in the corresponding LDAP Server record.

After configuring LDAP Server records for each of the AD domain controllers, PAM System Admin creates user accounts that need to be managed using *LDAP User record*.

This *LDAP User record* contains the user and password properties to indicate an AD user to manage the password for.

LDAP User record includes default task list with two tasks: *Check Status LDAP* and *Password Reset LDAP*.

To indicate that this particular user is defined in a specific LDAP Server, the PAM System Admin makes the LDAP Server record for this specific AD domain controller a [Shadow Account](#) of the task list of this specific LDAP User.

When PAM decides to reset the LDAP User password as it is defined by the policies attached to the LDAP User tasks, PAM will connect to the AD domain controller using a shadow account on record given by LDAP Server record and then PAM will change the password of the main LDAP User record.

At the end, PAM will contain few LDAP Server records, each representing specific Active Directory domain controller.

In addition, PAM will contain multiple LDAP User records representing accounts to manage.

Each LDAP User record will have a Shadow Record defined in its task list to indicate the specific AD domain controller and admin credentials used to rotate password for this user.

PAM System Admins might take advantage of PAM record type inheritance to simplify management of multiple accounts related to the same active directory.

To do that, the PAM system admin creates a Record Type for each Active Directory to designate a user of this [Active Directory](#).

This Specific LDAP User record type must have its parent record type defined as a LDAP User. Also, this Specific LDAP User record type must have a task list including

Check Status LDAP and Password Reset LDAP with the shadow account defined as a specific LDAP Server for this Active Directory domain controller.

With this Specific LDAP User record type in place, all managed accounts for this Active Directory server could be created using Specific LDAP User record type so that each managed account will have an automatically defined (and centrally managed) task list with the appropriate shadow account.

The steps with Specific LDAP User record type has to be repeated for all other Active Directories creating Specific2 LDAP User and Specific3 LDAP User record types for Specific2 and Specific3 Active Directories under management, each with different shadow account on their record type task lists.

For PAM it does not matter where exactly (Vaults, folders or sub-folders) the records of LDAP Server, LDAP User or Specific LDAP User record types are located.

However, it might be beneficial to copy related records to folders corresponding to specific active directories to simplify management and permission structure of these records.

PAM system admins might decide to store LDAP Server records representing Active Directory servers in the separate folder or keep LDAP Server record in the folder related to its active directory together with all other accounts in this active directory.

The folder organization depends on the general folder architecture of the PAM deployment.

Note that PAM forbids reusing shadow accounts between different [Vault](#) for security reasons.

PAM requires a secure LDAPS connection to [Active Directory](#) to perform password reset and rotation. For more information about how PAM uses LDAPS and how it is configured, please review our [Secure Connectivity to an Active Directory Domain Controller](#) article.

## Prerequisites

1. The PAM configuration should be performed using an PAM System Administrator account.
2. Enable the *LDAP User* and *LDAP Server* record types which are disabled in an out of the box PAM deployment
  - a. Navigate to Administration > **Records Types**.
  - b. Locate and select the Record Types LDAP Server and LDAP User, then click the Bulk Actions dropdown and choose **Enable**. This will make both Record Types available to be used as Records in PAM.
3. Establish trust with each Active Directory server under management by using the SSLImport command in the PAM CLI utility as described [here](#).

## Configuration

1. Create a new LDAP Server record. Navigate to your PAM Record List location and select LDAP Server from the Add Record dropdown menu.

2. For this new LDAP Server record, enter the URL to your LDAP server, the LDAP Administrator UPN and this Administrator's Password. For example:
  - **LDAP URL:** ldaps://dc-host.company.com:636
  - **User:** admin@company.com
  - **Password:** Adm1nP3ss@word8
3. Click **Save and Return** when finished.
4. Create a new LDAP User record. This record will contain the user account whose password will be reset or automatically rotated.
5. Enter the values in the new LDAP User record as needed. For example:
  - **User:** user@company.com
  - **Password:** usersPassword
6. Click **Save and Return** when finished.
7. Open this LDAP User's record Task list using Manage > **Tasks** button.
8. Click **Make Unique** button on the record task list.
9. Select your *LDAP Server* record created earlier as a [Shadow Account](#) on this record.
10. Click Save when finished.
11. Execute the *Password Reset LDAP* task on the LDAP User record to test and verify the configuration.
12. Repeat from step 4 to create additional LDAP User records to manage more active directory accounts in the AD defined by the LDAP Server record created in the step 1.
13. Repeat all steps to add another AD domain controller with managed accounts in this domain controller.

### *Configuring Automation using Record Types*

1. Create your LDAP Server record as described in the steps 1, 2 and 3 of the previous Configuration section.
2. Navigate to Administration > Record Types.
3. Click **New Record Type** to create a new record type.
4. Specify your new record type parameters:
  - **Name:** Some Recognizable AD Name LDAP Users
  - **Parent Type:** LDAP User
5. **Save** your new Record Type.
6. Click the **Tasks** button on this new record type's edit page.
7. Add *Check Status LDAP* and *Password Reset LDAP* to the task list with the desired password rotation policy events.
8. **Save** the Task list.
9. Select your *LDAP Server* record created on the step 1 as a **Shadow Record** for the Task list.

Note: By associating the LDAP Server record as a Shadow Account for the LDAP User record type, this configures PAM to use the User and Password for the Server to execute the Password Reset task for all the LDAP User records.

10. **Save** the *Task list*.

Note: You can also customize the password complexity policy by clicking the [Formula](#) button on this page.

11. Repeat the process for other [Active Directory](#) servers you wish to use under management.
12. Navigate to the record list and create a new record of the record type *Some Recognizable AD Name* LDAP Users as in the Configuration section. This time, the record will already contain shadow account for the Specific Active Directory which simplifies the management process of multiple accounts in the same [Active Directory](#).

## Password Reset Remote SSH

The “Password Reset Remote SSH” script uses different methods for root (id=0) account (passwd that asks for only new password) and other accounts (passwd that asks for existing password and then for new passwords).

This script also uses a shadow account when specified to run password reset using the **passwd USER** command.

The script “Password Reset Remote Root” can only reset the password for the root account without any shadow records.

However, this script could be used as an example to develop custom password reset scripts for specific scenarios not covered by “Password Reset Remote SSH” script.

The “Password Reset Remote SSH” script executed for the record without shadow record:

```
1 | if [ "`id -u`" -eq 0 ]; then
2 |     passwd <<EOF\n{{NEWPWD}}\n{{NEWPWD}}\nEOF
3 |     echo xtam passwd error code: $?
4 | else
5 |     passwd <<EOF\n{{OLDPWD}}\n{{NEWPWD}}\n{{NEWPWD}}\nEOF
6 |     echo xtam passwd error code: $?
7 | fi
```

The “Password Reset Remote SSH” script executed for the record with [shadow record](#):

```
1 | sudo -S passwd {{LOGIN}} <<EOF\n{{NEWPWD}}\n{{NEWPWD}}\nEOF
2 | echo xtam passwd error code: $?
```

## OpenLDAP Compliant Server Password Change

The following page describes the configuration process to automate the password reset or rotation of user and administrator accounts from an OpenLDAP compliant server.

1. Login to PAM with a System Administrator account.
2. Navigate to Administration > Records Types.
3. Locate and select the Record Types **LDAP Server** and **LDAP User**, then click the **Bulk Actions** dropdown and choose **Enable**. This will make both Record Types available to be used as Records in PAM.

Found 36 record types.

Record Type		Parent Record Type	Session Manager	Bulk Actions		New Record Type	actions
<input type="checkbox"/>	Active Directory			Select All			Edit
<input type="checkbox"/>	AD Query	Active Directory		Unselect All			Edit
<input type="checkbox"/>	AS400		SSH	Enable			Edit
<input type="checkbox"/>	Azure			Disable			Edit
<input type="checkbox"/>	Certificate						Edit
<input type="checkbox"/>	Cisco	Unix Host	SSH				Edit
<input type="checkbox"/>	Google Chrome		RemoteApp				Edit
<input type="checkbox"/>	Informix						Edit
<input type="checkbox"/>	Internet Explorer		RemoteApp				Edit
<input type="checkbox"/>	Juniper	Unix Host	SSH				Edit
<input checked="" type="checkbox"/>	LDAP Server						Edit
<input checked="" type="checkbox"/>	LDAP User						Edit

- Now that the [Record Types](#) are enabled, we will first create a new LDAP Server record. Navigate to your PAM Record List location and select LDAP Server from the **Add Record** dropdown menu.
- For this new **LDAP Server** record, enter the URL to your LDAP server, the LDAP Administrator DN and this Administrator's Password. For example:
  - **LDAP URL:**ldap://dcuseast01:10389
  - **User:**uid=admin,ou=system
  - **Password:**Adm1nPass@word1

An Administrator account is required for this record because it will be used as a [Shadow Account](#) to reset the passwords of other non-Administrative user accounts.

Please note that this process assumes the password for users is stored in the directory attribute **userPassword**. If this is not the case in your directory, then you will need to [add a new field](#) to the LDAP Server content type with the following values:

Field Type: **String**

Name: **PasswordAttribute**

Display Name: **Password Attribute**


Then when creating this LDAP Server record, you should specify the name of your directory attribute that stores passwords in the PAM record's **PasswordAttribute** field.

- Click **Save and Return** when finished.

LDAP Server

Name	LDAP Server
Description	Admin account for <u>LDAP</u> password reset
Reference Record	Search reference record...

---

Type	LDAP Server
LDAP URL	ldap://dcuseast01:10389
User	uid=admin,ou=system
Password	..... 


---

Save Save and Return Cancel

- Navigate back to Administration > Record Types and click the **Edit** button next to the *LDAP User* record type.
- Within the *LDAP User* record type configuration, click the **Tasks** button.

Record Type: LDAP User

Found 2 fields.

Formula **Tasks** Commands Save Delete Cancel 

Name	<u>LDAP User</u>
Description	LDAP User

You can also customize the password complexity policy by clicking the **Formula** button on this page.

- Now we will make our LDAP Server record as the [Shadow Account](#) for this task. In the Shadow Account field, enter the name of the LDAP Server record that was created in a previous step.

By associating the LDAP Server record as a [Shadow Account](#) for the LDAP User record type, this configures PAM to use the User and Password for the Server to execute the Password Reset task for all the LDAP User records.

- Click **Save** when finished.

Tasks for LDAP User

Add Task

Save

Shadow Account

LDAP Server

LDAP Server (Admin account for LDAP password reset)

Script	Policy	Actions
Password Reset LDAP	On demand	...

- Return to your PAM Record List and create a new LDAP User record. This record will contain the user account whose password will be reset or automatically rotated.
- Enter the values in the LDAP User record as needed. For example:
  - User:**uid=chrisk,ou=users,o=xtam
  - Password:**usersPassword
- Click **Save and Return** when finished.

LDAP User

Go to Parent Execute...

Name

LDAP User

Description

User

uid=chrisk,ou=users,o=xtam

Password

\*\*\*\*\*

🔒

Record Type: LDAP User

Created By: xtamadmin @ 09/06/2018 11:30

Last Modified By: xtamadmin @ 09/06/2018 11:30

Job Queue: (click to refresh)

Audit Log

Change History

Job History

Formula

Permissions

Tasks

Workflows

Manage Edit 🔔 ☆

Go to Parent

Execute...

Password Reset LDAP

- When the record is saved, you may now configure the *Tasks* on this record for automatic password reset or you can manually execute the *Password Reset* task to reset it now.

LDAP User

Go to Parent Execute...

Name

LDAP User

Description

User

uid=chrisk,ou=users,o=xtam

Password

\*\*\*\*\*

🔒

Record Type: LDAP User

Created By: xtamadmin @ 09/06/2018 11:30

Last Modified By: xtamadmin @ 09/06/2018 11:30

Job Queue: (click to refresh)

Audit Log

Change History

Job History

Formula

Permissions

Tasks

Workflows

Manage Edit 🔔 ☆

Go to Parent

Execute...

Password Reset LDAP

This same configuration can be used to reset an Administrator’s account password with the exception that a [Shadow Account](#) is not needed because these accounts can reset passwords without requiring elevated permissions. You would only need to create and use the LDAP Server record to reset that Administrator's account password.



# Recreating Database Links after Password Rotation

To support the scenario where database links are used with automated password rotation, PAM needs to re-create these links after the password has been updated.

The following article describes how to configure PAM to enable this functionality.

OLTP and DWH are generic terms representative of the database schemas used in the creation of the link (CREATE DATABASE LINK).

## Concepts

1. A script that will reset the password in OLTP or DWH database schema and trigger another task to update the link in TARGET database.
2. A script that will update the database link based on the password on record.
3. A record for schema at OLTP database (similar one could be created for DWH or in other databases) with the script #1 to reset its password and trigger link update.
4. A record for a shadow account in the TARGET database (sysdba) to perform the link update for record #5. This shadow record might be reused for all DB links in TARGET.
5. A record for schema at the TARGET database describing the link parameters with the script to update DB Link from #2 run as a shadow account with permissions from #4. This record is a link-signal for a trigger indicating where to update the db link. (similar one could be created for DWH or in other databases).

## Configuration

Below are more details about the setup. Feel free to modify certain aspects like names, scripts, variables to match your environment.

1. A script that will reset the password in OLTP or DWH database schema and trigger another task to update the link in TARGET database.

Note that the script below will trigger the script called Oracle Update DB Link after password reset. If you will choose another name for that script, you will need to update the trigger too.

- Create a script named: **Oracle Password Reset with Trigger**
- Job Execution Strategy: **Oracle DB**
- SQL:

```
1 | alter user {{LOGIN}} identified by "{{NEWPWD}}"
2 |
3 | -- #XTAM TRIGGER REF Oracle Update DB Link
```

# Script

Home / Scripts / Oracle Password Reset with Trigger

## Script Oracle Password Reset with Trigger

SaveFactory DefaultCancel↺

Script Name

Oracle Password Reset with Trigger

Description

Job Execution Strategy

Oracle DB

Custom Code (SQL)

```
1 alter user {{LOGIN}} identified by "{{NEWPWD}}"
2 -- #XTAM TRIGGER REF Oracle Update DB Link
```

2. A script that will update the database link based on the password on record.

Note that the link name here is linksrc. You need to use your link name here.

- Create a script named: **Oracle Update DB Link**
- Job Execution Strategy: **Oracle DB**

- SQL:

```
1 | ALTER PUBLIC DATABASE LINK linksrc CONNECT TO {{LOGIN}} IDENTIFIED BY {{OLDPWD}}
```

Script

Home / Scripts / Oracle Update DB Link

Script Oracle Update DB Link

Save Factory Default Cancel ↻

Script Name: Oracle Update DB Link

Description: Recreate Dependent DB Link

Job Execution Strategy: Oracle DB

Custom Code (SQL):

```
1 | ALTER PUBLIC DATABASE LINK linksrc CONNECT TO {{LOGIN}} IDENTIFIED BY {{OLDPWD}}
```

Code Hash: 1dedecc15114728cb77ffdde0613fa22 ↻

3. A record for schema at OLTP database (similar one could be created for DWH or in other databases) with the script to reset its password and trigger link update.

Create a regular Oracle DB record and add the task **Oracle Password Reset with Trigger** from #1. You can add task to a record itself or create a special record type for such records. In our example we called it *Oracle Source for Oracle Link*.

Record View
Default Root / Databases / Oracle Source for Oracle Link

Oracle Source for Oracle Link
Go to Parent Execute...

NameOracle Source for Oracle Link
DescriptionOLTP Database

Connection Stringdev.xtontech.com:1521/orclxt.xt.com
Userlinksrc
Password\*\*\*\*\*

Record Type: Oracle  
ID: i+AyER9h4G  
Created By: Jack Baker (baker) /Local @ 10/09/2020 17:25  
Last Modified By: Jack Baker (baker) /Local @ 10/12/2020 15:26

Last Action: Execute @ 10/12/2020 15:26  
Last Success: Execute @ 10/12/2020 15:26  
Job Queue: (click to refresh)

Audit LogChange HistoryJob History

GrantManageEdit

Check Status Remote Oracle DB
Oracle Password Reset with Trigger
Password Reset Remote Oracle DB

4. A record for shadow account in TARGET database (sysdba) to perform link update for record #5. This shadow record might be reused for all DB links in TARGET.

Create a regular Oracle DB record describing SYS account in the TARGER database.

Note how we named a user here: **SYS as sysdba**. We named this record *Oracle Target Shadow for Oracle Link*.

© 2025 Imprivata, Inc. All Rights Reserved.

| 798

Record View

Default Root / Databases / Oracle Target Shadow for Oracle Link

Oracle Target Shadow for Oracle Link

Go to Parent Execute...

Name

Oracle Target Shadow for Oracle Link

Description

Connection String

dev.xtontech.com:1521/orclxt\_xt.com

User

sys as sysdba

Password

\*\*\*\*\*

Record Type: Oracle

ID: i-M90YNIAr

Created By: Jack Baker (baker) /Local @ 10/09/2020 17:33

Last Modified By: Jack Baker (baker) /Local @ 10/12/2020 14:51

Last Action: Execute @ 10/09/2020 17:33

Last Success: Execute @ 10/09/2020 17:33

Job Queue: (click to refresh)

Audit Log

Change History

Job History

Grant

Manage

Edit

5. A record for schema at TARGET database describing the link parameters with the script to update DB Link. (similar one could be created for DWH or in other databases).

Create a regular Oracle record for the target database. When creating this record use Reference record you created in #4. It will fill all parameters. For this record, Manage / Tasks and define Shadow record for sysdba you created in #4. Also, add *Oracle Update DB Link* script we created in #2. This is the record that links it all together.

We named this record *Oracle Target for Oracle Link*.

Below is the edit screen demonstrating how does it reference the Source record.

Record Edit

Default Root / Databases / Oracle Target for Oracle Link

Oracle Target for Oracle Link

Name

Oracle Target for Oracle Link

Description

TARGET Database

Reference Record

Oracle Source for Oracle Link

Type

Oracle

Connection String

dev.xtontech.com:1521/orclxt.xt.com

User

linksrc

Password

\*\*\*\*\*

Password is Strong.

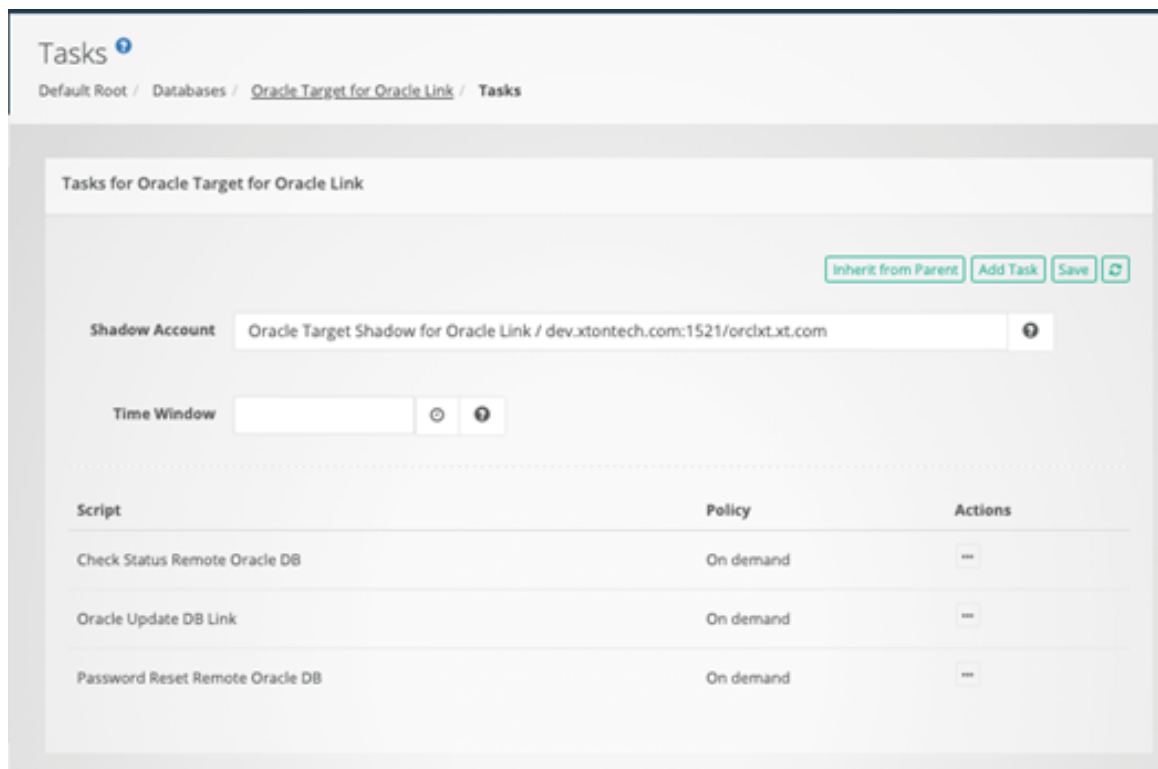
Save

Save and Return

Cancel

The screen shot below is the Manage / Task list definition for this record.

Notice [Shadow Account](#) and a task added.



## Operations

1. Execute *Oracle Password Reset with Trigger* script on the record *Oracle Source for Oracle Link* we have created in #3. This task could be run on demand or based on any other policy such as periodic or after certain event (like unlock).
2. After successful execution the job will schedule new *Oracle Update DB Link* task for the record *Oracle Target for Oracle Link* we created in #5.
3. The job *Oracle Update DB Link* will run to login as sysdba as a shadow account and update the password on the link because it is updated already after #a since target record references the source one and they have the same user / password on record.

## Generate Temporary AWS API Keys

Generate Temporary AWS API Keys for Privileged Users, Applications, Command Line and Automation.

PAM can generate AWS STS Temporary AWS API access keys (Access Key Id and Secret Key pair) for a specified duration based on the provided superuser access keys, those of which are stored safely in the PAM Identity Vault.

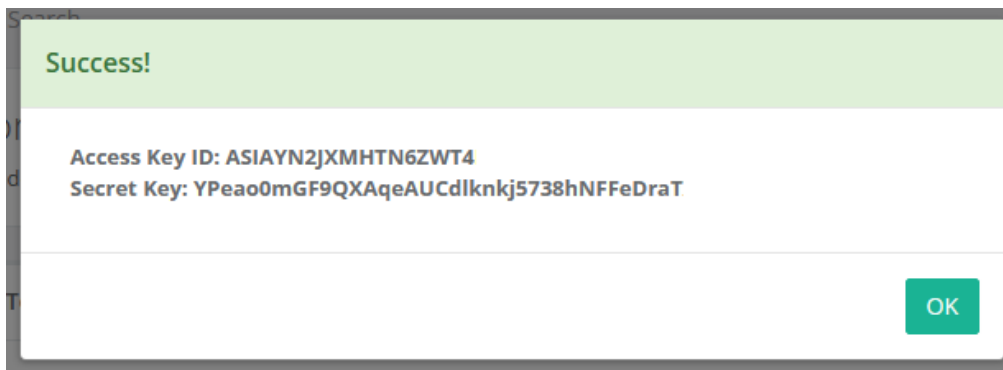
The option enables Just in Time access for users, applications, command line utilities and automation software to communicate with [Amazon Web Services](https://aws.amazon.com/) with least possible standing privileges.

### *Generate an AWS API Key Pair for Temporary Access*

1. First, we must enable the functionality, so login to PAM with a System Administrator account. A System Administrator account is only needed to enable the Record Type, not to manage or generate keys once it is configured.

2. Navigate to Administration > Record Types and locate the record type **AWS STS Temporary Access**. Click it **Edit** button, uncheck the *Hidden* option and click **Save**. This will unhide and make available to users' this record type. After this step, you will no longer need to use System Administrator access.
3. Navigate to *All Records* and into a container where you want to generate these temporary access keys. In this container, click the **New Record** option and select this type *AWS STS Temporary Access* from the drop-down menu.
4. Create the record as needed.
  - **Name:** Enter a recognizable name.
  - **Description:** Optionally, enter a description.
  - **Access Key ID:** Enter your superuser's AWS Access Key ID.
  - **Secret Key:** Enter your superuser's AWS Secret Key.
  - **Duration:** Optionally, define a length of time (in seconds) for which this key will be valid. The value must be between 900 and 129600 seconds.
5. Click **Save and Return** to create your record.

After the record is created, you can use the record's Execute > **AWS STS Temporary Ticket Generator** option to generate your on-demand temporary key pair.



When a temporary key pair is generated, a new event will be created in the *Audit Log*:

- **Time:** <when the key was generated>
- **User:** <who generated the key>
- **IP:** <the user's IP address at the time the key was generated>
- **Category:** Data
- **Level:** INFO
- **Event:** AWS STS Temporary
- **Message:** AWS STS Temporary Key Generated.
- **Region:** <region>, duration: <duration>

### *Additional Configuration Options*

PAM System Administrator may include extended options when enabling this record type through the use of additional fields.

The following fields, when added to this AWS STS Temporary Access record type, extends the functionality of this feature.

**Role ARN** field can be added to the record type to enable Assume Role option for temporary key generation.



When Role ARN is specified on the record, use out of the box AWS STS Assume Role task to generate temporary credentials with permissions restricted by the specified role.

- **Field Type:** String
- **Name:** RoleARN
- **Display Name:** Role ARN
- **Order:** 300

**STS Endpoint** can be added to the record type to overwrite the system default value of *sts.amazonaws.com*. Providing the ability for user's to enter another STS endpoint introduces support for multiple regions.

- **Field Type:** String
- **Name:** STSEndpoint
- **Display Name:** STS Endpoint
- **Order:** 400

**STS Region** can be added to the record type to overwrite the system default value of us-east-1 as the region.

- **Field Type:** String
- **Name:** STSRegion
- **Display Name:** STS Region
- **Order:** 500

You may also define these values globally in the PAM system configuration (`$PAM_HOME/web/conf/catalina.properties`).

Add these lines as needed, save the file and restart the **PamManagement/pammanager** service to complete the configuration:

```
1 | xtam.aws.sts.endpoint=<your STS endpoint>
2 | xtam.aws.sts.region=<your STS region>
```

## Job Execution Strategy Groovy

PAM Server includes a facility to run a script inside an PAM server itself, not even on the host OS it is deployed on (although this script might trigger an OS execution).

These scripts should be developed in the scripting language called [Groovy](#).

Groovy scripts work the same way whether PAM is deployed on Windows or on Linux OS.

Groovy scripts could be used to implement sophisticated password reset strategies for the WEB portals using REST API, custom devices.

They can also be used to automate system processes whether periodic ones or those based on PAM events such as session completion, password unlock or workflow execution for certain records or record types.

Groovy scripts are created in the [Script Library](#) as described in the following [guide](#).

A record type or a record task list can include the Groovy script as any other script in PAM. Check [Task Configuration guide](#).

System administrators can assign any task execution policies to a Groovy script such as scheduled periodic policies (once a month, etc), event-based policies (after session, etc) or manual on-demand policies.

Check [PAM policy guide](#).

## Groovy script specification

Groovy class in the job execution script should implement three functions.

1. The function **isReset** indicates whether the script resets password on record or it is just a script to automate something. Reset the password scripts generate a password based on the complexity formula. Reset password scripts also update records at the end of the successfully completed task execution workflow.
2. The function **execute** is called to execute the script. The function receives the following parameters in the argument array.
  - a. Record is the map of record attributes.
  - b. Shadow is the map of shadow record attributes.
  - c. Password is the new password to assign if applicable.
  - d. Parameters is the map of the parameters defined by the operator at the time of the scheduling of the task. This map also includes all record fields in using the key **RECORD.FieldName** as well as all fields of the shadow record using the key **SHADOW.FieldName**.
  - e. System logger for info, warn, debug and trace logs.

The function **execute** returns the value saved in the job execution details. When the function returns a value, the task is considered successful. When the function has thrown an exception, the task is considered to error.

1. The function **verify** is called to verify the results of the script execution. As an example, the function might be used to check the validity of newly reset password. The function receives the following parameters in the argument array.
  - a. Record is the map of record attributes.
  - b. Shadow is the map of shadow record attributes.
  - c. Password is the new password to assign if applicable.
  - d. System logger for info, warn, debug and trace logs.
4. The function **execute** returns the value saved in the job execution details. When the function returns a value, the task is considered successful. When the function thrown an exception, the task is considered to error. An example of an exception statement is given below

*throw new Exception ("Groovy script failure");*

When an exception is thrown the function stops its control flow. PAM catches the exception, saves it in job details and marks the job as **Error**.

## PAM job execution workflow

When job is scheduled based on policies (once a month), events (after session) or manually on-demand, PAM goes through several steps to process this job.

- **generate** – generates new password based on the record complexity formula if this is reset job.
- **reset** – executes the script (*calls Groovy execute*).
- **verify** – verifies the results of the script execution (checks the password, for example) – this part *calls Groovy.verify*

- **update** – updates a record with the newly generated, executed and verified password.
- **trigger** – optionally triggers dependencies such as update related services or fallbacks.
- **complete** – completes the job with either completed or error state.

As a result, the job could be on one of the following states that are displayed on the Job History report for a record or system one.

- **Scheduled** – the job is scheduled.
- **Generated** – PAM generates a password for the job. On-demand job when user provides a password land in this status in the job queue right away.
- **Executed** – script is executed.
- **Verified** – script is verified.
- **Updated** – record is updated with the new password (if this is isReset job).
- **Error** – job failed.
- **Completed** – job completed successfully.
- **Cancelled** – job is cancelled in the job history report.

### *Methods of the record and shadow record objects*

Record and shadow record objects passed to execute or verify functions have the following methods that access record attributes:

```

getCert()
getCheckStatusSelf()
getCommandPassword()
getCommandUser()
getConnectionString()
getEnabledSSL()
getHost()
getHostNameDNS()
getIntPort()
getPassword()
getPasswordAttribute()
getPasswordSu()
getPort()
getPrologue()
getReconcilePassword()
getReconcilePasswordSU()
getReconcileUser()
getReconcileUserSU()
getService()
getServicePort()

```

```
getUser()
getUserSu()
```

### *Script access to record and shadow record custom field values*

In addition to this, the script has access to all custom fields for a record or a shadow record through parameters argument.

In the example below we used a parameter called **RECORD:Host**.

In this case, the script developer can use any other out of the box or custom field instead of Host defined in a record to get its value in a script.

For shadow record the value would be **SHADOW:FieldName**.

```
1 | def String execute(final Object... args) {
2 |     def record = args[0];
3 |     def shadow = args[1];
4 |     def password = args[2];
5 |     def params = args[3];
6 |     def logger = args[4];
7 |
8 |     def user = record.getUser();
9 |     return ("XTAM Success Execute: " + user + "
field: " + params.get("RECORD:Host"));
10| }
```

## Job Execution Strategy Interactive SSH

PAM Server includes the facility to run a screen-scraping script on the remote server using SSH protocol called Interactive SSH.

Instead of connecting to a remote server and running a remote command on this server, the Interactive SSH strategy waits for the server prompt and types something in return.

- Scripts for the Interactive SSH strategy contain multiple lines of expected prompt and resulting output that the strategy executes on the remote server.
- Interactive SSH strategy is useful to implement status check, password reset or other custom automation logic on the remote devices with limiting scripting capabilities such as network routers, old Unix operating systems or custom devices with limiting shell.
- Interactive SSH scripts are created in the **Script Library** as described in the following [guide](#).
- A record type or a record task list can include an Interactive SSH script like any other script in the system. Check [Task Configuration guide](#).
- System administrators can assign any task execution policies to an Interactive SSH script such as scheduled periodic policies (once a month, etc), event-based policies (after session, etc) or manual on-demand policies. Check [system policy guide](#).

### *Interactive SSH script specification*

Interactive SSH script contains multiple lines executed one after another one.

Each line is a pair or a triple of prompts separated with -> character in the following format

**EXPECTED-PROMPT->OUTPUT**

or

## EXPECTED-PROMPT->OUTPUT->ERROR-CONDITION

Below is the example of version check on the remote Cisco router

```
>->show version
```

```
>->exit
```

The script reads:

- open connection to the remote device;
- wait for > prompt from the device;
- type show version command;
- wait for > prompt from the device;
- type exit command that terminates the session.

PAM job execution engine will capture the output of the script and present it in the job execution report in the **Details** field of the selected job.

When the Interactive SSH job execution strategy does not receive the expected prompt, it will abandon script execution with an *Error* status if the prompt does not appear after the timeout.

## EXPECTED-PROMPT

**EXPECTED-PROMPT** is the prompt that the Interactive SSH strategy expects from the server to produce.

The EXPECTED-PROMPT could be a fixed string like in a Cisco example above or a regular expression started with the `\r` characters like in the example below.

The example waits for the `$` or `#` prompts from the server before executing `su` - a command with the switch user on the record.

```
\r[$#]->su - {{SYSUSR}}
```

EXPECTED-PROMPT can also include terminal escape character in the form of `\e` characters.

The script in the example waits for the yellow `#` prompt from the server before executing shell commands.

```
# \e[0m->ls -alp
```

```
# \e[0m->echo completed
```

```
# \e[0m->exit
```

## OUTPUT

OUTPUT is the string that the Interactive SSH strategy prints in response to the expected server prompt.

OUTPUT could be *any command*.

It can also include the following placeholders to represent the values in the record fields:

**{{LOGIN}}** - User on the record

**{{OLDPWD}}** - current Password on the record

**{{NEWPWD}}** - new password (generated or specified when running on-demand password reset)

**{{SYSUSR}}** - Switch User on the record

**{{SYSPWD}}** - Switch User Password on the record

**{{SHADOW\_LOGIN}}** - Shadow User

**{{SHADOW\_PASSWORD}}** - Shadow User Password

**{{RECORD:FieldName}}** - Values of custom fields on the record

**{{SHADOW:FieldName}}** - Values of custom fields on shadow record

**\$\$ {User-Defined-Value}** - the value specified by the operator executing the script on demand from the application GUI

## ERROR-CONDITION

**ERROR-CONDITION** is a comma separated list of prompts from the execution of the previous command that causes the Interactive SSH strategy to abandon script execution.

The error conditions are useful to capture failures of the password reset to communicate the error back to the Interactive SSH strategy.

### *Return Result*

Interactive SSH strategy captures the output from the remote device during the script execution, whites out the sensitive information such as passwords and stores the output in the **Details** of the job execution.

Interactive SSH strategy processes the script output to validate the job success.

Specifically, the script can use the following key sentences to communicate success or failure results back to the strategy so it will update logs and record with a new password accordingly.

**Password Change Successful** - Success

**Password Change Unsuccessful** - Error

**Failure to wait for the expected character** - Error

**Failure to execute sequence** - Error

**XTAM Success** - Success

**xtam passwd error code: 0** - Success

**ERROR** - Error

**command failed** - Error

## Privileged SSH Sessions:

Creating secure PAM SSH sessions with or without the use of Native Client Side Applications.

For far too long, IT departments gave the actual secrets (logins, passwords, ssh keys or passphrases) to administrators, developers or outside contractors that needed access to their business's privileged systems and endpoints.

These secrets were often shared via emails, Excel files, SharePoint lists or countless other methods which clearly opened a glaring hole in any corporate security policy.

Not to mention, how could these secrets ever been changed or updated without negatively impacting these users' workflows.

The downsides and security risks are obvious, but what other option is there?

### *Imprivata Privileged Access Management*

Meet Privileged Access Management (PAM).

With PAM you can easily allow administrators, developers and contractors to create secure, privileged and recorded sessions to remote endpoints using the SSH or SFTP protocol without providing the passwords, keys or passphrases.

And most importantly, this can be accomplished directly in their desktop or mobile web browser (with no additional requirements) or using their existing native desktop SSH clients like PuTTY, WinSCP, OpenSSH or SecureCRT.



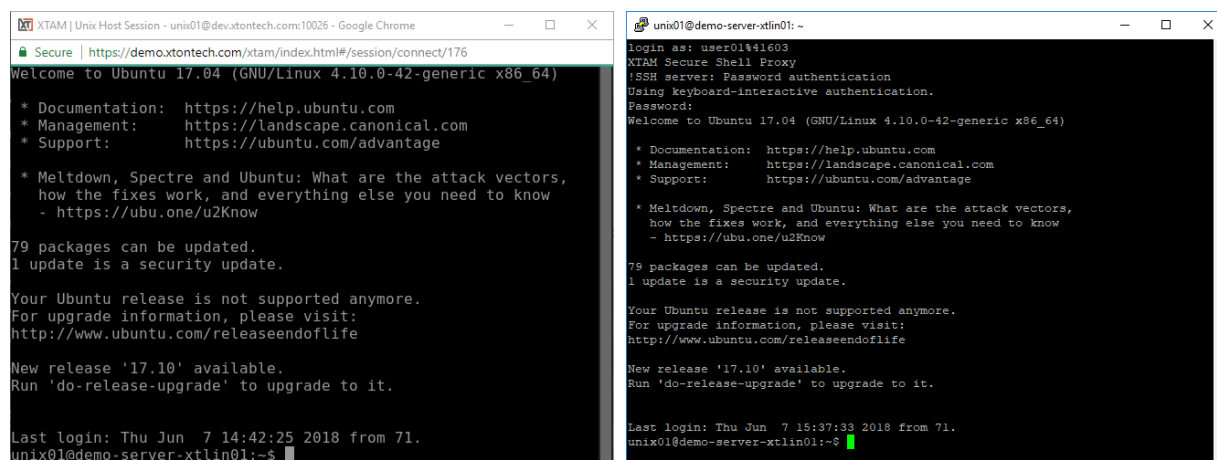
PAM secures your sensitive connection secrets in its Identity Vault, you share access to these secrets (but not the actual secrets themselves) with selected users and they simply *Connect to the endpoint*.

You decide who, where and when the access is granted and PAM will connect, audit and record their activity and even rotate the passwords as needed.

It doesn't get much easier or more secure than that!

PAM provides secure, privileged SSH access to your server and endpoints with the following methods:

- Directly in your [web browser](#) without the need of client side agents or applications.
- Natively using your own [client side applications](#) like PuTTY or SecureCRT.
- [Remote App](#) technology that provide a Jump Server like native application experience.



Secure PAM SSH session in your browser (left) and in a native desktop client like PuTTY (right)

## Use PAM

Use PAM instead of others Password Vaults or Session Brokers.

Others typically require heavy server installs and agents (or modified clients) in order to create such remote sessions, while others have limited support for remote protocols or don't offer password resets or rotation.

PAM creates a streamlined approach to:

- Establishing secure, “password-less” access to remote endpoints without agents
- Providing access to multiple endpoints with only the user’s personal login account
- Eliminating the use of shared accounts
- Allowing the continued use of common desktop SSH clients like [PuTTY](#)
- Auditing user activity during their connected sessions with reporting and notification options
- Recording keystrokes and file transfer operations
- Enforcing limited or time restricted user access via configured access request workflows
- Randomizing passwords as needed based on time or event based policies
- Providing users with access to privileged systems without disclosing the secrets to them
- Maintaining all endpoint details, secrets and information in a secure, 256-bit encrypted Vault

## *PAM Accomplishing*

How does PAM accomplish this?

PAM brokers the SSH connections through its Session Manager module in order to secure the login credentials, enforce the permissions and workflow requirements and overlay the auditing, recording and reporting functionality with the session.

To better explain how it works, let’s create a simple example scenario.

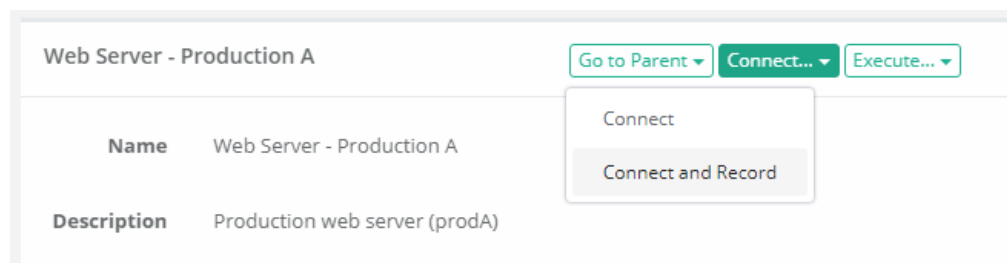
Bob, your outside contractor, needs to login to your Ubuntu web server to resolve an issue. You don’t feel comfortable providing Bob with login information (password, key or passphrase) and you don’t really have the time to “watch” over him, so you give him access to your web server in PAM and let it secure Bob’s activities.

Now all Bob has to do is securely login into PAM (optionally with MFA or 2FA) and find this shared web server record.

He opens the record and simply clicks the **Connect** button to open a remote session directly in his browser, no agents or clients required.

PAM establishes the connection using the details in the record, which Bob cannot see nor copy, and then hands control over to him.

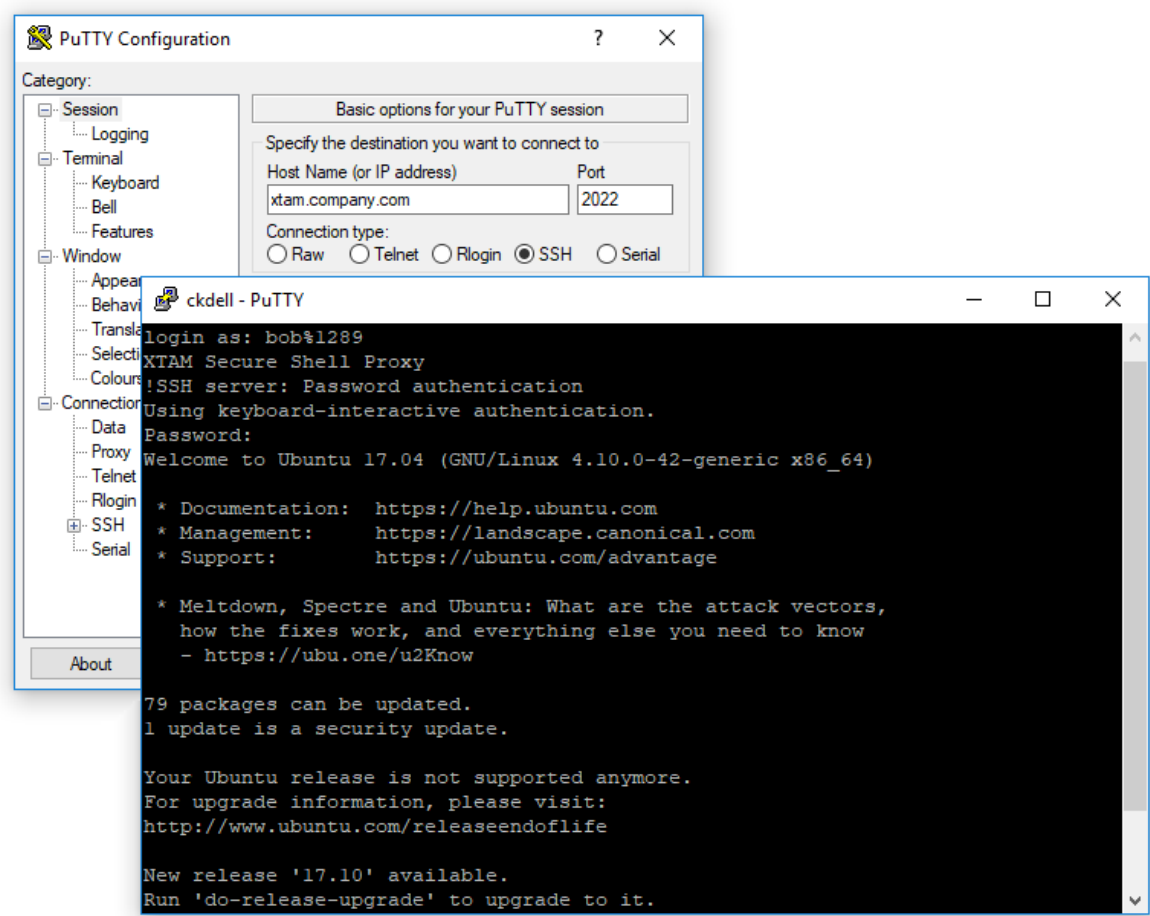
Bob works on the server to resolve the issue and when done he simply logs out all while PAM is monitoring and recording his activities in the background.



**Alternatively,** if Bob prefers to use his native PuTTY client he simply creates a session to PAM, specifying the web server’s record ID and his PAM login credentials, and PAM will broker the connection and create the remote session to the server directly in PuTTY.



So Bob can jump between his PuTTY session, use his familiar shortcuts and formatting, work on your web server all without him knowing the actual server secrets.



Record	User	Start Time	Completion Time	Status	Rating	Recording
Web Server - Production A	Bob Barker (bob)	06/07/2018 17:23:11		Active		Recording... <span>⋮</span>

Please review the following articles to further understand how to configure secure, remote SSH sessions in PAM.

[Create secure, password-less SSH sessions in your web browser](#)

[Create secure, password-less SSH sessions using native desktop clients like PuTTY, OpenSSH or SecureCRT](#)

## Workflows

PAM provides the ability to associate workflows to users to request control which requires approval before their request is enabled or their task can be executed.

When a user is bound by a workflow, instead of them having the ability to immediately perform a permissible action, they must request and receive approval before this action can be performed.

Workflows can also be used to restrict access based on time, days, IP addresses and other configuration options.

For more information and workflow examples, we encourage you to read our articles about [Workflow configuration and use](#).

## Components

To begin understanding Workflows, it is important to understand the various components that are used to construct, design, bind and use throughout the system.

- **Core Workflow** – The core workflow itself contains several building blocks
  - **Templates** - The workflow's template contains *the type of workflow*, *the steps* (who approves the request) and *the ranking of each principal* (how many approvals are required to advance the workflow to the next step). Templates can only be created, managed and deleted by System Administrators.
  - **Bindings** - The workflow's binding is the association between a template (the process) and its principal (who, what and when) that will require approval to perform an action. The binding contains of the associated template, the associated user or group that will be assigned the workflow and its configuration. Bindings can be applied globally by System Administrators or they can be applied to individual records (or multiple using inheritance) by those users with the required [object permissions](#).
  - **Instances** - A list of all active and completed workflows in the system. This includes who initiated the workflow, with which record, at what time and any additional details. The *Workflow Instance* page can also be used to terminate pending or previously approved requests.
- **Requester** - The requester is the user who initiates a workflow by requesting an action like **Connect**, **Unlock** or **Edit**. The requester is associated to a workflow by being listed as a User in the workflow's Binding.
- **Approver** - The approver is the user who approves or rejects a step in the workflow. Approvers are defined in the steps of the workflow's Template. If an Approver rejects a request at any step, then the workflow is immediately completed, and the requested access is not granted to the requester.
- **Status** - The status of the workflow displays the current step as well as previous approval or rejection comments. The status is visible only to the Requester, Auditors and System Administrators.
- **My Workflows** - The personal area of the system where Approvers will find workflows that require their approval and Requesters will find details of their active and historical requests.

# Managing Templates

To manage workflow templates, you must first login with your System Administrator account and then navigate to the Administration > Workflows > Templates tab.

## Create a New Template

To create a new workflow template, select the **Templates** tab on the Workflow page and then click the **Add** button.

Configure your workflow template as required.

Name	Enter a unique name for your template.
Type	Select from the available types: <ul style="list-style-type: none"><li>• <b>Automatic Approval</b> – the system will automatically approve the request. No human interaction required.</li><li>• <b>Interactive Approval</b> – requires user approval in the form of one or more approval steps.</li><li>• <b>Restrict Access</b> - creates a template that restricts access to options based on who and what is bound to the template. For example, this type would be used if you did not want users to Connect to a system after business hours.</li><li>• <b>Delegated Approval</b>- allows users to delegate their approval action to the system.</li></ul>
Step <i>n</i>	Defines the list of approvers per step. Each listed approver will be notified when there is a request pending their approval. <ul style="list-style-type: none"><li>• When using Groups as an approver, each member of the group will be notified of pending requests.</li><li>• Rank determines how many “approves” are required in total to advance the workflow to the next step.</li><li>• When the last step is fully approved, only then will the requester gain the needed approval to use their request operation.</li><li>• A requester may be included in their own approval template; however, they will not be permitted to approve their own request.</li><li>• To add additional steps, click the <b>Add Step</b> button.</li></ul>

Click the **Save** button when you are finished.

New templates are created in a *Draft* state which means they cannot be used in a binding until it is published. To publish your new template, open its Action menu and select the **Publish** option.

## Edit a Template

To edit an existing template, navigate to the Administration > Workflows > Templates tab, locate your template from the list, open its Action menu and select the **Edit** option.

Make the required updates to your template and then click the **Save** button.

Edited templates are automatically returned to the *Draft* state and must be *Published* before they can be used in new bindings.

To publish your updated template, open its Action menu and select the **Publish** option.

NOTE: Edits made to templates will be reflected only in new workflow instances. Existing workflow instances will retain the configuration of their templates at the time it was initiated by the requester.

## Delete a Template

To delete an existing template, navigate to the Administration > Workflows > Templates tab, locate your template from the list, open its Action menu and select the **Delete** option.

You cannot delete a template that is currently being used in any binding.

# Manage Bindings

To manage workflow bindings, you must be able to access the Manage > Workflows options which requires Owner or System Administrator permissions.

## Create a New Binding

To create a binding, you must decide on which objects you wish to restrict.

Workflow bindings take advantage of container inheritance, so if you apply your binding to the All Records or Root Folder for example, then it will inherit down to every object in your system’s vault (which inherits from its parent).

This may, or may not, be the desired goal so consider which object(s) you want to apply workflows to first.

1. When you decided on the object to apply the workflow, select its Manage > **Workflows** option.
- For containers, first navigate inside this container and then select the Manage > **Workflows** option from the options along the top.
- For records, first view or open the record and then select the Manage > **Workflows** option.

NOTE: Bindings created in the Administration > Workflows > Bindings tab will be applied to the All Records or Root Folder container. Only System Administrators can create and manage bindings applied to the All Records or Root Folder container.

2. On this *Workflow Bindings* page, click the **Add** button to create a new binding.
3. Configure your binding as required by populating all the necessary options.

Workflow Template	Select the published template to be used from the dropdown list. Note that only Published templates will be available for selection.
Workflow Design	Displays a read-only view of the selected workflow template.
Assign to All Users	Check this box to apply this binding to all users. Checking this option will disable the <i>Users</i> parameter. Pay special attention to assigning a workflow to an administrative action for all users of the system because it will limit the ability to perform administrative functions without approval.
Users	Add your principals (users or groups) to whom the binding will be applied. Binded users will require approval to utilize defined actions during the configured time periods.
IP Filter	<p>Enter an IP address(es) that act as a filter for the binding. IP Filter is a comma separated list of IP addresses (i.e. 10.0.0.12) or IP addresses with IP mask (i.e. 10.0.0.0/24) optionally preceded by a minus sign to indicate that the binding will apply to IP addresses outside of the specified range.</p> <p>For example, if you want the binding to only be applied to a user that comes from an IP address, then enter that address in the filter.</p>

Actions	<p>Select which Actions will require approval for the bound users.</p> <ul style="list-style-type: none"> <li>• <b>Administration</b> – Requires the user to have approved access before they can make Administrative changes to the system. For a list of Administration actions, please see our <a href="#">Workflow Binding</a> article.</li> <li>• <b>Record Control</b> – Requires the user to have approved access before they can Unlock or Edit the object.</li> <li>• <b>Connect Control</b> – Requires the user to have approved access before they can Connect to a session.</li> <li>• <b>Task Control</b> - Requires the user to have approved access before they can Execute an on-demand task.</li> </ul>
Time Selector	<p>A selected or checked Time Selector will mean that during this time period, the bound user will need to request access while an unchecked option will mean that the binding will be disabled, and the action will be available without requiring approval.</p> <p>Select which time selectors to apply to this binding.</p> <p>A selected or checked time selector means that the binded user will require approval when requested during this time period(s).</p> <p><b>CRON EXPRESSION HELP</b></p> <p>Examples of time execution window formats:</p> <p>* * <b>1-7 ? * SUN,SAT</b> * - between 1am and 7am, on every Sunday and Saturday</p> <p>* * <b>0,1,2,3,12,22,23 ? * MON,TUE,WED</b> * - during 0am, 1am, 2am, 3am, 12pm, 22pm and 23pm, on every Monday, Tuesday and Wednesday</p> <p>System Administrators can define the time, day or date values of each time selector in Administration &gt; Settings &gt; Parameters.</p>

Duration	<p>Setting a workflow binding's Duration value will allow a different template to be applied based on the length of time the requester submits.</p> <p>Duration is a threshold between applying two workflow templates. When the Duration is empty, it means any requested time period, but when you create a second near-identical binding with a duration defined, then it sets that cutoff.</p> <p>The duration is defined in minutes.</p> <p>Duration triggers this request approval workflow for long requested access time.</p> <p>Note that binding with duration set requires default binding created to cover the cases for short requested durations. Otherwise the system will not apply workflow requirements for the designated actions considering that no default workflow means open access. This default binding without duration could be applied to all system users or assets, or only to those with the duration set. Default binding could be defined with auto-approval workflow which would mean that only long requests would require people approval. Default and several duration-based bindings combined allow users to select emergency workflow with different approval scenarios by requesting access for shorter time.</p> <p>Another use of duration-based bindings is to restrict disproportionately long requests by applying Restrict Access workflow for long durations while maintaining automatic or human-approved templates for shorted requests.</p>
Checkout	<p>The Checkout parameter enforces accountability on records by only permitting a single user (the approved requester) to access the record actions while in the checked-out state.</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b> – The record will not be Checked Out. The option will be set to not Check Out the record and the requester cannot change this setting.</li> <li>• <b>Optional</b> – The requester will decide to Check Out the record or not when making the access request.</li> <li>• <b>Required</b> – The record will be forced to Checked Out. The option will be automatically set to Check Out the record and the requester cannot change this setting.</li> </ul> <p>The system will not perform the operation for any user with the exception of the one who checked out the record.</p>
MFA	<p>The MFA parameter enables the enforcement of MFA when the user attempts to use their approved action.</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b> – MFA will not be required.</li> <li>• <b>Required</b> – The user will be required to use MFA when the approved action is initiated.</li> </ul> <p>Currently the option supports TOTP, Duo Security OTP and Radius MFA for Unlock and Connect actions.</p>

Behavior Profile	Applies the selected <a href="#">Behavior Profile</a> to the configured binding.
Ticket Types	<p>Select which ticket types to apply to this binding.</p> <p>Ticket types are a comma-separated list of ticketing systems to provide related ticket information from when submitting access request governed by this binding.</p> <p>Precede a ticket type in the list with the asterisk character to indicate that the ticket number for this type is mandatory required to request access.</p>
Weight	<p>This value determines which workflow will be initiated when the same user(s) and time restriction(s) are enabled.</p> <p>A binding with a lower order will be applied rather than an equivalent binding of a higher value.</p>

4. Click the **Save** button to save your binding.

#### Edit a Binding

To edit a binding, navigate to the Manage > Workflows page on the object where the binding exists, open the Actions menu and select the **Edit** option.

Make the desired updates and click the **Save** to complete the editing process.

#### Delete a Binding

To delete a binding, navigate to the Manage > Workflows page on the object where the binding exists, open the Actions menu and select the **Delete** option.

Confirm your binding delete operation to complete its removal.



# Check Instance Status

The status and details of workflow instances can be reviewed in the system by various users.

## Requester

A requestor may check the current status of their requests by one of two methods:

1. Navigate to the Management > My Workflows > **My Requests** tab. Locate the request in the list, open the Actions menu and select the **Details** option. The Workflow Instance page will display the current status and other relevant details about their request.
2. On the object where your request was submitted. The original *Request* button is now displayed as *Requested*, clicking this **Requested** button will open the Workflow Instance page displaying the current status and other relevant details about their request.

## Auditor

An account with the Auditor [global role](#) may review, but not take any actions against, Workflow Instances by opening the **Requests** report in the Reports section of the menu. In this report, this Auditor will be able to review all Pending, Active and Completed workflow requests and use the **Details** option to view information about a specific request.

The **Sessions** option in this same Actions menu and on the *Details* page will generate a report of all remote sessions, if any, that were established during the time of this workflow instance.

## System Administrator

An account with the System Administrator [global role](#) may review and take actions against Workflow Instances by opening the **Requests** report in the Reports section of the menu.

In this report, this System Administrator will be able to review all Pending, Active and Completed workflow requests and use the **Details** option to view information about a specific request.

The **Sessions** option in this same Actions menu and on the *Details* page will generate a report of all remote sessions, if any, that were established during the time of this workflow instance.

# Terminate Requests Before Approval

A submitted request can be terminated or cancelled before it is approved by either the Requestor or a System Administrator.

## Requestor

A requestor may terminate their own submitted request before its approval by navigating to the Management > My Workflows > My Requests tab.

Locate the request you would like to terminate, open its Action menu and select the **Terminate** option.

Provide a reason why you are terminating your request and finally click **Reject** to complete the process.

## System Administrator

A System Administrator may terminate a submitted request of another user by navigating to the Reports > Requests report.

Locate the request you would like to terminate, open its Action menu and select the **Details** option.

On the Details page, confirm this is the request that you wish to terminate and then click the **Terminate** button.

Provide a reason why you are terminating the request and finally click **Reject** to complete the process.

# Terminate Requests After Approval

A request can be terminated or cancelled after it is approved by either the Requestor, Approvers or a System Administrator.

## Requestor

A requestor may terminate their own approved request by navigating to the Management > My Workflows > My Requests tab.

Locate the request you would like to terminate, open its Action menu and select the **Terminate** option.

Provide a reason why you are terminating your request and finally click **Reject** to complete the process.

## Approver

An approver may terminate an approver request of another user (even if they did not originally approve it) by navigating to the Management > My Workflows > My Requests tab.

Locate the request you would like to terminate, open its Action menu and select the **Terminate** option.

Provide a reason why you are terminating the user's request and finally click **Reject** to complete the process.

## System Administrator

A System Administrator may terminate a submitted request of another user by navigating to the Reports > Requests report.

Locate the request you would like to terminate, open its Action menu and select the **Details** option.

On the Details page, confirm this is the request that you wish to terminate and then click the **Terminate** button.

Provide a reason why you are terminating the request and finally click **Reject** to complete the process.

# Approve or Reject Requests

A user who is included in the Workflow Template as an approver, whether individually or as a group member, will receive a notification when there is a request pending their approval.

For multi-step approval templates, approvers will only be notified when the workflow instance reaches their step, i.e. Step 2 approvers will not be notified until the workflow advances to past Step 1, if it ever does.

## Interactive Approval

To approve or reject a request, navigate to the Management > My Workflows > Requests for Approval tab.

This page will display all requests that are pending your approval.

For the request, open its Actions menu and select either **Approve** or **Reject** from the menu.

Be careful with either selection as once you submit your decision, it cannot be rescinded.

- If you decide to *Approve* the request, you will simply need to click **OK** on the confirmation dialog box to submit your approval.
- If you decide to *Reject* the request, you will be required to submit a reason for the rejection and then you may click the **Reject** button to submit your rejection.

## Email Approval

NOTE: A single Reject decision from any step of the approval process will cause the workflow instance to be rejected entirely.

To approve or reject a request with an email response, once you receive the email notification regarding the Requestor’s request, simply reply to this same email with one of the following case insensitive words in the first line of the email body:

To <b><u>Approve</u></b> the Access Request	To <b><u>Reject</u></b> the Access Request
Yes	No
Approve	Reject
Approved	Rejected
Ok	{Anything other than the listed <i>Approve</i> words will also reject the request}

### Notes about the Access Request Email Approval Response:

- This Email Approval feature has to be enabled in PAM. Please talk to your PAM System Administrator to determine if this feature is available for use.
- Approvers can use standard desktop email clients or mobile email apps and respond to the approval request email by sending a reply with the above words, without requiring the Approver to first login to PAM.

- The Approver must reply using the same email address that received the email approval request.
- All words contained in the first line of the email body may be included in the Reason field for the Approval or Rejection action.
- Any words contained in the first line of the email body that are not one of the above Approval words will be detected as a Rejection response.
- Periods or other punctuation marks are allowed at the end of the word.

After your decision is submitted, the request will be removed from your **Request for Approval** page for this step.

If this is a multi-step workflow template and you are an Approver in a future step of this same request, you may receive an additional notification and this request may be required again, pending your approval.

NOTE: If you are included as an Approver on a template for your own submitted request, your request will not appear in your Request for Approval queue. A requestor cannot Approve or Reject their own request.

# Getting Started with Workflows

This guide is designed for PAM System Administrators to learn about Workflows and will meet the following goals.

To complete the guide be sure that you have access to a System Administrator account (used for Design and Approval) and a non-Admin user account (*used for Requesting*).

- [1. Design a new workflow](#)
- [2. Request an action \(initiate the workflow\)](#)
- [3. Review the workflow request](#)
- [4. Approve the request](#)
- [5. Gain access to the requested action](#)

## Stage 1: Design an Approval Workflow

1. Login to PAM as a System Administrator and navigate to Administrator > Workflows.
2. In the *Templates* tab, click the Add button. The workflow template configures the steps required to progress the workflow through the approval process.
3. Enter **My First Workflow** into the *Name* field.
4. Select the Type *Interactive Approval*.
5. Next to Step 1, click the **Add** button.
6. When the *Add Approver* dialog appears, enter your current System Administrator account into the Principal field and click **Add**. This account will be used to Approve the request workflow.
7. For the Rank value, leave the default 1 and click **Select**. Rank determines the total number of approvals in order to advance the workflow steps. For this walk-through, we will only designate one approver so their sole approval will advance the workflow to the Approved state.

My First Workflow

SaveCancelAdd Step↺

Name

My First Workflow

Type

Interactive Approval

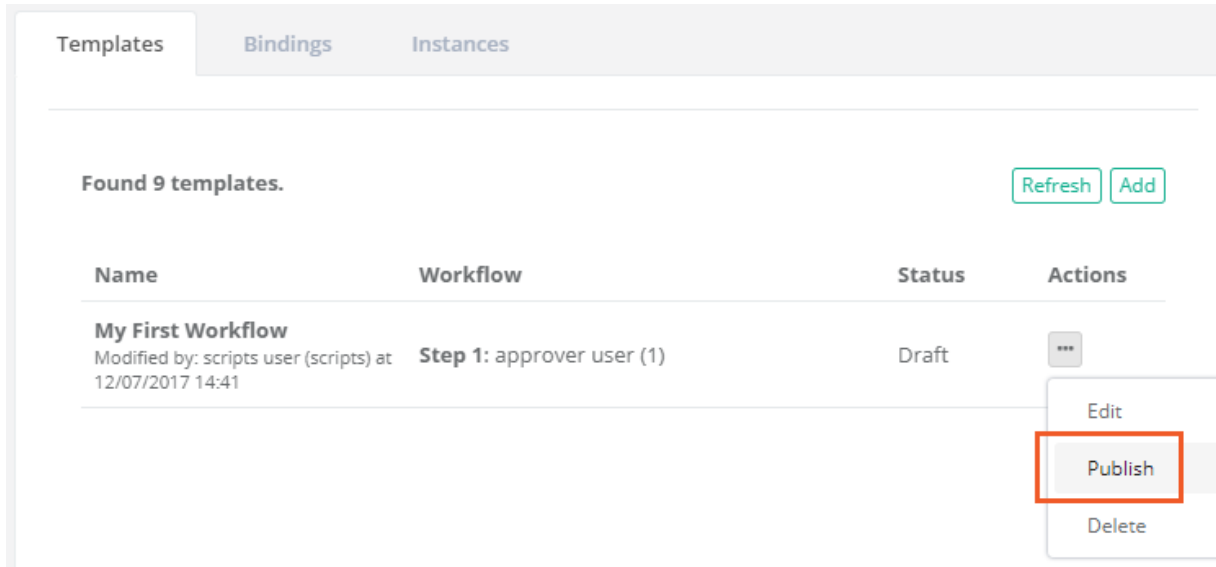
Step 1

Add

approver approver /Local (1) ▾

8. Our template is now complete. We have created a simple one step workflow whose sole approver is your System Administrator account. Click **Save** to continue and then return back to the Workflows section using the navigation breadcrumbs.

9. Back in the Templates section, you will now see our workflow with the status *Draft*. Templates in the *Draft* state cannot be used in an active Workflow, so we must Publish it to continue. Open the Actions menu for our workflow and select the option **Publish**.



10. Confirm the *Publish* operation by clicking OK in the confirmation dialog. The Templates list will refresh and your workflow will now be in the state Published.
11. Switch to the *Bindings* tab and click the **Add** button. The workflow binding will associate our template to an action that will require approval from a designated user(s).
12. In the Template dropdown menu, select *My First Workflow* or the name you entered in step 3 above.
13. For the Users, click the **Add** button. In the Principal field, enter your non-Admin user account, click the **Add** button and then **Select**. You have just assigned this template to this user which means they will require approval.
14. For Actions, check the box next to **Connect Control**. This will assign the approval request to the Connect option in a record.
15. For Time Selectors, check all available options. This will ensure that for this walk-through, the workflow will be enabled regardless of your current system time.
16. For Order, leave the default value. Order defines workflow precedence if multiple templates are assigned to the same user. A lower order will take precedence over a higher order if both are applied to the same user with identical time selectors.
17. Click the **Save** button to complete the binding.

SaveCancelRefresh

Workflow Template ?

My First Workflow

Workflow Design

Step 1: approver approver /Local (1)

Assign to All Users ?

☐

Users ?

Add

user test (usertest) /Local

IP Filter ?

Actions ?

☐ Administration  
☐ Record Control  
☒ Connect Control  
☐ Task Control

Time Selector ?

☒ Work Hours  
☒ After Hours  
☒ Weekends  
☒ Holidays  

Cron Expression

🕒

Duration ?

Use ? hints for your clarification of each parameter.

Checkout ?

Disabled

MFA ?

Disabled

Ticket Types ?

Weight ?

100

18. Your workflow design is now complete.

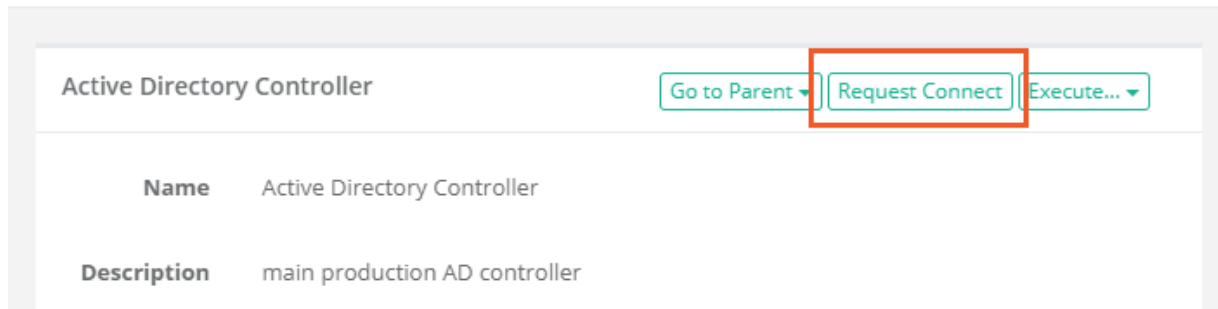


## Stage 2: Request an Action that requires Approval

1. Login to PAM with your non-Admin account. Locate any record that you have Connect permissions to and select the **Request Connect** option. Note that if the button says *Connect* rather than *Request Connect* then ensure you are logged in as the PAM user identified in our workflow binding.

### Record View

Home / Records List / **Active Directory Controller**



The screenshot shows the 'Record View' for 'Active Directory Controller'. At the top, there are three buttons: 'Go to Parent', 'Request Connect', and 'Execute...'. The 'Request Connect' button is highlighted with a red rectangular box. Below the buttons, there is a table with two rows: 'Name' with the value 'Active Directory Controller' and 'Description' with the value 'main production AD controller'.

2. Rather than launching the remote session, you will be presented with a Request Access dialog. In the *Reason* field, enter a brief reason for why you are requesting access to this Action. This reason will be sent to the Approver(s) for their consideration.

Note the Access Request form facilitates the adoption of request-based access to sensitive assets and allows users to submit access requests quickly and with fewer GUI interactions:

- a. users can select request *Reason* from the list of top 10 previously provided entries;
- b. the request *Reason* field auto-prompts a user to select one of the tops used reasons while the user types the new request reason;
- c. system administrators can change the default requested time using the system parameter *Default Requested Time*.

3. Next, select the checkbox option to choose between a time period as defined in Minutes or for one-time access for a future date and time range.
  - a. If you select minutes, enter any value greater than 0. The minutes will indicate the amount of time this Action is available to the user beginning from the time that the approval workflow is completed as **Approved**.
  - b. If you select the range, enter or select using the **Calendar** button, a *Requested From* value and a *Request To* value in the future. This will indicate the date range where this Action will be available to the user after the approval workflow is completed as *Approved*.
4. Click the **Request** button to submit the request.

## Request Access

### Reason ?

I need to apply security updates

### Requested Minutes ?

60

### ✓ Requested From ?

2017-12-09



12

00

### Requested To ?

2017-12-09



13

30

Cancel

Request

5. After the record refreshes, the **Request** Connect button will now change to **Connect Requested** indicating that it was submitted and the approval workflow has been initiated.
6. This user may click the **Connect Requested** button at any time during the approval process to see its current status or to *Terminate* or *Cancel* this active request.

## Record View

Home / Records List / **Active Directory Controller**

Active Directory Controller		Go to Parent ▾	<b>Connect Requested</b>	Execute... ▾
<b>Name</b>	Active Directory Controller			
<b>Description</b>	main production AD controller			

## Stage 3: Review the Workflow Request

1. Log out of PAM non-Admin account and back in as your PAM Admin account. Navigate to the **Reports** section and select the *Requests* report.

2. Your non-Admin user request will be listed. Included will be the *Request Time*, *Workflow Template Name*, *Action*, *Request Reason* and *Status* which is currently **Active**. You may click **Details** to see all the information related to this Action request.

Found 22 instances. Last Week Refresh

Show  entries Search:

Showing 1 to 22 of 22 entries

Time	Requester	Workflow	Action	Object	Reason	Status	Actions
12/07/2017 15:05:06	scripts user	My First Workflow	Connect:12/09/2017 12:00 - 12/09/2017 13:30	Active Directory Controller	I need to apply security updates	Active	<a href="#">Details</a>

3. You may also notice that your PAM Administrator account, which is the Approver in this walkthrough, has received an in-app notification and an email notification (if email was configured) alerting you to a request awaiting your approval.

## Stage 4: Approve the Request

1. Still logged in as PAM Administrator account (Approver), navigate to Management > My Workflows.
2. Select the tab *Requests for Approval*.
3. The submitted request from Stage 2 should be listed. Under its Actions menu, select the option **Approve**.
  - a. We will Approve this request in this walk-through, but please do later test this same process using the Reject option. Any single Reject in an Approval Workflow will immediately deny the requester's request.

My Requests **Requests for Approval**

Found 1 requests. Refresh

Requester	Requested Time	Request	Step	Object	Reason	Actions
scripts user (scripts)	12/07/2017 15:05	Connect : 12/09/2017 12:00 - 12/09/2017 13:30	1	Active Directory Controller	I need to apply security updates	<div><div>...</div><div>Approve</div><div>Reject</div></div>

4. Once approved, click the **OK** button on the confirmation dialog box.
5. The request has been approved, you may now return to the Workflow Instances view (Administration > Workflows > Instances) to check the status. Since this was a single step approval with a sole Approver, the

workflow is now complete and its status is listed as Approved.

Found 22 instances. Last Week Refresh

Show 50 entries Search:

Showing 1 to 22 of 22 entries

Time	Requester	Workflow	Action	Object	Reason	Status	Actions
12/07/2017 15:05:06	scripts user	My First Workflow	Connect:12/09/2017 12:00 - 12/09/2017 13:30	Active Directory Controller	I need to apply security updates	Approved	<span>Details</span>

## Stage 5: Gain Access to the Approved Action

- Now that the request has been approved, let's log out of your PAM System Administration (Approver) account and log back in with our non-Admin (Requester) account.
- Navigate back to the *Record* where the request was made. The **Connect** button will now be in the one of the following states:

- If the request was made using the minutes option, then the **Connect** button will now have the Connect options available and this user will be able to start a new remote session for the amount of time requested.

Active Directory Controller

Go to Parent Connect... Execute...

- If the request was made using the date range option and the current time is within this range, then the **Connect** button will now have the Connect options available and this user will be able to start a new remote session during this time period.

Active Directory Controller

Go to Parent Connect... Execute...

- If the request was made using the date range option and the current time is not within this range, then the Connect button will continue to display the **Request Connect** option. When the Requested From (start time) time arrives, the record's Connect button will become active for this time period. Otherwise, this user is able to make an additional request for this action again.

Active Directory Controller

Go to Parent Request Connect Execute...

- At anytime, this user may navigate to Management > My Workflows and use the *My Requests* tab to view all their past, present and future requests. This is a good location to remind yourself of when your Action

will become available for future date range requests.

My Requests		Requests for Approval				
Found 23 requests.						<button>Refresh</button>
Object	Requested Time	Request	Reason	Approvers	Status	Actions
Active Directory Controller	12/07/2017 15:05	Connect : 12/09/2017 12:00 - 12/09/2017 13:30	I need to apply security updates	approver user:Approved	Approved	...

This completes the Approval Workflow walkthrough.

For additional workflow topics and how-to guides, return to the [Approval Workflow](#) main page and use the topics listed at the bottom to navigate the available articles.

## Designing Workflow Templates

When constructing your Workflows, it is crucial that you understand Workflow Templates so that you can build an effective approval process.

In this article, the following terms will be used.

- **Template:** The template is the component of the Approval Workflow that defines which approver(s) must approve or reject the access request.
- **Requester:** The principal that initiates the access request to an object or action.
- **Approver(s):** The principal(s) that are designated in the template who either approve or reject the access request.
- **Rank:** The total number of approvals required to advance the workflow to the next step.
- **Step(s):** The steps required to be completed before the access request is granted.

The first step in constructing any successful workflow is designing a well thought out plan.

Ask yourself, when a user makes a certain request, who should be responsible for its approval and how should this approval process flow?

Let's begin by designing a common approval workflow example.

*Our scenario is a member of our IT department, John, needs to access the Active Directory Domain Controller at 10AM on a Saturday morning.*

This is not business hours, so needing to access this privileged system during this time period is quite uncommon.

For this reason John requests access and the workflow process begins.

For our design, this scenario will require that John receives approval from both of his immediate Supervisors, Bill and Linda, that way they know that he needs access and they can further question his need if applicable.

Furthermore, because this is deemed a highly privileged system and the request is happening outside of normal operating business hours, our CIO, Daryl, will also need to consent.

In the end, this means that John will need approval from both Bill and Linda and then Daryl before his access to the AD controller is granted.

## Template Planning

Now that we have the plan, let's get started constructing our template.

1. Workflow templates can be globally created meaning they will be available for use with any workflow binding or they can be created in a vault where they can only be used with workflow bindings in this specific vault.
  - If you wish to create a global workflow template, login to PAM as a System Administrator and navigate to Administration > Workflows > Templates.
  - If you wish to create a vault workflow template, login to PAM with an account that has Record Control: Owner permission to the vault and in this vault navigate to Manage > Workflows > Templates.
2. Click the **Add** button to create a new Template.
3. Enter a unique **Name** for this Template. Later on, we will use this Template with a Binding referencing this name so make sure you enter something recognizable like *Highly Privileged Off Hours Approval*.
4. Next to Step 1, click the **Add** button.

Highly Privileged Off Hours Approval

Refresh Save Cancel Add Step

Name Highly Privileged Off Hours Approval

Step 1 Add

5. When the Add Approver dialog appears, we are going to enter the account name of John's first supervisor, Bill, and click **Add**. Then we are going to add the account name of John's second supervisor, Linda, and again click Add. Both of John's supervisors should now be shown in the Selected Principals section of the dialog.
6. For **Rank**, enter the value 2. Rank 2 means that a total of two approvals will be needed in order to advance to the next step and since two principals are defined, both will be required.

### Add Approver

**Principal** ?

Add

**Selected Principals**

Bill Jones ▾
Linda Walls ▾

**Rank** ?

Cancel
Select

7. Click the **Select** button to complete the constructing of this step.
8. With Step 1 complete, click the **Add Step** button to add Step 2.

### Highly Privileged Off Hours Approval

Refresh
Save
Cancel
Add Step

**Name**

---

**Step 1**

Add
Bill Jones (2) ▾
Linda Walls (2) ▾

9. When Step 2 appears, click its **Add** button to begin the construction.
10. When the Add Approver dialog appears, we are going to enter the account name of John's CIO Daryl and click **Add**. Daryl's account should now be displayed in the Selected Principals section.
11. For Rank, we are going to enter a value of 1 because for Step 2, only one approval, Daryl's, will be required to advance the workflow.

### Add Approver

**Principal ?**

Add

**Selected Principals**

Daryl Basham ▼

**Rank ?**

Cancel
Select

12. Click the **Select** button to complete the constructing of this step.
13. Our Workflow Template is now constructed. Click the **Save** button to complete the template.

### Highly Privileged Off Hours Approval

Refresh
Save
Cancel
Add Step

**Name**

---

**Step 1**
Add

Bill Jones (2) ▼

Linda Walls (2) ▼

**Step 2**
Add

Daryl Basham (1) ▼

To summarize, this template consists of two steps.

**Step 1** requires the approval of two principals, both of which are defined by their accounts, before it advances to **Step 2** which requires only a single approval before it completes which ultimately means the access request is granted to the requester.

As with any approval workflow in PAM, this logic is based on the Approver(s) actually approving the request. If any Approver at any step decides to *Reject* the access request, then the workflow is completed and the Requestor's access request is denied.

At this time, the Requestor would need to create a new access request and its approval would then begin again at **Step 1**.



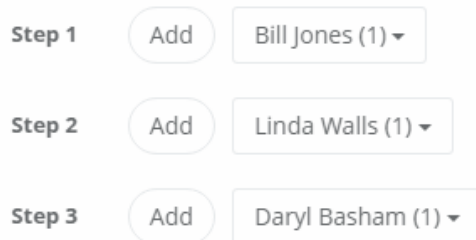
## Alternative Configurations

Here are a few alternative configurations and scenarios for our example workflow.

- **Chain of Command Approval:** If John's supervisor, Bill and Linda, do not share equal responsibilities, then you can separate them into additional steps.

**Step 1**, *Bill* (rank 1), **Step 2**, *Linda* (rank 1) and finally **Step 3**, *Daryl* (rank 1).

This will ensure that Bill is notified and approves first, then Linda is notified and approves before Daryl receives his notification and finally signs off on the request.

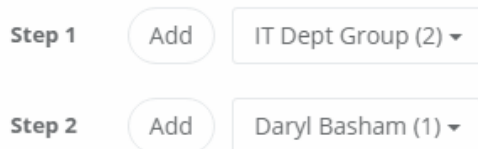


The diagram illustrates a three-step approval process. Step 1 includes an 'Add' button and a dropdown menu showing 'Bill Jones (1)'. Step 2 includes an 'Add' button and a dropdown menu showing 'Linda Walls (1)'. Step 3 includes an 'Add' button and a dropdown menu showing 'Daryl Basham (1)'. The steps are arranged vertically, indicating a sequential flow.

- **Group Approval:** If an IT department group exists, then rather than specifying specific users (Bill and Linda) the group's membership can be used.

**Step 1**, *IT Dept Group* (rank 2) and **Step 2**, *Daryl* (rank 1).

This creates the scenario where every user in the IT Dept Group will be notified of the request and any two members will need to approve before it advances to Daryl in **Step 2**.



The diagram illustrates a two-step approval process. Step 1 includes an 'Add' button and a dropdown menu showing 'IT Dept Group (2)'. Step 2 includes an 'Add' button and a dropdown menu showing 'Daryl Basham (1)'. The steps are arranged vertically, indicating a sequential flow.

Please note that if you incorporate Group's in your template steps, be careful that your ranking is not greater than the number of members in the group. For example, if your IT Dept Group has a rank of 5, but only three members exist than this step will not be able to advance since there are not five principals (group members) to approve. Due to the dynamic nature of Groups, if the group membership today is 5, tomorrow it may be 7 and next week it may be 4, ensuring the Rank never exceeds the total number of group members is key to a successful approval plan.

- **Group and Principal Approval:** This is a combination of both Groups used as Principals as well as specific users.

We want at least two members of the *IT Dept Group* (rank 3) to approve and we want Linda, who is not a member of this group, to be given the opportunity as well (rank 3).

This also constructs the scenario where Linda is "virtually" included in the IT Dept Group without having to actually include her in the group.

**Step 1**   Add   IT Dept Group (3) ▼   Linda Walls (3) ▼

**Step 2**   Add   Daryl Basham (1) ▼

- **Multiple Group Approval:** We could also use two or more Groups in a Step.

For example, we want two members of the *IT Dept Group* (rank 2) and three members of the *Security Dept Group* (rank 3).

This creates a priority status approval process where only two member of the IT Dept Group, three members of the Security Dept Group or a combination of both could be used to advance the Step (1 member of IT plus 1 member of Security would equal rank 2).

**Step 1**   Add   IT Dept Group (2) ▼   Security Dept Group (3) ▼

**Step 2**   Add   Daryl Basham (1) ▼

- **Emergency Approval:** This creates an “emergency” principal associated to one or multiple steps by assigning a rank 1 to their principal.

*IT Dept Group* (rank 2) plus *Linda* (rank 1) creates the situation where the IT Dept Group would approve with two approving members or Linda may advance the entire step herself by simply approving the request first.

This is particularly useful if the template is used for workflows during emergency off-peak times when it is more likely that many of the principals may not be available (overnight, weekends or holidays) to approve a step.

**Step 1**   Add   IT Dept Group (2) ▼   Linda Walls (1) ▼

**Step 2**   Add   Daryl Basham (1) ▼

As you can tell by just a few of these examples, the flexibility provided with multiple approvers, ranked approvers and multiple steps allows for the construction of a number of different templates that can be created to meet most approval requirements.

## IP Based Restrictions

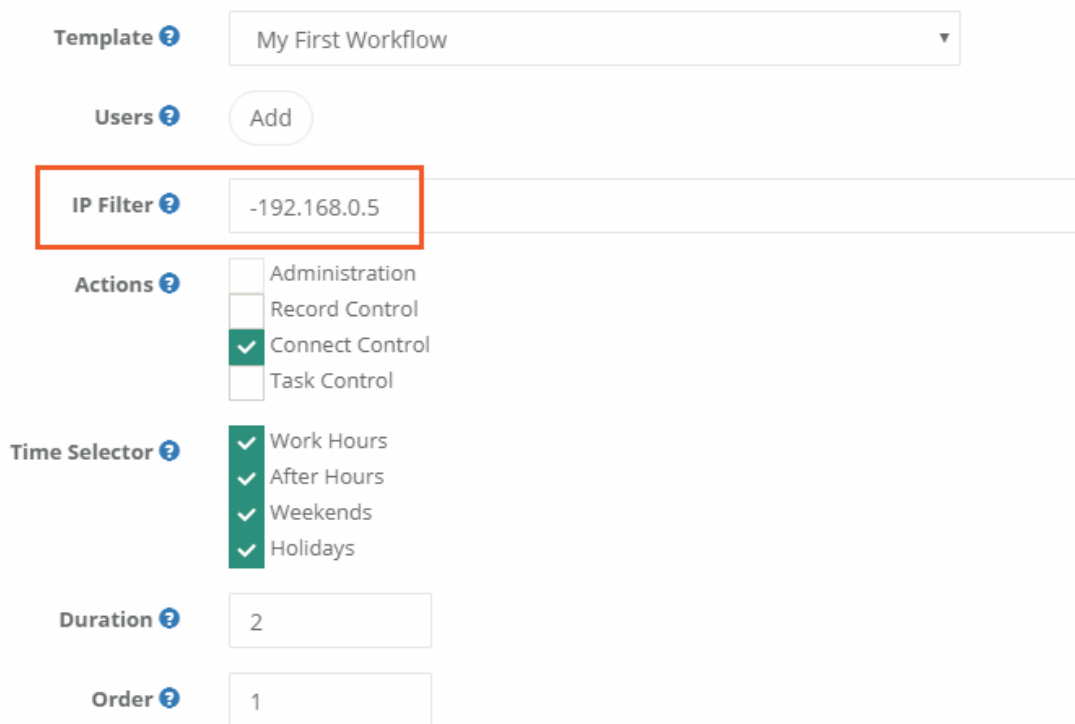
The use case is straight forward, I want to apply an Approval Workflow to an action when a user accesses PAM from within or outside a specific IP address.

When the user is at their work computer, they do not require approval however when they go home or work remotely, do require approval.

Using an **IP Filter** in your workflow binding you can accomplish this quite easily.

## Associate a Client IP

1. Login to PAM as a System Administrator.
2. Navigate to Workflow Bindings at Administration > Workflows > Bindings.
3. Select your existing Binding and click the **Edit** button in the Actions menu or click **Add** to create a new Binding.
4. Enter an *IP Address* or *IP Range* into the **IP Filter** field. *Configuration examples are shown at the bottom of this page.*
  - a. Example: An IP value of *192.168.0.5* would indicate that any user from this specific IP address would require approval.
  - b. Example: An IP value of *-192.168.0.5* would indicate that any user not from this specific IP address would require approval.
5. Optionally, you may also select a Principal(s) for the **Users** to work in combination with the IP Filter. If the Users parameter is left empty, it will apply to all PAM users satisfying the IP Filter requirement.
6. Click the **Save** button to complete the configuration.



Template ? My First Workflow

Users ? Add

IP Filter ? -192.168.0.5

Actions ?  
☐ Administration  
☐ Record Control  
☒ Connect Control  
☐ Task Control

Time Selector ?  
☒ Work Hours  
☒ After Hours  
☒ Weekends  
☒ Holidays

Duration ? 2

Order ? 1

## IP Filter Configuration Example Scenarios

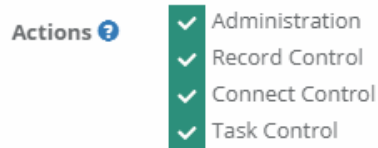
If you want to apply this workflow when a user accesses PAM:

- from a specific IP address then enter this: *192.168.0.5*
- from anywhere but a specific IP address then enter this: *-192.168.0.5*
- from an IP address using CIDR notation then enter this: *192.168.0.0/24*
- from any of these IP addresses then enter this: *192.168.0.5,192.168.0.6,10.0.0.88,70.54.48.786*
- from any of these IP addresses except one then enter this: *192.168.0.0/24,-192.168.0.6*

# Workflow Binding Actions

Binding Actions are used to determine which functions require approval for the listed user or groups before they may use them.

A selected or checked **Action** will mean that for this group of functions, the user will need to request access before it can be used while an unchecked option will mean that the action will be immediately available to this user without requiring approval.



## Available Binding Actions:

- **Administration:** Requires the user to have approved access before they can make Administrative changes to the PAM. This includes limiting access to the following functions:
  - Updating Global Permissions
  - Updating Global Roles
  - Export and Import Database Options
  - Updating Local User passwords
  - Adding users to Local Groups
  - Publishing Workflow Templates
  - Adding, Updating or Removing Workflow Bindings (globally configured)
  - Adding, Updating or Removing Permissions (vaults, folders and records)
  - Updating System Parameters
- **Record Control:** Requires the user to have approved access before they can **Unlock** or **Edit** this System record.
- **Connect Control:** Requires the user to have approved access before they can **Connect** to this System session.
- **Task Control:** Requires the user to have approved access before they can **Execute** this System task.

# Workflow Time Selectors

Time Selectors are used in workflow bindings to determine which time periods to restricts actions for the listed user or groups.

A selected or checked Time Selector will mean that during this time period, the user will need to request access while an unchecked option will mean that the request option will be disabled and the action will be immediately available without requiring approval.




**To configure the Time Selector ranges used in workflow bindings:**

1. Login to PAM as a System Administrator and navigate to Administration > Settings > Parameters.
2. The following parameters are available for configuration:
  - a. **Holidays:** Enter the days that PAM will use as reference for Holidays.  
Dates should be entered as M/D and multiple dates should be separated with a comma. For example, 1/15,10/5 represents January 15 and October 5.

<b>Holidays</b>	1/15,10/5		Save
-----------------	-----------	---	------

- b. **Weekend:** Enter the days PAM will use as reference for Weekends.  
Days should be entered as text and multiple days should be separated with a comma. For example, Saturday, Sunday.

<b>Weekend</b>	Sunday,Saturday		Save
----------------	-----------------	---	------

- c. **Work Hours:** Enter the time range(s) that PAM will use as reference for Work Hours (relative to PAM server time). Time range(s) outside of those specified will be used as reference for After Hours.  
For example, if 8:30-17:30 is entered (HH:MM-HH:MM), Work Hours is referenced as 8:30AM to 5:30PM whereas After Hours is referenced as 5:31PM to 8:29AM.

<b>Work Hours</b>	8:30-13,14-17:30		Save
-------------------	------------------	---	------

3. Click the **Save** button next to each individual parameter after it has been updated.  
The Time Selectors have now been updated and will be immediately used in new and existing bindings.

## Workflow Binding Duration

Setting a workflow binding's Duration value will allow a different template to be applied based on the length of the time the requester submits.

For example, if a user requests a short amount of time for access then it could be approved by a small group of approvers, perhaps just their immediate manager or supervisor or maybe it is auto-approved.

However, if a user requests a longer amount of time, say several hours or even days, then it should go through a more stringent review and approval process that may include additional managerial approval.

Let's now show you how to configure this workflow in PAM. Our scenario is simple, but should provide a base level so that you can customize it to your specific needs. We are going to apply a workflow binding to our IT member John.

When John needs to Connect to our production Unix server, he will need to first submit a request.

However, if John just needs to login really quickly to fix a production issue, we don't want him to sit around and wait for many people to approve it as time can become critical.

So, if John requests access to the server for less than 10 minutes, the request will be auto-approved.

Conversely, if John requests access for 10 or more minutes, then it will go through our normal, multi-tiered approval process and he will need to wait until it completes.

Before you begin, ensure that two [workflow templates](#) are already created. For our scenario, one will be auto-approved and the other will require at least two approvals in order to complete.

1. **Login** to PAM with a user who has *Owner* permissions to your record or is a *System Administrator*.
2. **Open** the record where this workflow will be applied and select *Manage > Workflows*.
3. If not already unique, click the **Make Unique** button. *For this scenario, we will make the record unique, but please note this is not required. You may apply this workflow configuration to a parent object and have it inherit to the child object(s) as well.*
4. Click the **Add** button to create a new workflow binding on this record.
5. **Configure** your workflow binding using the following as an example. This will be an example of applying the workflow template for an extended amount of requested time (10 or more minutes).
  - a. **Workflow Template:** Select your multi-step approval template. In our scenario this will be our *Production Server Approval* template.
  - b. **Users:** Apply the binding to a user(s) or group(s)
  - c. **IP Filter:** Leave empty
  - d. **Actions:** Enable at least one action. We will choose *Connect Control* for this example.
  - e. **Time Selectors:** Enable at least one action. We will choose *Work Hours* because we are doing this during business hours.
  - f. **Duration:** Enter a value of 10. Now when a user requests an extended period of time to this record (10 or more minutes), this binding and ultimately this template will be applied to their submitted request.
  - g. **Checkout:** Choose a value as required.

h. **Weight:** Choose a value as required.

SaveCancelRefresh

Workflow Template ?

Production Server Approval ▼

Users ?

Add

John Williams ▼

IP Filter ?

Actions ?

☐

Administration

☐

Record Control

☒

Connect Control

☐

Task Control

Time Selector ?

☒

Work Hours

☐

After Hours☐☐

Duration ?

10

Checkout ?

Required ▼

Weight ?

100

6. Click the **Save** button to complete your first binding.

Now we are going to create another workflow binding that will be applied when a user requests access for a brief amount of time (less than 10 minutes).

7. Click the **Add** button to create a new workflow binding on this record.

8. Configure your workflow binding exactly as you did in the previous steps with the exception of **Workflow Template** and **Duration**.

- Workflow Template:** Select your automatically approved template. In our scenario this will be our *Auto Approved* template.
- Duration:** Leave this empty. While this configuration *typically* means any requested time will have this template applied, in this scenario when the workflow engine evaluates this binding against our first (because they are identical to the user and access), it actually applies this binding and its

template for any requests less than 10 minutes.

SaveCancelRefresh

Workflow Template ?

Auto Approved ▼

Users ?

Add

John Williams ▼

IP Filter ?

Actions ?

☐ Administration

☐ Record Control

☒ Connect Control

☐ Task Control

Time Selector ?

☒ Work Hours

☐ After Hours

☐ Weekends

☐ Holidays

Duration ?

Checkout ?

Required ▼

Weight ?

100

9. Click the **Save** button to complete your second binding.

Return back to the record’s Workflow Bindings page (Manage > Workflows) and you should now see two bindings displayed, only differences being in the *Workflow Template* and *Duration* as shown in the screenshot below.

Workflow Bindings for Unix server

Found 2 bindings.

AddInherit from ParentBulk Actions ▼Refresh

	Workflow Template	Users	IP Filter	What	When	Duration	Checkout	Weight	Actions
<input type="checkbox"/>	Auto Approved	John Williams		Connect	Work Hours		Required	100	...
<input type="checkbox"/>	Production Server Approval	John Williams		Connect	Work Hours	10	Required	100	...

Now let’s test these bindings.



1. Login to PAM with the user account that has these bindings applied and navigate to this record.
2. Click on the **Request Connect** button to open the *Request Access* dialog.
  - a. In the Requested Minutes field, enter a value of **5**. Because this value is less than our Duration of 10, our first, *Auto Approved* template will be applied as shown in the Workflow Template field.
  - b. In the Requested Minutes field, enter a value of **120**. Because this value is greater than our Duration of 10, our second, *Production Server Approval* template will be applied as shown in the *Workflow Template* field.

The image displays two side-by-side screenshots of the 'Request Access' dialog box. Both screenshots show a 'Reason' field, a 'Requested Minutes' field, 'Requested From' and 'Requested To' date pickers, and a 'Checkout Required' checkbox. In the left screenshot, 'Requested Minutes' is 5 and 'Workflow Template' is 'Auto Approved'. In the right screenshot, 'Requested Minutes' is 120 and 'Workflow Template' is 'Production Server Approval'. Red boxes highlight the 'Requested Minutes' and 'Workflow Template' fields in both screenshots.

To summarize, think of **Duration** as setting that threshold between applying the two workflow templates. When the Duration is empty, it means any requested time period from one to a million minutes, but when you create that second near-identical binding with a duration defined, then it sets that cutoff. In our example, the first binding defines the threshold at 10 or more minutes and the second binding with an undefined (empty) duration covers the remaining possible times (less than 10).

If either of these requests are submitted, then the appropriate template would be applied and notification would be sent to the required *Approvers*.

Now that this concept is hopefully more clear, feel free to return to the bindings and modify them as needed to fulfill your business requirements.

[< Back to Request and Approval Workflows](#)

## Check Out Option

The Check Out feature enforces accountability on records by only permitting a single user to access the record while in the checked out state.

Combining the **Check Out** function with a password reset policy extends this feature to include a One Time Password scenario, where the password is automatically queued for rotation when the **Check In** action is executed.

The user who checks out the record will have the ability to use this object for the time that they have requested or they may checkin the record when they are complete.

Record Owners and System Administrators may force a checkin to immediately release the record in the case where emergency access is required or simply because the requester forgot or is unavailable.

This article will cover the following areas of interest:

- 1. [How to Configure the Check Out Feature](#)
- 2. [How to Configure Check Out with a Password Reset Policy to create One Time Passwords](#)
- 3. [The User Experience of the Check Out Feature \(checkout and checkin\)](#)

In this article, we will continue using the *My First Workflow* example that was created in our [Getting Started Guide: System Approval Workflows](#). If you have not already, review that guide to become familiar with PAM workflows or if you already have one in your System instance, you may use that instead.

## Configuring the Check Out Feature

How to configure the check out feature:

- 1. Login to the System as a System Administrator.
- 2. Navigate to Administration > Workflows > Bindings.
- 3. Locate the Binding that is associated to the template *My First Workflow* and choose its **Edit** option.

Templates

Bindings

Found 8 templates.

Add

Workflow Template	Users	IP Filter	What	When	Duration	Weight	
My First Workflow	scripts user		Connect	Work Hours, After Hours, Weekends, Holidays	5	1	<div><div>Edit</div><div>Delete</div></div>

- 4. On the Binding page, scroll down and locate the **Checkout** option. Select one of the following states:

Checkout ?

Disabled

Disabled

Optional

Required

- a. **Disabled:** The record will not be Checked Out. The option will be set to not Check Out the record and the requester cannot change this setting.
- b. **Optional:** The requester will decide whether or not to Check Out the record when making the access request.
- c. **Required:** The record will be Checked Out. The option will be set to Check Out the record and the requester cannot change this setting.

5. Click the **Save** button when complete.

This binding now has your selected Checkout state applied.

## Configuring Check Out with a Password Reset Policy

To configure check out with a password reset policy to create one time passwords:

1. Navigate to the record where you want to implement the One Time Password feature.
2. On this record, choose the Manage > Tasks option.
3. Select the Task Password Reset Remote Windows and choose Edit Policy in the Actions menu.

To learn more about how Tasks are configured, including with Record Type inheritance, please review this article [Task Configuration and Execution](#)

4. Locate and check the option **After Check-In**.

Task

---

[Save](#) [Cancel](#) [Refresh](#)

**Script**

Password Reset Remote Windows ▼

**Event**

---

☐ After creating or updating a record

---

☒ After Check-In

5. Click the **Save** button when complete.

Now whenever the record is Checked in, this Password Reset task will be automatically queued for rotation by the system.

You should also include the **After Expire** policy event. This will include the scenario where the user does not check in the record and instead the approved time period expires. After this expiration, the password reset policy will then be triggered.

## The User Experience of the Check Out Feature

Let's now walk through how a user interacts with the Check Out feature, including Check In.

1. Login to the System with the user account that is applied to this workflow binding.
2. Navigate to this record and click the **Request Connect** option.

- The Request Access dialog will appear. Fill out it as needed and take note of the Checkout option towards the bottom. Depending on how you configured the binding, it will appear in one of these states:

☐ Checkout ?

☒ Checkout ?

☒ Checkout ?

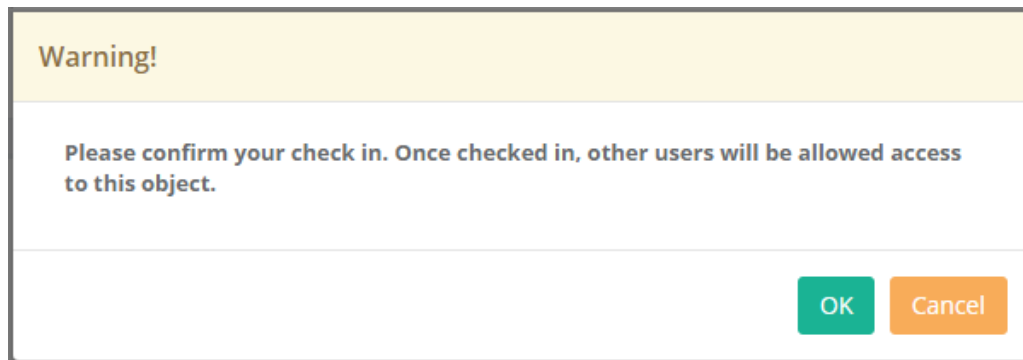
- Click the **Request** button to submit your request
- Using your *System Administrator* account, approve this user's request.
- Once approved, the record will be automatically checked out to this user now or when the requested time begins. Take note that the record now displays who it is Checked Out to and the time for when it will be automatically checked back in.

**Checked Out**

scripts user (scripts) / 03/01/2018 17:14

Checkin

- At this point, you may use this record until the requested time expires or click the **Checkin** button to complete the request immediately. Regardless of your option, once the record is checked in, you will need to request access again to continue working.



- Optionally, while the record is checked out, navigate to it with the System Administrator account to see how the record appears for other users. The action options, *Connect*, *Execute*, *Edit* and *Grant* are removed while checked out to another user; however the record Owner or System Administrator will have access to the **Checkin** button as well. At any time, they may override the check out and force the checkin of this record which will return the record to its default Checked In state and therefore would require this user to request access again.

To be clear, any users with at least *Viewer* will be able to see who the record is checked out to and when it will expire, but only record *Owners* or *System Administrators* will have the option to force the checkin on another user.

## MFA Requirements

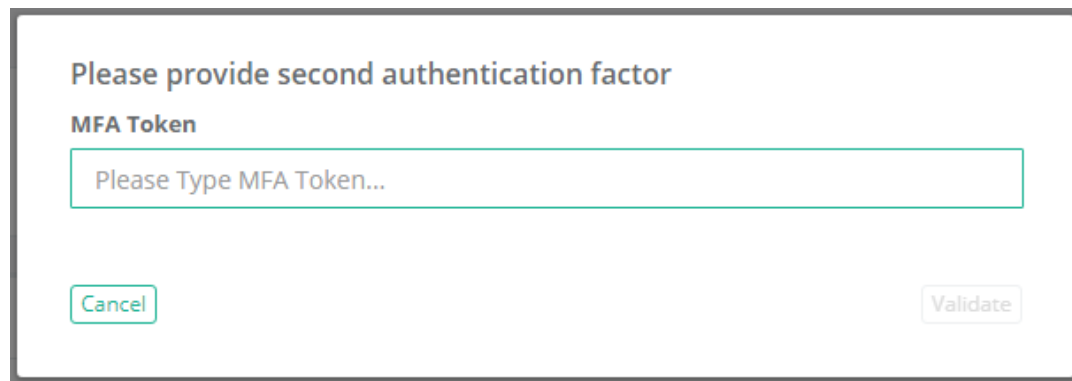
In addition to requiring user's to authenticate with a MFA provider like Duo, [Google](#) or MS Authenticator or other [TOTP providers](#), using Workflow Engine of PAM you can require a second MFA token before the same approved user can *Connect*, *Unlock*, *Edit* or *Execute Tasks* with Records.

To enable MFA enforcement with a Workflow Binding, create a new *Workflow Binding* or edit an existing one, locate the **MFA** parameter and select between the available choices:

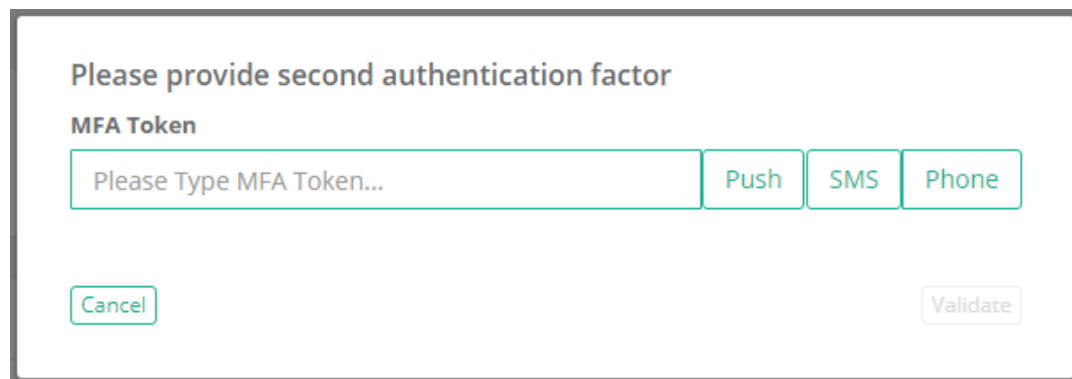
- **Disabled:** Select this option to not require MFA before the user may perform their approved action.
- **Required:** Select this option to require MFA before the user may perform their approved action.

**Save** your binding when you are finished.

When the approved user then attempts to perform this approved action, they will be presented with a MFA Token prompt like shown below. They must authenticate with their MFA provider in order to proceed.



A screenshot of a web interface for MFA authentication. The title is "Please provide second authentication factor". Below it is the label "MFA Token". There is a large text input field with the placeholder text "Please Type MFA Token...". At the bottom left is a "Cancel" button, and at the bottom right is a "Validate" button.



A screenshot of a web interface for MFA authentication, similar to the one above but with additional options. The title is "Please provide second authentication factor". Below it is the label "MFA Token". There is a large text input field with the placeholder text "Please Type MFA Token...". To the right of the input field are three buttons: "Push", "SMS", and "Phone". At the bottom left is a "Cancel" button, and at the bottom right is a "Validate" button.

## Request and Approval Workflows

PAM provides the ability to associate workflows to users to request control which requires the approval from others before their request is enabled or their task can be executed.

## Cases and scenarios

**The following use cases and scenarios are covered when workflows are used in PAM.**

1. **Dual Control or Four Eyes:** The concept of Dual Control (also known as Four Eyes or Peer Approval) is to prevent any one user from being able to access any system without the knowledge and consent of another. This type of secondary approval is often applied to Administrators themselves so that critical

systems require extra approval in order to access grant access, unlock passwords or even execute tasks.

- For example, a user should not be able to connect to the Active Directory Controller or unlock your Domain Admin password without the approval from the IT Manager or CSO.
2. **One-time Access:** This option provides a user the ability to request and to be approved one-time access for either a limited amount of time (60 minutes) or for a defined period of time (Saturday 6AM to Sunday 8PM). Once the time has expired, the user would need to once again request for that action.
    - For example, an outside contractor needs remote access to your internal server for maintenance or updates for the next 120 minutes or Thursday night after business hours.
  3. **Access Request:** This provides the ability for users to access records, but requires that they provide a reason for needing access to the remote system or secret. The Approval user or group then decides whether to approve or reject their request for an action.
    - For example, an internal IT department member needs to unlock the password for the web server, but this action should only be granted when the IT director's consent.
  4. **Emergency Access:** Emergency or off-peak workflows can be configured to notify and request approval from a different set of approvers than what is configured for on-peak or business hours. This ensures that emergency access to critical systems or tasks can be executed without having to wait until your business opens the following day or week.
    - For example, a critical service goes offline during the weekend or holiday and a user needs immediate access to resolve the situation.
  5. **Delegate Admin Roles to Object Management:** Configure workflow bindings and object permissions directly to container objects (vaults or folder) in order to delegate object management to a specific user or group without granting them access to the content of the container. By creating unique workflow bindings, the configuration, management or administering of these objects can be delegated to non-Administrators within Access Manager.
    - For example, a user can manage the permissions and workflows of the *Infrastructure* vault without being given access to the content within it.

## Approval Workflows

To further explain the Approval Workflows, it is important to understand their components.

1. **Workflow:** The workflow object itself can only be created, modified or deleted by system administrators and consists of the following core components:

- a. **Templates:** The workflow's template contains the type of workflow, the steps (who approves the request) and the ranking of each principal (how many approvals are required to advance the workflow to the next step).
  - b. **Bindings:** The workflow's binding is the association between a template (the process) and its principal (who, what and when) that will require approval to perform an action. The binding contains of the associated template, the associated user or group that will be assigned the workflow, the actions that will require approval and finally the time restrictions applied to the approval process.
  - c. **Instances:** The list of all active and completed workflows in the System. This includes who initiated the workflow, with which record, at what time and additional details.
2. **Requester:** The requester is the user who initiates a workflow by requesting an action like **Connect** or **Unlock**. The requester is associated to a workflow by being listed as a User in the workflow's Binding.
  3. **Approver:** The approver is the user who approves or rejects a step in the workflow. Approvers are defined in the steps of the workflow's Template. If an Approver rejects a request at any step, then the workflow is immediately completed and the action is not granted to the requester.
  4. **Status:** The current status of the workflow displays the current step as well as previous approval or rejection comments. The status is visible only to Requesters, current Approvers and System Administrators.
  5. **My Workflows:** The area of PAM where Approvers will find workflows that require their approval and Requesters will find their list and details of active and previous requests.

Please note when designing your workflows, that a user may be binded to a workflow that also includes them in the template as an approver. This configuration is permitted; however, a user in this scenario will not be given the ability or opportunity to approve their own request. You cannot approve your own request.

## Generating a Workflow Request

If a workflow template has been bound to a user or group, then before they can access objects or actions they will need to request Access and ultimately receive approval.

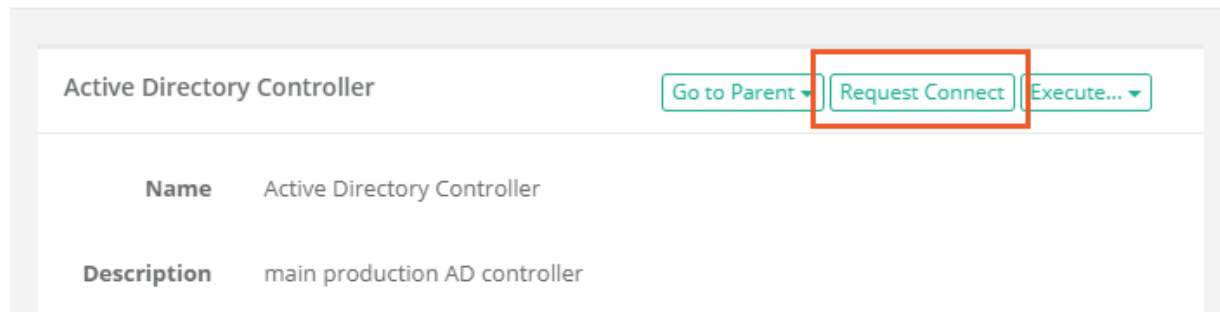
When approved, the requested access or action will become available for the requested time period. If rejected, the requested access or action will not become available and the user will need to make the request again.

## To request access or actions using a workflow

1. Click the **Request Connect** button for the access or action that you would like to request.

### Record View

Home / Records List / **Active Directory Controller**



2. When the *Request Access* screen appears, enter the following information:
  - a. **Reason:** Enter a brief reason for why you are requesting access to this Action. This reason will be sent to the Approver(s) for their consideration.
  - b. Choose between **Requested Minutes** and **Requested From** by selecting the appropriate radio button.
    - **Requested Minutes:** Enter any value greater than 0. The minutes will indicate the amount of time this Action is available to you beginning from the time that the approval workflow is completed as *Approved*. When the time expires, the action will revert back to requiring a Request.
    - **Requested From / To:** Enter or select using the *Calendar* button, a *Requested From* value and a *Request To* value in the future. This will indicate the date range where this Action will be available to you after the approval workflow is completed as *Approved*. When the time expires, the action will revert back to requiring a Request.



- c. Click the **Request** button to submit your request.

## Request Access

### Reason ?

I need to apply security updates

### Requested Minutes ?

60

### ✓ Requested From ?

2017-12-09



12

: 00

### Requested To ?

2017-12-09



13

: 30

Cancel

Request

3. A confirmation dialog will appear alerting you that the request has been submitted. Click **OK** to confirm the message.
4. The Request button will now update to let you know that the Action has been Requested. To see the current status of your request, you may click this **Requested** button or navigate to Management > My Workflows > My Requests.

## Record View

Home / Records List / **Active Directory Controller**

Active Directory Controller		Go to Parent ▾	Connect Requested	Execute... ▾
Name	Active Directory Controller			
Description	main production AD controller			

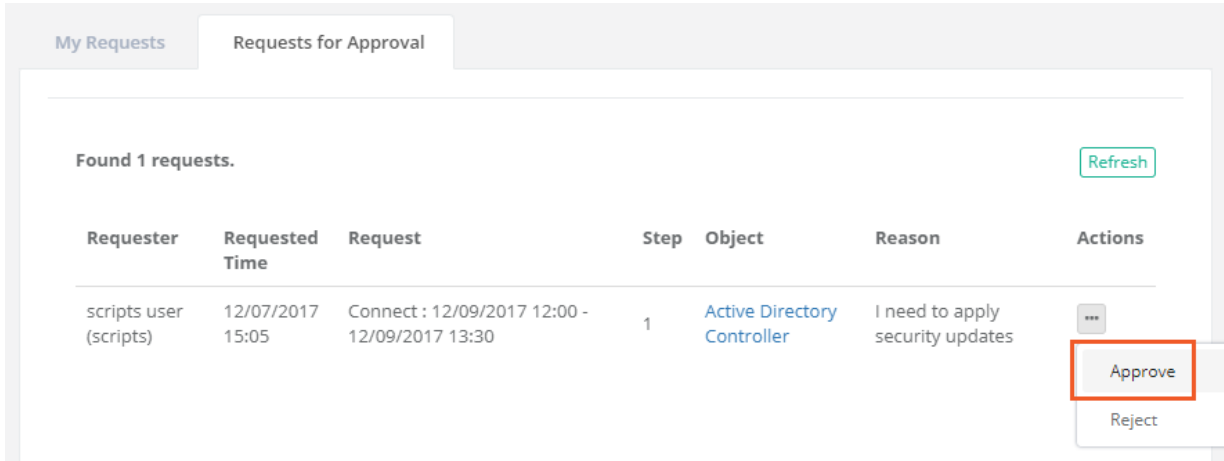
## Approving and Rejecting Requests

When a user requests access to an object or action and you are included in one of the workflow template steps, then a notification will be sent to alert you that a workflow is pending your action.

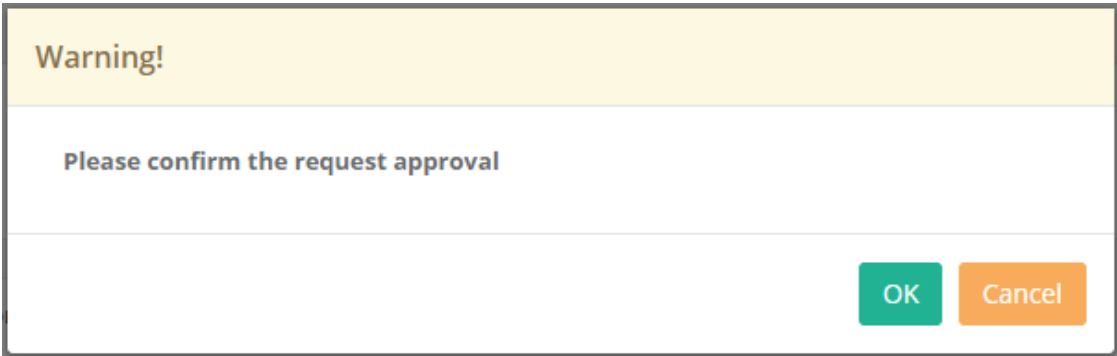
It is at this point, that you will need to review the user’s request and determine whether you wish to Approve or Reject their request.

To approve a request using a workflow:

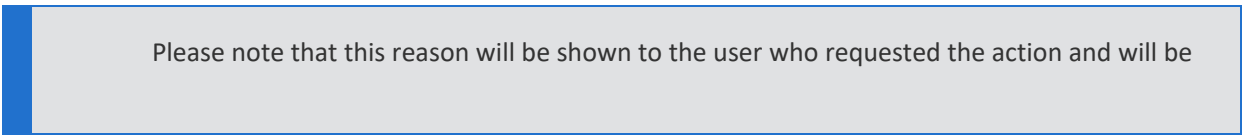
- 1. Once notified, navigate to Management > My Workflows > Requests for Approval.
- 2. Review the user’s request and decide whether you will Approve or Reject the request. Open the **Actions** menu next to the request and select either **Approve** or **Reject**.



- a. If you select **Approve**, a confirmation dialog will appear. Click **OK** to complete the approval process.



- b. If you select **Reject**, a dialog will appear requiring a reason. Enter a reason why the request is being rejected and click the **Reject** button to complete the process.



logged in the workflow instance.

### Reject Request

**Reason**

Not today. Let's wait until the weekend.

CancelReject

3. The requests will now be removed from your approval queue.

A couple additional notes about the Approval process to consider:

- If you are listed as an Approver in a multiple step workflow, this request may appear in your *Requests for Approval* queue again at a later time. The *Steps* column in the request will indicate which step the workflow is currently on.
- A single Reject by *any* Approver will complete the workflow (regardless of step) and notify the requester that the approval was rejected. At this point they would need to make the request again which will restart the process at the beginning.
- If you are the requester and listed as an Approver, you will not be permitted to approve your own request.

## Additional options available to Workflow Approvers

These additional options can be found by accessing the Approved workflow's Details page located in Management > My Workflows > My Requests.

- Workflows Approver(s) may *Join* (web session) or *Terminate* any active session (Connect) that they approved. *Record Control* or *Connect Control* permission is not required.
- Workflows Approver(s) may *review* the *Session Report* and *Session Events* report for any supported session (Connect) that they approved. *Record Control* or *Connect Control* permission is not required.

## Using Email to Approve or Reject Requests

PAM email approval response allows users to approve or reject workflow access requests by simply replying to the Approval request email received after the access is submitted for approval.

This allows Approvers the ability to approve or reject records without logging into the System.

## Enable the Approval by Email Feature

1. Login to PAM with a System Administrator account. Only System Administrators can configure, enable and disable this feature.
2. Navigate to Administration > Settings > Mail Server and add a value for the following parameters and **Save** when completed:

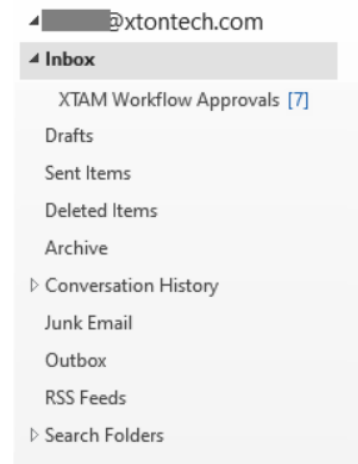
- **IMAP Port:** enter your IMAP port. Default value is 993.
- **IMAP Folder:** enter the name of an existing folder where the approved emails will be delivered to the email address specified in the *Login* field. For example, if the approval email replies are delivered to the default Inbox, enter the value *Inbox*. If these emails are automatically moved to another existing folder or sub-folder, enter the path like `Inbox/PAM Workflow Approvals`.

The IMAP Folder defined is the folder that System will monitor for access request email responses. It is required that all approval emails that are replied to by Approvers end up in this folder or else they will not be found. If you define a location other than the default *Inbox*, then ensure you have created the necessary rules in the mailbox or email server to automatically move these emails to this folder or sub-folder.

We recommend the use of a dedicated email address for the purpose of Mail Server integration and **Approve by Email** functionality so as not to interfere with personal email usage. Email folders that contain a large number of emails can decrease the performance of PAM processing service, therefore PAM deletes access request responses after they are processed.

#### IMAP Mailbox

Server	<input type="text"/>
IMAP Port	<input type="text" value="993"/>
Login	<input type="text" value="...@xtontech.com"/>
Password	<input type="password" value="....."/>
IMAP Folder	<input type="text" value="Inbox/XTAM Workflow Approvals"/>
Use TLS	<input checked="" type="checkbox"/>



3. Navigate to Administration > Settings > Parameters and locate the parameter **Approve by Mail**. Change this setting to *Enabled* then click its **Save** button to enable this feature.

## Email Responding to Access Requests

Responding to Access Requests through Email Replies.

When an access request has been submitted for approval, the Approver(s) will receive a notification to their email address.

Once received, the Approver can respond to the access request by simply replying to that original request email notification.

When responding to an access request, the first line of the email body needs to contain one of the following case insensitive words:

To <u>Approve</u> the Access Request	To <u>Reject</u> the Access Request
Yes	No
Approve	Reject
Approved	Rejected
Ok	{Anything other than the listed <i>Approve</i> words will also reject}

You can add custom *Approval* keywords to PAM by navigating to Administration > Settings > Parameters > Approve by Mail Keywords.

Add additional keywords to this comma separated list that can be used to Approve workflow requests using email replies.

Please note that these are Approval keywords only as any keywords that are not designated for Approval in this list will automatically be detected for Rejection.

## Access Request Email Response

Notes for consideration about the Access Request Email Response.

- Approvers can use standard desktop email clients or mobile email apps and respond to the approval request email by sending a reply with the above words, without requiring the *Approver* to first login to PAM.
- The *Approver* must reply using the same email address that received the email approval request.
- All words contained in the first line of the email body may be included in the Reason field for the Approval or Rejection action.
- Any words contained in the first line of the email body that are not one of the above Approval words will be detected as a Rejection response.
- Periods or other punctuation marks are allowed at the end of the word.
- Approvers can go to their **Requests for Approval** Management page in PAM by clicking the link provided in the request access email.

## Access Request Email Process

Notes for consideration about the Access Request Email Process.

- When the access request response email is sent, it will be delivered to the email address in the Mail Server configuration *Login* account and must arrive in the folder defined in the Mail Server configuration *IMAP Folder*.
- The **Approve by Email** feature has to be *Enabled* in PAM by a System Administrator.
- The Audit Message for the Event Workflow Step Approved will include the value *By email* to indicate this was approved or rejected by an email response.

## Troubleshooting: Emails not Coming

If the Workflow emails are not coming through:

- Ensure that the User is subscribed to the needed alerts here: Management > My Profile > Subscriptions.
- Restart the **PamManagement** service (Windows) or the **pammanager** service (Linux) on all PAM Node(s). This has been seen to rectify issues with stuck notifications or large queues.
- Update to the latest PAM version as notification or mail queue fixes may be needed.

## Granting Approved Access to Others

Some scenarios require the user to request access for themselves to certain actions in a record, however what if you want to grant access for another user because you are assigning them a job to complete?

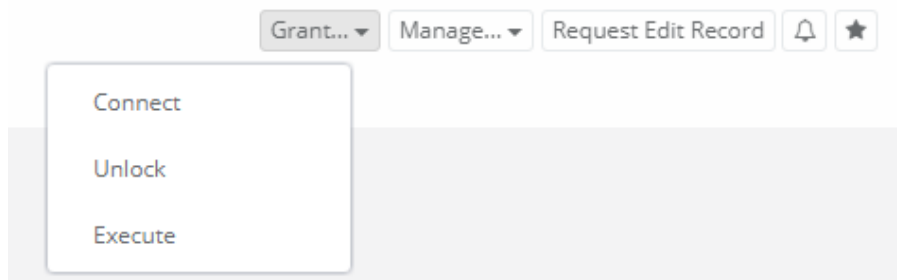
Instead of asking that user to login and then request access, you can go to the record yourself and grant them access for a specific time period or range and for a specific action like **Connect** or **Unlock**.

### To Grant Access on behalf of another User

1. Login to PAM as the Owner of the record or as an System Administrator. Like sharing records, this functionality is limited to [Owners and System Administrators](#) only.
2. Navigate to and open the record in which you want another user to have access to. *Note that a workflow must be applied to this record in order to grant access since it uses the workflow to ultimately approve the request.*

To simplify the process, you could create a [single step workflow template](#) with yourself being the only approver or you could create an [auto-approved workflow template](#) to eliminate the requirement of approving this request all together.

3. Click the **Grant** button and then select the action from the menu you would like to Grant Access to in this record.



4. In the *Grant Access* dialog, populate the following fields
  - a. **Reason:** Enter a reason why you are granting this access to the user(s).
  - b. **Requested Time:** Enter either a time period (in minutes) that the user will have access to this action or a time range (from and to) that the user will have access to this action.

- c. **User:** Add the user(s) that you are granting access.

### Grant Unlock Access

Reason ?

patch server

Requested Minutes ?

60

✓ Requested From ?

2018-01-27



08

: 00

Requested To ?

2018-01-27



17

: 00

User ?

Enter User or Group Name...

Add

Selected Users

John Williams ▾

Cancel

Request

- Click the **Request** button to initiate the approval workflow.
- The approval workflow has now been initiated. A status confirmation dialog will now appear alerting you to the Submitted status of this grant action. Click **Close**.

### Grant Access Status

Users

Status

john

Submitted

Close

- This other user will see the action option in the *Requested* state until the workflow has been approved. Once approved, the action will become available to the user for the duration of the time specified.

Connect Requested

Execute Requested

Unlock Requested

The approval workflow has now been initiated on behalf of this other user. Once the workflow has been fully approved, this user will have access to the action defined in the request for the time period that was specified.

Connect... ▼

Execute... ▼



## Canceling Your Request

After your Access Request has been submitted, the approval workflow process will begin; however you have the ability to cancel your request at any time before the process is complete.

Once you cancel your request, the workflow will immediately complete and be marked as **Terminated**.

### To cancel your Access Request

1. Navigate to Management > My Workflows > My Requests.
2. Locate the request that you would like to cancel, open this request's Actions menu and choose the **Terminate** option.

My Requests

Requests for Approval

Found 26 requests.

Refresh

Object	Requested Time	Request	Reason	Approvers	Status	Actions
Active Directory Controller	12/14/2017 16:40	Unlock : 45	Routine maintenance		Active	<div>...</div> <div>Details</div> <div>Terminate</div>
B	12/14/2017 16:39	Unlock : 45	Maintenance	scripts user:Rejected (Terminated with reason: mistake)	Rejected	

3. Enter a reason for the cancellation and click the **Reject** button.



### Reject Request

**Reason**

Ran out of time today, will need to do this later.

Cancel

Reject

- The request is now cancelled and will appear in your **My Requests** view with the Approvers displayed as your account with the Terminated message.

Object	Requested Time	Request	Reason	Approvers	Status	Actions
Active Directory Controller	12/14/2017 16:40	Unlock : 45	Routine maintenance	scripts user:Rejected (Terminated with reason: Ran out of time today, will need to do this later.)	Rejected	...

## Canceling Another User’s Request

Once a workflow request has been fully Approved, the requester now has access to the function they requested and for the time period in which they requested it.

If you want to Terminate this approved, and now available, function to this user, then please review the steps provided below.

### To cancel an Approved Access Request

- Login to PAM as a System Administrator. Only users with the System Administrator role will be able to Terminate an approved and active access request of another user.

Any users that are included in the Workflow Template (i.e. *Approvers*) of the Approved Workflow can now also Terminate or Cancel this instance. To do so, navigate to Management > My Workflows > My Requests, locate the approved workflow that you wish to cancel and from its *Actions* menu select **Details**. Review and confirm this is the desired Workflow Instance that you wish to cancel, click the **Terminate** button, provide a required **Reason** and click **OK**. The currently Approved workflow for this user will now be cancelled, terminated or checked-in.

- Navigate to Reports > Requests.
- Locate the request that you would like to cancel, open this request’s *Actions* menu and choose the **Details** option.

## Requests Report

Found 2 requests.

Last Week 

Show  entries

Search:

CSV

PDF

XLSX

PDF Protected

CSV Protected

XLSX Protected

Showing 1 to 2 of 2 entries

Request ID	Time	Requester	Workflow	Action	Object	Reason	Status	Actions
56408	06/21/2018 14:25:20	user 01	test01	Connect:60	adfsd	test auditor terminate	Approved	...
56392	06/21/2018 14:22:16	user 01	test01	Connect:30	adfsd	test terminate admin		

First Previous 1 Next Last

- Review the *Details* page to ensure that this is the request that you wish to Terminate. When ready, click the **Terminate** button located in the upper right corner of this page.

Workflow Instance: test01

**Terminate**

Request ID

Template

Created By

Requested By

Requested At

Requested Action

Reason

Object

- Enter a reason for the termination and then click the **Reject** button.

## Reject Request

**Reason**

I accidentally approved this time period. Please resubmit for next week.

Cancel

Reject

6. The request is now terminated and will appear in the *Requests* report with its status set to **Completed**. You can open the *Details* page again to see the Terminated event along with the reason.

Approvers	Step 1: Service Administrator (xtamadmin) at 06/21/2018 14:26 Approved
	Step 65536: Service Administrator (xtamadmin) at 06/21/2018 14:43 Rejected: Terminated with reason: I accidentally approved this time period. Please resubmit for next week.
Workflow Design	Step 1: Service Administrator (1)

## Auto-Approved Workflows

There may be scenarios or time periods (Time Selectors) where you will still want to require a user to *Request Access*, however you want this request to be automatically approved.

The benefits for this are:

- The user will still need to request access therefore supplying a reason and a requested time period.
- The workflow request will become an event in both the *System Audit Log* and the *Workflow Instance Log*.
- Provides the ability to customize time periods where users may need immediate access when approvers may be unavailable to process their request in a timely manner (i.e. Weekends and Holidays).

## To create an auto-approved workflow

1. Navigate to Administration > Workflows > Templates.
2. Click the **Add** button to create a new workflow template.
3. Enter a **Name** for the workflow template.
4. Select the type **Automatic Approval** from the dropdown menu.

[Save](#) [Cancel](#) [↺](#)

Name	<input type="text" value="Automatically Approved Workflow Template"/>
Type	<div>Automatic Approval ▼</div>

---

Do not send notifications ☐

5. Check the *Do not send notifications* box if you wish to suppress notifications from this template being sent to the Requestor(s).
6. Return to Administration > Workflows > Templates, select this template's *Actions menu* and choose the **Publish** option.
7. Navigate to Administration > Workflows > Bindings.
8. Click the **Add** button to create a new workflow binding.
9. In the *Templates* dropdown menu, select the template created in the previous steps.
10. Populate the remaining options in the Binding and click **Save** when complete.

Workflow Template ?
Automatically Approved Workflow Template

Workflow Design
Automatic Approval

Assign to All Users ?
☐

Users ?

Add
Service Administrator (pamadmin) /Local ▼

IP Filter ?

Actions ?

☐ Administration
☐ Record Control
☒ Connect Control
☐ Task Control

Time Selector ?

☐ Work Hours
☐ After Hours
☒ Weekends
☒ Holidays

Cron Expression
 ⓘ

Duration ?

Checkout ?
Disabled ▼

MFA ?
Disabled ▼

Ticket Types ?

Weight ?

The User(s) assigned in the binding now has an auto-approved workflow assigned to them during the time periods and actions defined.

## Workflow Time Expiration

When an action is requested, the user making the request (the requester) has to define either how much time they need with the action (a time period) or when in the future they would like this action to become available (a time range).

But what happens to this approved action once this time expires?

### Request Access

Reason ?

☒ Requested Minutes ?
(Requested Time Period)

---

☐ Requested From ?

:

☐ Requested To ?

:

(Request Time Range)

A number of things may happen depending on how PAM is configured, so let's begin with the action itself.

When the requested time expires for any action, the action returns back to the Request state and the user must request access again.

That means the action will no longer be accessible to this user and the entire approval process begins again. For example, if the requested action is to the **Unlock** button of a record, the Unlock button will return back to its default **Request Unlock** state when time expires and this user will no longer be able to reveal the secured password, secret or file.

Instead they will need to open a new *Request Access* workflow.

Password

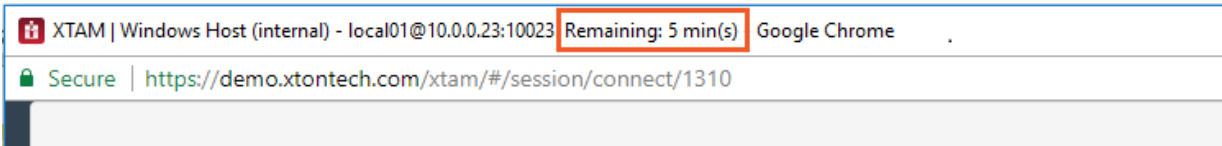
Another scenario that may occur is what happens when the time expires during an active *remote session*? And the answer to this question is, it depends on how PAM is configured by the System Administrator(s).

By default, if the requested time expires during an active session (the request action in this scenario is on a record's Connect option), then that active session will automatically **Terminate**.

The session will close and the user will not be permitted to Connect again because the connect option will revert back to its default **Request Connect** state.

So if the user needs additional time with this remote host, then they will request again with a new time period or range and once approved, the Connect option will return.

Active sessions that will automatically terminate will display the remaining time until termination in the session’s title bar.



The other option would be for System Administrators to configure the session to allow active sessions to **Continue**.

What this ultimately does is ensure that any sessions that are active when the requested time expires remain active so that the user’s can continue working with the remote host.

Once the user completes their own session, then they will not be able to open a new session because the connect option will return to its default **Request Connect** state.

This leaves the session in an “open ended” state as it only requires the user to start the session during the requested time, not complete it.

Windows Host (internal)



It should be noted that System Administrators also have the option to define an Idle Timeout period that is used for all remote sessions.

This will terminate any active sessions that remain idle for longer than the defined time limit.

In conjunction with the open-ended approved sessions, the idle time limit prevents a user from leaving an approved session open for much longer (overnight or over the weekend) than what was originally intended.

If you are a System Administrator, both the **Session Idle Timeout** and the **Session Request Enforcement** options are located in Administration > Settings > Parameters.

A screenshot of a configuration page titled 'Session Parameters'. It contains four rows of settings, each with a label, a value field, a help icon, and a 'Save' button. The first row is 'Session Idle Timeout' with the value '0', highlighted with a red box. The second row is 'Session RDP Resize Method' with the value 'Reconnect'. The third row is 'Session RDP Screen Size' with the value '1024x768'. The fourth row is 'Session Request Enforcement' with the value 'Terminate', highlighted with a red box.

In summary,

- When the requested time expires for an action, the action returns back to its default Request state and the user must request access again.
- When the requested time expires during an active remote session, the session will either **Continue** until the user completes it themselves or it will automatically **Terminate** (remaining time is displayed in the Session Title Bar) depending on the System configuration. Regardless, the Connect option will return to its Request state and the user must request access again to open a new remote session.
  - **Continue** means the user must start but not complete the session during the requested time.
  - **Terminate** means the user must start and complete the session during the requested time.

## Modifying Workflows

### Conditions

Once a workflow has been created, you may **Edit** or **Delete** it with the following conditions:

- Only PAM System Administrators will be able to create, update or delete workflows.
- Changes to an existing workflow will be applied to new instances. Currently Active or In-progress workflow instances will maintain their original configuration.
- Any changes to a workflow template must be Published before they can be used in a binding.
- Workflow templates may not be deleted if they are currently being used in a binding.
- If a binding is removed from a user (Edit or Delete) who has an Active request, this action will immediately become available to the user regardless of the workflow process. The workflow will remain in its Active state until it is either Terminated by the user or Rejected by an approver.

### Update workflow template

**To update an existing workflow template:**

1. Navigate to Administration > Workflows > Templates.
2. Locate the template that you wish to update, open its Actions menu and choose the **Edit** option.
3. Make the necessary updates and click the **Save** button when you are finished.
4. Return to the Templates main page, locate the template that was just updated whose status will be Draft, open its Actions menu and choose the **Publish** option. The template is now updated.

### Update workflow binding

**To update an existing workflow binding:**

1. Navigate to Administration > Workflows > Bindings.
2. Locate the binding that you wish to update, open its Actions menu and choose the **Edit** option.
3. Make the necessary updates and click the **Save** button when you are finished.
4. The binding is now updated.

### Delete workflow template

**To delete an existing workflow template:**

1. Navigate to Administration > Workflows > Templates.
2. Locate the template that you wish to delete, open its Actions menu and choose the **Delete** option.
3. Confirm the delete option by clicking the **OK** button.
4. The template is now deleted.



# Delete workflow binding

## To delete an existing workflow binding:

1. Navigate to Administration > Workflows > Bindings.
2. Locate the binding that you wish to delete, open its Actions menu and choose the **Delete** option.
3. Confirm the delete option by clicking the **OK** button.
4. The binding is now deleted.

# Workflow Template Types

When creating a Workflow Template, the following types are available: **Automatic Approval**, **Interactive Approval** and **Restrict Access**.

## Workflow Template

Home / Workflows / Workflow Template

Please specify workflow template name

Save Cancel Add Step ↺

Name

Type 

Interactive Approval ▼  
Automatic Approval  
Interactive Approval  
Restrict Access  
Delegated Approval

Step 1

Created By: system at  
Last Modified By: system at  
Status: -

## Automatic Approval

This type creates an automatically approved workflow template.

You would select this type when you want to make use of the **Request Access** option for users, but if you want to the request itself to be automatically approved.

For example, if an Admin needs to access a server to resolve a specific ticket, this user could enter the ticket number in the request form so that it becomes part of the audit trail and then their access is immediately granted.

Because it does not require any approvals, this type does not include options to add Approvers or Steps.

## Interactive Approval

This type creates an interactive approval process template. This is a traditional approval process that requires at least one user to Approve the workflow request in order for the requested user to gain access to their requested option.

## Delegated Approval

Delegated Approval workflow allows users to delegate their approval action to the system.

The system approves all requests for these workflows automatically on the behalf of the specified approvers.

Approvers receive notifications as well as permissions to review, join and terminate sessions granted by this automatically approved request in the way that approvers of interactive workflows do.

Delegated Approval workflow allows to add notifications and permissions of automatic approvals to designated individuals.

## Restrict Access

This type creates a template that restricts access to options based on who and what is bound to the template.

For example, if you do not want the Connect option to be available at all for a specific user or group or during a specific time of day (i.e. after work hours) or even a specific location (determined by IP Address), then using this template type will remove the option from the Record.

Because it does not require any approvals, this type does not include options to add Approvers or Steps.

Note that an Interactive Approval template type can still be configured to be an auto-approved workflow by simply not adding any Approvers to the template (i.e. an empty Step 1).

## Formulas

### Password Formula

Privileged Access Management Password Formulas (define complexity and length).

When PAM is used to automatically generate a new password, it uses the defined *Formula* in order to randomize a value that conforms to its requirements.

System Formulas can be unique to record types (i.e. a different formula for Windows vs Unix endpoints) or it can be unique to records themselves (i.e. a different formula for each Windows endpoint).

If you manually enter a *new password* to be used for the reset procedure, it also must meet the requirements defined in the formula.

**To define your System formula on a record type**, you will need to have the System Administrator role.

Once logged in with your System Administrator account, navigate to Administration > Record Types and then click the **Edit** button next to the record type you wish to update.

Finally, click the **Formula** button to open its configuration page. Make the required changes to the formula and then click the **Save** button to finalize the update.

**To define your PAM formula on a record**, you will need to have at least the *Editor* role for this record.

Once logged in, select the Manage > Formula option and then the **Make Unique** button on its configuration page to break the Formula inheritance.

Make the required changes to the formula and then click the **Save** button to finalize the update.

Production Web Server

Go to Parent

Connect... ▾

Execute... ▾

Name

Production Web Server

Description

Host

192.168.11.106

Port

User

ad2\neon

Password

\*\*\*\*\*

Command Controls

Formula

Permissions

Tasks

Workflows

Archive

Manage ▲

Edit

Record Type: Windows Host

ID: i-8pknppY4UZG

ID-CAP: L-1HM8PWDG3UDXS

Created By: Service Administrator (xtamadmin) /Local @ 06/11/2021 15:33

Last Modified By: Service Administrator (xtamadmin) /Local @ 06/15/2021 17:38

Last Action: Connect @ 06/15/2021 18:12

Last Success: Connect @ 06/15/2021 18:12

Job Queue: (click to refresh)


Audit Log

Change History

Sessions

Job History

[Make Unique](#) [Cancel](#) 

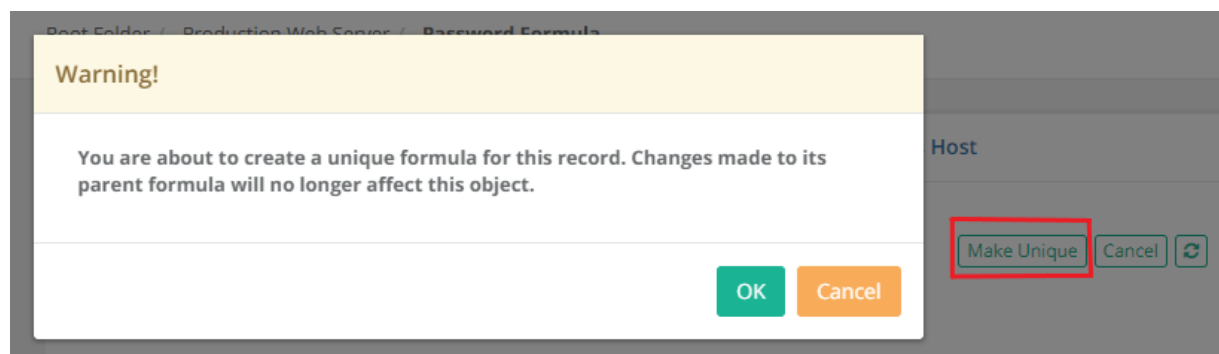
XKCD Formula 	<input type="checkbox"/>
Minimum Password Length	<input type="text" value="8"/>
Maximum Password Length	<input type="text" value="20"/>
Minimum Number of Upper Case Characters	<input type="text" value="1"/>
Minimum Number of Lower Case Characters	<input type="text" value="1"/>
Minimum Number of Numeric Characters	<input type="text" value="1"/>
Minimum Number of Special Characters	<input type="text" value="1"/> <input type="text" value="!@#\$%^*()_+&lt;&gt;?:~=-{}[]"/>
Minimum Number of Whitespace Characters	<input type="text" value="0"/>
Forbid Using User Name	<input type="checkbox"/>

Sample  [Generate](#)



Password is Very Strong.

Once logged in, select the Manage > Formula option and then the **Make Unique** button on its configuration page to break the Formula inheritance.



## XKCD generator to password formula

XKCD generator to password formula as an option to construct passwords from several dictionary words separated with the provided delimiter.

The strength and practical use of such passwords popularized by [XKCD comic strip](#) as those that are easy for people to remember and hard to computers to break.

XKCD password generator allows to specify the number of words to use, the set of separators and number of lower- and upper-case letters in the passwords as an alternative to traditional requirements for the presence of numbers, special characters, upper- and lower-case characters in the passwords.

### Password Formula for Production Web Server

Inherit from Parent Save Cancel ↺

XKCD Formula ?

☒

Minimum Number of Upper Case Characters

1

Minimum Number of Lower Case Characters

1

Number of Words

3

Delimiter

-+

Sample

gating-issuinG-mandate

Generate

Password is Very Strong.

Make the required changes to the formula and then click the **Save** button to finalize the update.

## Formula Options

The following options are available when configuring your PAM formula. Enter a zero to exclude the option from the formula.

- **XKCD Formula:** Formula that allows to generate a password from several random words of English dictionary separated with specified delimiter. This kind of password is much easier to remember.
- **Minimum Password Length:** Define the minimum number of characters. Must be a value or 1 or higher.
- **Maximum Password Length:** Define the maximum number of characters. Be aware of the password length limit on your systems when entering this value. Older systems may be not support extremely long passwords which could result in errors.
- **Minimum Number of Upper Case Characters:** Define the minimum number of upper case characters.
- **Minimum Number of Lower Case Characters:** Define the minimum number of lower case characters.
- **Minimum Number of Numeric Characters:** Define the minimum number of numeric characters.

- **Minimum Number of Special Characters:** Define the minimum number of non-alphanumeric characters. You may also customize the list of available non-alphanumeric characters that can be used.
- **Minimum Number of Whitespace Characters:** Define the minimum number of whitespace (spaces) characters.
- **Forbid Using User Name:** Enable this option to forbid the user from entering their name in the password.

PAM will not allow you to create a formula where your combined *minimum number* options does not conform to your min / max password length. For example, if you formula has a password length of 20-30 (min-max) characters and you attempt to define a minimum of 10 upper, 10 lower, 10 numeric and 10 special characters. This will generate a password of at least 40 characters which is outside of the permissible range.

To create a custom dictionary, add a list of words in the text file `eng_words.txt` one word per line, zip the file in the `eng_words.zip` and copy the ZIP in the `$PAM_HOME/content/templates` folder. Use the default dictionary located in the `$PAM_HOME/web/webapps/pam/templates/eng_words.zip` as an initial template.

[< Generate Strong, Unique Passwords](#)

## Local Users Password Formula

It's easy to generate, reveal and copy passwords to the clipboard when creating or editing Local Users.

Changing the *System Local Users Password Requirements* (length and complexity).

When creating local users in System, the default password formula is set to 8 characters, including the use of 1 upper case, 1 lower case and 1 numeric character.

If you would like to modify this requirement, please perform the following procedure.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Local Users.
3. Click the **Formula** button.



4. Modify the password formula requirements as needed and then click the **Save** button when finished.

The password requirements for PAM Local User accounts are now updated and will be enforced on new user (s) creation or existing users' password changes.

## Random Password Generator Screen

Privileged Access Management contains an easy random password generator screen accessible from any part of the WEB application.

**Generate Password** allows a user to quickly generate a random password for various uses.

Once the password is generated, the user may select and copy the password from their browser or use the **Copy** button to send the password directly to their clipboard.

The random password is generated using the system-level [password formula](#) accessible from Administration / Local Users / Formula screen and can only be modified by a Privileged Access Management System Administrator.

## Password Formula ?

Home / Local Users / Password Formula

Password Formula for

Save

Minimum Password Length

12

Maximum Password Length

48

Minimum Number of Upper Case Characters

2

Minimum Number of Lower Case Characters

2

Minimum Number of Numeric Characters

2

Minimum Number of Special Characters

2

!@#\$%^&\*()\_+<>?:~=-{}[]

Minimum Number of Whitespace Characters

0

Forbid Using User Name

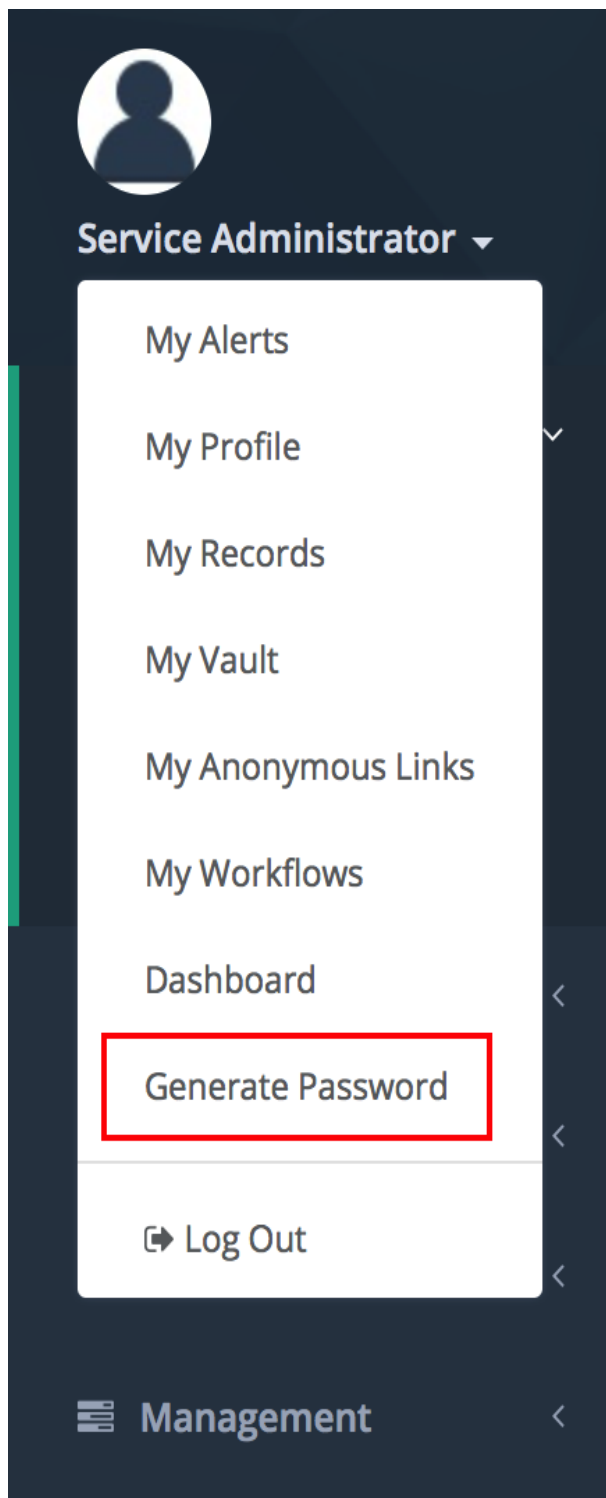
☒

Sample

=JB!4YvjJWh\*8j{-aq;

Generate

Any logged in PAM user can access the *Generate Password* option by opening the dropdown menu located under their Profile picture.






A **Generate Password** field appears at the top of your page:



## Generate Password

\*\*\*\*\*






Close

the **Unlock** button will unlock or lock the current password:

## Generate Password

:sC]rM16hdO1Dm^M~#kYoXgzrLEL{C)+eK\*<E\$






Close

the **Generate** button will generate a new random password:

## Generate Password

QE>A!s6=rmU]sS3?hCe9qm-enZ!3]tB5






Generate

Close

the **Copy** button will copy the current password to your clipboard:

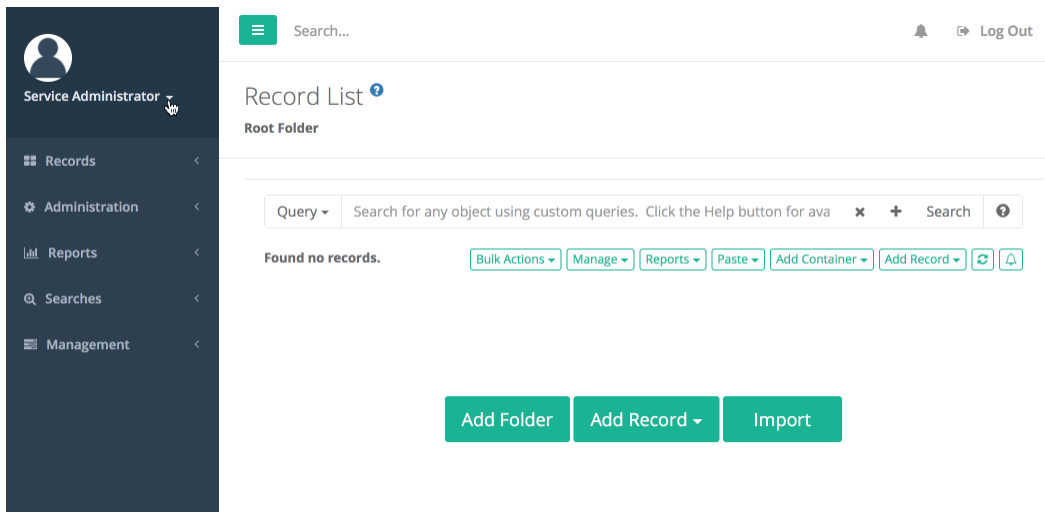
## Generate Password

QE>A!s6=rmU]sS3?hCe9qm-enZ!3]tB5



Copy

Close



## Script Library

Within, PAM [Tasks](#) are used to execute commands against managed endpoints. Some of the most common examples of Tasks are password reset or rotation, group membership cleanup and managing service accounts. These Tasks consist of two components; a *Script* (the code) that defines what is to be executed against the endpoint (“*reset the password*”) and an [Event](#) (the time or action) that defines when the script is to be executed (“*every Sunday*” or “*after Check-In*”).

The Script library contains a listing of all scripts that are currently stored and available for use within the application’s Tasks.

This includes the out of the box scripts that can be used for common code execution like resetting Windows/Linux/Cisco/etc passwords as well as any custom scripts that have been created by System Administrators.

For Netscaler, Fortigate, NetApp and Cisco Nexus network devices are available *Check Status* and *Password Reset* scripts.

When configuring a [Task](#), only scripts that are created and stored in the [Script Library](#) will be available for use.

Any user who has been granted the global *System Administrator* role may access and modify the contents of the Script Library, located at Administration > Scripts.

Any user who has been granted the global *Auditor* role may access but not modify the contents of the [Script library](#).

Found 55 scripts.

[Create](#) 

Name / Description	Driver	Actions
<input type="checkbox"/> Check Status Remote Cisco <i>Use to check status on a Cisco device.</i>	Cisco	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> Check Status Remote Informix DB <i>Use to check status on in Informix DB.</i>	Informix DB	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> Check Status Remote Juniper <i>Use to check status on a Juniper device.</i>	Juniper	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> Check Status Remote Oracle DB <i>Use to check status on in Oracle DB.</i>	Oracle DB	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> Check Status Remote Palo Alto Networks <i>Use to check status on a Palo Alto Networks device.</i>	Palo Alto	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> Check Status Remote SSH	Unix Remote	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> Check Status Remote Windows	Windows Remote	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> Elevate Privileges on a Windows Host <i>A Windows script to add the logged in XTAM user to the local Administrator group.</i>	Windows Remote	<a href="#">Edit</a> <a href="#">Delete</a>

## The Script library columns

- **Name / Description:** Displays the Name of the script (required value) as well as the Description (optional value) below it in italics.
- **Driver:** Displays the type of Endpoint, Device or Service this script was written to support. For example, Windows Remote, Cisco, Informix DB, Remote Apps, etc.
- **Actions:** Provides a list of available options that may be performed against the selected script.

We do not recommend you Edit or Delete the out-of-the-box scripts, instead use the **Create** option to create a custom script that can be used for modifications.

## Creating a new script

1. Login to the PAM with an account that has been granted the System Administrator role.
2. Navigate to Administration > Scripts and click on the **Create** button.
3. Enter the values for your new script into the following fields:
  - a. **Script Name** (required): Enter a name for your script.
  - b. **Description** (optional): Enter a description of your script.
  - c. **Job Execution Strategy** (required): Select the type of endpoint, device or service the script will be used against.
  - d. **Custom Code()** (required): Type or paste your script into this field.
4. Click the **Save** button when you are done and then **OK** to confirm your action.

Once the script has been saved to the library, you may when select it from the **Script** drop down menu when configuring an System task.

## Editing an existing script

1. Login to the PAM with an account that has been granted the System Administrator role.
2. Navigate to Administration > Scripts and click on the **Edit** button for the selected script.
3. The selected script with its current configuration will load into an editable form. Make the desired changes and then click the **Save** button. If you are modifying one of the System out-of-the-box scripts, then you may click the **Factory Default** button from this same editable form to return the script to its original, shipped configuration. button, then **OK** to confirm your action.

If you are modifying one of the System out-of-the-box scripts, then you may click the **Factory Default** button from this same editable form to return the script to its original, shipped configuration.

## Deleting an existing script

1. Login to the PAM with an account that has been granted the System Administrator role.
2. Navigate to Administration > Scripts and click on the **Delete** button for the selected script.
3. Confirm this delete action by clicking the **OK** button on the confirmation pop-up message.

Note that a script currently in use cannot be deleted.

Please use caution with the **Delete** option as there is no Undo button to restore a deleted script.

## Script for task to trigger another task

To trigger a task with another task for the same record after its successful completion comment at the end of the task in the following form to trigger script-name if it is assigned to the record:

```
1 | #XTAM TRIGGER SELF script-name
```

## Scripts Library

The Scripts library contains a listing of all scripts that are currently stored and available for use within a task. This includes the out of the box scripts that can be used for common code execution like resetting or rotating Windows or Linux passwords as well as any custom scripts that have been created by System Administrators. When configuring a Task, only scripts that are created and stored in the Scripts library will be available for use.

Any user who has been granted the global System Administrator role may access and modify the contents of the Script Library, located at Administration > Scripts.

Any user who has been granted the global Auditor role may access but not modify the contents of the Script library.

## Creating Custom Scripts

Adding your own scripts to the system's Scripts library allows you to incorporate your custom code with PAM's automated, policy driven task engine.

To create your own scripts, navigate to Administration > Scripts and click the **Create** button. Enter the values as needed into the available fields and click **Save** to complete the creation process.

Script Name	Enter a name for your custom script
Description	Enter a description for your custom script
Job Execution Strategy	Select the job execution strategy that will be used to execute the custom code. The selected value is usually representative of the device, service or endpoint that the code will be executed against.
Custom Code	Enter your custom code or script into this field.

## Editing Existing Scripts

To edit an existing script, navigate to Administration > Scripts and click the **Edit** button for the desired script. Make the necessary changes and click the **Save** button to complete the edit operation.

When working with one of the "out of the box" scripts, you can use the **Factory Default** button to restore the script and its configuration to its default, shipped state, overwriting any changes that have been made to this script.

Click the **Save** button after using this option.

Tip: PAM comes "out of the box" with many prebuilt scripts. While it is possible to edit or delete any of these scripts, we recommend that you create new scripts rather than editing or deleting them.

## Deleting Existing Scripts

To delete an existing script, navigate to Administration > Scripts and click the **Delete** button for the desired script.

Scripts that are currently assigned to a task or are in-use cannot be deleted.

Tip: PAM comes "out of the box" with many prebuilt scripts. While it is possible to edit or delete any of these scripts, we recommend that you create new scripts rather than editing or deleting them.

## Using Variables or Placeholders

Using the PAM Task and Job Engine, remote commands and scripts can be executed against a remote host.

In conjunction with the PAM Identity [Vault](#), the execution of these tasks can be shared and delegated to other users who may not necessarily have native permissions to perform such actions on the host.

It is in this scenario, where PAM provides the flexibility for the user executing the task to determine some of the parameters of the operation.

Let's begin by taking a look at a simplistic script that one may wish to run against a remote host:

```
1 | netsh.exe advfirewall set privateprofile state off
```

This basic script will set the Private Profile of the Windows Firewall *Off* on the host.

A very specific script that executes a very specific command which expects a very specific result.

However, what if you wanted your user to be able to turn *On* the firewall profile rather than *Off*:

```
1 | netsh.exe advfirewall set privateprofile state on
```

Well, that is simple too. Just create another script with the state on.

And what if you wanted the user to be able to check the status settings of a firewall profile.

```
1 | netsh.exe advfirewall show publicprofile
```

There's a script for that as well.

So you could conceivably create a specific script for every possible scenario (*on, off, status for public; on, off, status for private; on, off, status for domain*), but that would be incredibly time consuming, extremely difficult to manage and not very efficient for users.

This is precisely where the power of variables or placeholders comes in to the picture.

Rather than creating dozens of individual scripts (which the system will certainly support if you choose), you can create a single script using placeholders and allow the user to implement the commands they need.

And that would look like this:

```
1 | netsh.exe ${Service Name} ${Command}
```

When the above script is executed in PAM, the user executing it will be asked to provide the values defined by the placeholders, `${Service Name}` and `${Command}`.

They can then enter which service and command that they specifically want to execute and the PAM job engine will replace those in the script and then execute it accordingly.

**Script Parameters**

**Service Name**

**Command**

Cancel OK

In this example, the user would enter *advfirewall* and *set privateprofile state off* into the Script Parameters dialog, the engine will add those values into the placeholders and execute the command:

```
1 | netsh.exe advfirewall set privateprofile state off
```

This provides much greater flexibility to the users to determine exactly which command they want to execute without having to pre-create dozens or hundreds of scripts for them.

**Script Parameters**

**Service Name**

**Command**

Cancel OK

The results or output of the script will be displayed in the Job History page of this record.

You could use this functionality in any script that you want to configure, but here are a few more examples.

*To restart a service in a Unix or Linux host:*

```
1 | SRV=${Service Name}
2 | ACT=${Command (options: start,stop,restart,status)}
3 | sudo service $SRV $ACT
4 | echo Results:
5 | ps -ef | grep $SRV
```

**Script Parameters**

**Service Name**

**Command (options: start,stop,restart,status)**

*To create a new user in Active Directory and add them to a group:*

```

1 New-ADUser -Name '${Name}' -Path '${Path}' -userPrincipalName '${UPN}' -
  DisplayName '${Display Name}' -AccountPassword (ConvertTo-SecureString
  '${Password}' -AsPlainText -Force) -ChangePasswordAtLogon $true -Enabled $false
2 Add-ADGroupMember '${Domain Group}' '${Name}'
3 write-host "----- User ${Name} has been created -----"

```

**Script Parameters**

**Name**

**Path**

**UPN**

**Display Name**

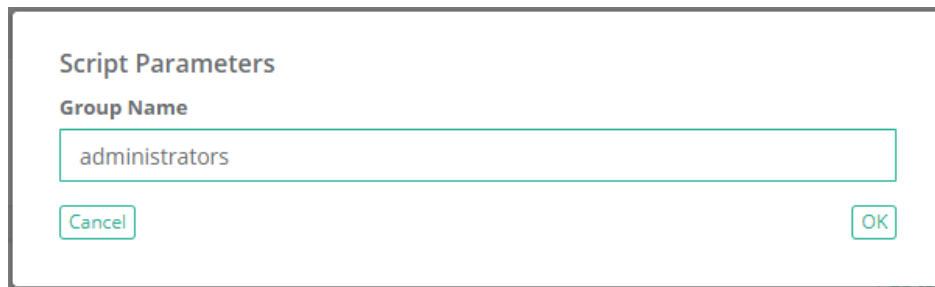
**Password**

**Domain Group**



To list the members of a Windows local group:

```
1 | ([ADSI]'WinNT://./${Group Name},group').members() | ForEach{$_.GetType  
(').InvokeMember('ADspath', 'GetProperty', $null, $_, $null).Replace  
( 'WinNT://', '' ) }
```



A screenshot of a 'Script Parameters' dialog box. It has a title bar 'Script Parameters'. Below the title bar is a label 'Group Name' followed by a text input field containing the text 'administrators'. At the bottom of the dialog are two buttons: 'Cancel' on the left and 'OK' on the right.

Script designers can use values from any record field in the scripts using **{{RECORD:FieldName}}** placeholder and any field of a shadow record using **{{SHADOW:FieldName}}** placeholder. Note that **FieldName** in this context is the name of the field from the record type architecture (not display name visible on the record view).

Script designers can also use predefined placeholders for frequently used fields:

**{{LOGIN}}** - User on record

**{{NEWPWD}}**, **{{PWDNEW}}** or **{{NEWPWD-BASE64}}** - New password

**{{OLDPWD}}**, **{{PWDOLD}}** or **{{OLDPWD-BASE64}}** - Old password or Password on record

**{{DOMAIN}}** - domain part of the User on record

**{{SHADOW\_LOGIN}}** - User name of the Shadow record

**{{SHADOW\_PASSWORD}}** or **{{SHADOW\_PASSWORD-BASE64}}** - Password on the Shadow record

**{{PAMLOGIN}}** - User name of the currently logged in user (the field is useful for on-demand tasks triggered interactively by user actions)

**{{PAMACCOUNT}}** - Username of the currently logged in user of a UPN format (The **{{PAMACCOUNT}}** variable will remove the "@domain" portion of the username, An example: *administrator@pam* will be replaced as *administrator*.)

## Discovery

### Discovery Query

Privileged Access Management includes an option to run a discovery query across your environment to locate and report on found endpoints and their configurations.

This scan can be configured to be automatically run at scheduled intervals and the resulting report can be used to create new records that can immediately be placed under management. In addition, the optional Auto-Import option will create Records for newly discovered hosts.

Discovery queries can be constructed for several scenarios:

Active Directory Query	This query creates a scan across the entire network using the supplied Active Directory account(s) to attempt to communicate with all found endpoints. This option requires that the system be integrated with your Active Directory.
IP-Range Query	This query creates a scan across a specific range of IP address (From – To) and attempt to communicate with the found endpoints using PowerShell (Windows) or SSH (Unix/Linux) in combination with the supplied account(s).
CSV-Based Query	This query creates a scan based on the endpoints that are supplied using an external CSV file.  If a list of endpoints is already available to you, then this option will use that for the input of the scan and attempt communication using PowerShell or SSH in combination with the supplied account(s).
Amazon EC2 Query	This query creates a scan based on accessible EC2 instances running in your Amazon AWS environments.  AWS Keys, regions, credentials and other information is required in order to successfully complete this query.

## Creating a New Query

To create a new Discovery query:

1. Navigate to Administration > Discovery and click the **Add Query** button to select your query type.
2. When the new Discovery query page opens, configure the query as required.
3. When finished, click the **Save** button.

Newly created queries, that are enabled, will be queued for processing immediately.

For information about each available option, please click the option's **Help** button for a brief description or read our online article [Privileged Discovery Queries](#).

## Managing Existing Queries

To manage your existing queries, navigate to the Administration > Discovery page and click on the desired button as described below.

Edit	Use the Edit button to make changes to the selected query's configuration.
View	Use the View button to view the results of the executed query.
Enable	Use the Enable button to enable a currently disabled query (supports multiple selections).
Disable	Use the Disable button to disable a currently enabled query (supports multiple selections).
Delete	Use the Delete button to delete the currently selected queries (supports multiple selections).
Refresh	Use the Refresh button to refresh the list of queries to display the latest configuration and status.

## Viewing a Query Report

To review the results of a Discovery Query after it has completed at least one run, click its **View** button.

The Discovery results report will list all hosts that were found during the previous run(s).

The default view is filtered to the *Connected* state, but you may switch between the available options: All, Open Port and Connected.

All	Displays all the endpoints that were found regardless of the response.
Open Port	Displays the endpoints that were found with an open port (PowerShell or SSH) regardless of the response.
Connected	Displays all the endpoints that were found, and communication was successfully established using one of the Accounts provided in the query.

Other options available within the Discovery Query report include:

Remove Hosts	Use this option to remove <u>all</u> discovered hosts from the report.
Copy	Use this option to copy the selected host(s) that can then be pasted to a container in a Record List as a new record.

## Deleting Queries

To delete an existing query, navigate to the Administration > Discovery page.

Select the query that you wish to delete and finally click on the **Delete** button to remove it.

The delete operation can support both single and multiple selections.

Delete will remove both the query and all its previous results.

Use the *Disable* option instead if you want to stop the query from executing and retain the previous results.

## Scheduling Queries

Discovery Queries are configured to be queued every 120 minutes.

New queries will be added to the job queue when saved; however existing queries that are edited will not be updated to the queue.

To change this default 120-minute schedule:

1. Navigate to the Administration > Settings > Application Nodes tab.
2. In the list of Application Nodes, locate the node that is labeled as the *Worker* and click its **Edit** button.
3. Enter your desired interval in the Discovery *Idle Time* setting (defined in minutes between scans) and click the **Save** button when finished.

## Privileged Discovery Query

Privileged Access Management (PAM) includes an option to run a discovery across your network to locate and report on found privileged endpoints and their configurations.

This scan can be configured to be automatically run at scheduled intervals and the resulting report can be used to create new records that can immediately be placed under management.

In addition, the Auto-Import option will create Records for newly discovered hosts.

With the Privileged Access Management Discovery, you can expect:

1. A scan of your corporate network that will identify all endpoints that respond.
2. A regular report that includes a list of all endpoints discovered as well as information about itself.
3. To more easily create managed records from endpoints found that are categorized as privileged.
4. Multiple options that will allow for customizing the scan to fit the design of your requirements.

[Discover Queries](#)

[Creating a Discovery Query](#)

[Discovery Query Reports](#)

[Discovery Query Report Actions](#)

[Discovery Query Schedule](#)

## Discover Queries

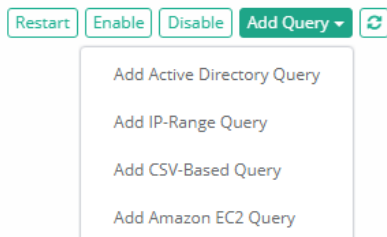
The following discovery queries are available.

1. **Active Directory Query:** This query creates a scan across the entire network using the supplied Active Directory account(s) to attempt to communicate with all found endpoints.
2. **IP-Range Query:** This query creates a scan across a specific range of IP address (From – To) and attempts to communicate with the found endpoints using PowerShell (Windows) and SSH (Unix/Linux) in combination with the supplied account(s).
3. **CSV-Based Query:** This query creates a scan based on the endpoints that are supplied using an external CSV file. If a list of endpoints is already available to your, then this option will use that for the input of the scan and attempt communication using PowerShell or SSH in combination with the supplied account(s).  
[Click to download a sample CSV template.](#)
4. **Amazon EC2 Query:** This query creates a scan based on accessible EC2 images running in Amazon AWS environments. AWS Keys, regions, credentials and other information is required in order to successfully complete this query. For more information, please read our [Discovery for AWS](#) article.

## Creating a Discovery Query

How to create an PAM Discovery Query.

1. Login to PAM using a System Administrator account.
2. Navigate to Administration > Discovery.
3. Create a new Discovery query by clicking the **Add Query** button and then selecting the desired Query type as described in a previous section of this article.



4. Depending on the query selected, the following options may be available:

For Amazon EC2 Queries, please see our [Discovery for AWS](#) article for configuration details.

- a. **Name:** *(All)* The name of the discovery query.
- b. **Filter:** *(Active Directory Query)* Provides a method to filter endpoints based on the following values from AD: name, dnshostname, operatingsystem, operatingsystemservicepack
- c. **IP From:** *(IP-Range Query)* The starting IP address for the range.
- d. **IP To:** *(IP-Range Query)* The ending IP address for the range.
- e. **Use PowerShell:** *(IP-Range Query, CSV-Based Query)* Check the box to enable the use of PowerShell for the scan (for Windows endpoints). *Only PowerShell or SSH can be selected per query. If you would like to use both Protocols, then a second query must be created.*
- f. **Use SSH:** *(IP-Range Query, CSV-Based Query)* Check the box to enable the use of SSH for the scan (for Unix or Linux based endpoints). *Only PowerShell or SSH can be selected per query. If you would like to use both Protocols, then a second query must be created.*
- g. **Non-Standard Ports:** *(IP-Range Query, CSV-Based Query)* Comma-separated list of non-standard ports to try during host discovery. If not specified the discovery process will attempt to connect to a remote host using port 22 for the SSH protocol and to the WS-Management port 5985 for the PowerShell protocol.
- h. **Discover Local Accounts:** *(All)* Defines the type of user account to discover on the connected end-point. Discovered accounts could be either manually or automatically imported into the system as records. When imported, these accounts will be assigned a shadow record as a main host for future task executions. The following options are available:
  - **All Accounts:** Discovery will list all local accounts found on the end-point.
  - **Privileged Accounts:** Discovery will list only privileged accounts on the end-points. Privileged accounts in this context are those accounts in the local Administrators groups (Windows) and members of the sudo group (Unix). Unlike the All Accounts options, this list may include both local and domain accounts. These domain accounts will not be auto-imported to the vault.

Note that both the Windows and Unix scripts for All Accounts and Privileged Accounts discovery could be customized using the [Scripts library](#).

- i. **Upload CSV:** *(CSV-Based Query)* Upload the CSV file that contains the list of endpoints to be included in the scan. Click the Sample button to generate a CSV file that can be used as a template for proper formatting.
- j. **Accounts:** *(All)* Enter the account(s) that will be used to attempt communication with the found endpoints. You may add one or more accounts for each discovery query.
- k. **Enable Auto-Import:** *(All)* Check this box to enable the results of this query to be automatically imported and created as managed records. This applies to newly discovered hosts only.
- l. **Record Type for Auto-Import:** *(All)* Select the Record Type that will be used when creating the auto-imported hosts. This record type will be applied to all auto-imported hosts.

- m. **Folder for Auto-Import:** *(All)* Select the container where the hosts will be automatically imported into. If left empty, all discovered hosts will be imported into the System Root Folder.
- n. **Auto-Import Filter:** The auto-import process will only import records that contain either the Windows Service or Service Account (Log On As or Run As...) that is selected by this provided filter.
- o. **Account Type for Auto-Import:** *(All)* This parameter defines which account will be associated with the discovered record during the auto-import process. The following options are available:
  - **Use connected account:** Auto-import process will use the account successfully connected to the destination host during discovery process as an account on record.
  - **Use referenced account:** Auto-import process will use the specified referenced record as an account on record. Use this option when several discovered and imported records reference the same account.
  - **Use provided account:** Auto-import process will use the specified account as an account on record. Use this option to associate specific account with the newly imported records. Typically, a record type shadow account is used to set password for the imported record.
- p. **Reference Record for Auto-Import:** *(Use referenced account)* Auto-import process will use the specified record as a referenced record for all imported records. Typically, this option is used when several imported records should reference the same account (such as Windows domain Administrator).
- q. **Account for Auto-Import:** *(Use provided account)* Auto-import process will use the specified account as an account on record for all imported records (for example, Windows local Administrator). Typically, record type shadow account will be used to set password for the specified account upon record creation.
- r. **Record Type for Local Accounts:** *(All)* This parameter defines a Record type for the records imported to the system from the discovered accounts when copying discovered account to the vault manually or using automatic import process. Discovered accounts refer to all or privileged accounts detected on the end-point after initial login in addition to the account used to discover the end-point. Leave this parameter blank to disable auto-importing of discovered account even when auto-importing the end-point host.
- s. **Filter for Local Accounts:** *(All)* This parameter defines a regular expression filter for the discovered accounts when copying discovered account to the vault using automatic import process. Discovered accounts refer to all privileged accounts detected on the end-point after initial login in addition to the account used to discover the end-point. Filter example to auto import all local accounts started with Admin: `^Admin(.*)`. Leave this parameter blank to auto-import all discovered accounts.
- t. **Record Name Pattern:** This optional parameter defines a name pattern for records imported from this Discovery Query. The following placeholders are supported:
  - `${name}` - Name
  - `${host}` - Host Name
  - `${host.short}` - Short Host Name
  - `${account}` - Account
  - `${user}` - Account without Domain
- u. **Auto-Import Name Check:** *(Active Directory query only)* Check this box to enable the [hostname verification check](#) prior to auto-import. If the checks succeeds, the record will be imported; if the

check fails, the record will not be imported and a message will be added to the report.

- v. **Enable Query:** (All) Check this box to enable the query. Uncheck to disable the query.
  - w. **Sample:** (Active Directory Query, CSV-Based Query) Click the sample button to generate a sample configuration that can be used as a template for proper configuration.
5. Check the **Enabled** option to enable the query or leave it unchecked for it to remain disabled.
  6. Click the **Save** button when finished.

## Discovery Query Reports

How to review a Discovery Query report:

1. Login to PAM using a System Administrator account.
2. Navigate to Administration > Discovery.
3. Next to any Discovery Query that has already been completed, click the **View** button to open this query's report.

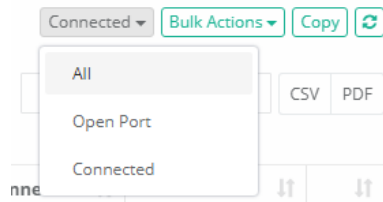
### Queries

Found 3 queries.

[Restart](#) [Enable](#) [Disable](#) [Add Query](#) [Refresh](#)

	Name	Scan Type	Filter	Protocols	Enabled	Actions
<input type="checkbox"/>	IP Discovery	IP Range	10.0.0.1 - 10.0.0.255	PowerShell,SSH		<a href="#">Edit</a> <a href="#">View</a>
<input type="checkbox"/>	IT Admin Scan	IP Range	10.0.0.1 - 10.0.0.255	PowerShell,SSH	✓	<a href="#">Edit</a> <a href="#">View</a>
<input type="checkbox"/>	IP Range Discovery	IP Range	10.0.0.1 - 10.0.0.255	PowerShell	✓	<a href="#">Edit</a> <a href="#">View</a>

4. When the report loads, you the filter option along the top to choose your report view. The following options are available as a filter:



- a. **All:** Displays all the endpoints that were found regardless of the response.
  - b. **Open Port:** Displays the endpoints that were found with an open port (PowerShell or SSH) regardless of the response.
  - c. **Connected:** Displays all the endpoints that were found and communication was successfully established using one of the Accounts provided in the Query.
5. Use the Search box to locate a specific endpoint and use the CSV or PDF options to export the results to a file.

# Discovery Query Report Actions

The following information and actions can be taken from the Discovery Query Report.

1. You can learn additional information about the endpoint by clicking its **View** button. This may provide information about the endpoint’s connection time, status, Operating System, Administrators group membership, custom Services and more.

Showing 1 to 2 of 2 entries

	Host	OS	Protocol	Status	Created	Last Logon	Last Attempt	Last Connected	User	
<input type="checkbox"/>	10.0.0.60	Microsoft Windows Server 2012 R2 Standard	PowerShell	Connected	09/26/2017 13:04:13		04/23/2018 09:09:32	04/23/2018 09:09:47	contractor@xt.com	View
<input type="checkbox"/>	10.0.0.24	Microsoft Windows Server 2012 R2 Standard	PowerShell	Connected	07/11/2017 09:11:28		04/27/2018 01:19:02	04/27/2018 01:19:12	contractor@xt.com	View

First Previous 1 Next Last

2. **Search** to locate specific endpoints and export results to either a CSV or PDF file.
3. **Sort** report based on column headers to more easily organize and locate privileged endpoints.
4. Automatically create new managed records from *Connected* endpoints by selecting its row(s), clicking the **Copy** button and then Pasting it to an appropriate location in your System Records. Please note that the ability to create records from Discovered endpoints is only available when its Status is *Connected*.

Showing 1 to 2 of 2 entries

	Host	OS	Protocol	Status	Created	Last Logon	Last Attempt	Last Connected	User	
<input type="checkbox"/>	10.0.0.60	Microsoft Windows Server 2012 R2 Standard	PowerShell	Connected	09/26/2017 13:04:13		04/23/2018 09:09:32	04/23/2018 09:09:47	contractor@xt.com	View
<input type="checkbox"/>	10.0.0.24	Microsoft Windows Server 2012 R2 Standard	PowerShell	Connected	07/11/2017 09:11:28		04/27/2018 01:19:02	04/27/2018 01:19:12	contractor@xt.com	View

First Previous 1 Next Last

# Discovery Query Schedule

By default, Discovery Queries are configured to be run every 120 minutes.

New queries will be added to the job queue when saved; however existing queries that are edited will not be updated in the queue.

At any time, you may select a query or multiple queries and click the **Restart** button to add them to the queue for processing.

To update the default query schedule:

1. Login to PAM using a System Administrator account.
2. Navigate to Administration > Settings.
3. On the Application Nodes tab, click on the node defined as the Worker to open its configuration.

Found 2 nodes.

Node	Message Queue	Discovery	Notification	Job Queue	Render Queue	Scheduling	Aggregation	Session
ckdell:GUI 2.3.201804261736 / 04/27/2018 09:42	Idle: 0.5						Idle: 30	Idle: 5
ckdell:Worker 2.3.201804261736 / 04/27/2018 09:41	Idle: 0.5	Pool: 5 Idle: 2	Pool: 5 Idle: 5	Pool: 5 Idle: 0.5	Pool: 5 Idle: 0.5	Idle: 120		

4. Locate the option labeled **Discovery** and modify its value as needed. Value is based on minutes between scans.



	Idle Time	Pool Size
Message Queue	30	
Discovery	120	5
Notification	300	5

- Click the **Save** button when finished.

## AWS EC2 Discovery

Privileged Access Management Discovery Queries for Amazon EC2 Instances.

As more businesses begin or continue to move critical infrastructure to cloud systems like AWS, the security to find, access and manipulate these services becomes ever increasing and vital.

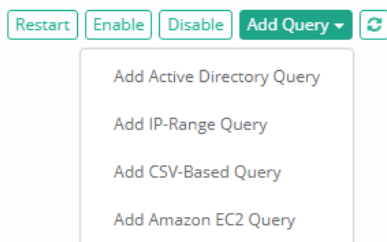
Using Privileged Access Management, administrators can discover these instances, secure access to them, rotate their SSH keys and enable auditing and recording to ensure only trusted users can access these critical, cloud based systems.

In addition, the Auto-Import option will create Records for newly discovered hosts.

In this article, the Discovery process to allow authorized Administrators the ability to automatically detect these instances will be described.

### Configure Privileged Asset Discovery for AWS EC2 Instances:

- Login to PAM using a System Administrator account.
- Navigate to Administration > Discovery.
- Create a new Discovery query by clicking the **Add Query** button and then select **Add Amazon EC2 Query**.



- A new Amazon EC2 Discovery configuration page will appear with the following options:
  - Name:** The name of the discovery query.
  - Access Key:** Enter the Access Key to be used for connecting to AWS.
  - Secret Key:** Enter the Secret Key associated to the Access Key, to be used for connecting to AWS.
  - Host Field:** Select the value that will be displayed in the Host Field when compiling the Discovery Report.

- e. **Name Field:** Select the value that will be displayed in the Name Field when compiling the Discovery Report.
- f. **Regions:** Check all the regions that are to be included in the discovery scan. At least one region must be checked.
- g. **Use PowerShell:** Check the box to enable the use of PowerShell for the scan (for Windows endpoints). *Only PowerShell or SSH can be selected per query. If you would like to use both Protocols, then a second query must be created.*
- h. **Use SSH:** Check the box to enable the use of SSH for the scan (for Unix or Linux based endpoints). *Only PowerShell or SSH can be selected per query. If you would like to use both Protocols, then a second query must be created.*
- i. **Non-Standard Ports:** Comma-separated list of non-standard ports to try during host discovery. If not specified the discovery process will attempt to connect to a remote host using port 22 for the SSH protocol and to the WS-Management port 5985 for the PowerShell protocol.
- j. **Accounts:** Enter the account(s) that will be used to attempt communication with the found endpoints. You may add one or more accounts for each discovery query and can specify either a Password or Private Key.
- k. **Enable Auto-Import:** Check this box to enable the results of this query to be automatically imported and created as managed records. This applies to newly discovered hosts only.
- l. **Record Type for Auto-Import:** Select the Record Type that will be used when creating the auto-imported hosts. This record type will be applied to all auto-imported hosts.
- m. **Folder for Auto-Import:** Select the container where the hosts will be automatically imported into. If left empty, all discovered hosts will be imported into the System Root Folder.
- n. **Auto-Import Filter:** The auto-import process will only import records that contain either the Windows Service or Service Account (Log On As or Run As...) that is selected by this provided filter.
- o. **Account Type for Auto-Import:** (All) This parameter defines which account will be associated with the discovered record during the auto-import process. The following options are available:
  - Use connected account: Auto-import process will use the account successfully connected to the destination host during discovery process as an account on record.
  - Use referenced account: Auto-import process will use the specified referenced record as an account on record. Use this option when several discovered and imported records reference the same account.
  - Use provided account: Auto-import process will use the specified account as an account on record. Use this option to associate specific account with the newly imported records. Typically, a record type shadow account is used to set password for the imported record.
- p. **Reference Record for Auto-Import:** (Use referenced account) Auto-import process will use the specified record as a referenced record for all imported records. Typically, this option is used when several imported records should reference the same account (such as Windows domain Administrator).
- q. **Account for Auto-Import:** (Use provided account) Auto-import process will use the specified account as an account on record for all imported records (for example, Windows local Administrator). Typically, record type shadow account will be used to set password for the specified account upon record creation.

r. **Enable Query:** Check this box to enable the query. Uncheck to disable the query.

5. Click the **Save** button when finished.

#### Queries

Found 2 queries.

[Restart](#) [Enable](#) [Disable](#) [Add Query](#) [Refresh](#)

	Name	Scan Type	Filter	Protocols	Last Scan	Enabled	Actions
<input type="checkbox"/>	AWS 01	Amazon EC2		PowerShell,SSH	09/28/2018 08:21:00	✓	<a href="#">Edit</a> <a href="#">View</a>
<input type="checkbox"/>	Admin	Active Directory		PowerShell			<a href="#">Edit</a> <a href="#">View</a>

## Command Control

Command Control in Privileged Access Management offers Administrators the ability to restrict commands that can be executed via a **whitelist** or **blacklist** in both Windows and Unix remote sessions.

In addition to the command restrictions themselves, Command Control can also place restrictions on command Arguments and what can, cannot or is required to be “piped” to commands.

The following use cases and scenarios are covered when *Command Control* is implemented in the System.

1. Restrict the types of commands that can be executed in both Windows and Unix based remote sessions. Forbid users from executing a shutdown command or only permit users to execute service restart commands.
2. Restrict command arguments and what can be piped into commands to provide further flexibility. This allows users to execute a wide range of commands while restricting their use to a limited set of arguments (allow, deny or require).
3. Prevent specific applications from being launched through the use of **whitelist** and **blacklist** catalogs. A common need is to prevent server jumping.
4. Inhibit the ability of users to view, extract or modify critical or sensitive content. Prevent your sensitive systems from (un)intentional abuse and your sensitive content from being distributed.

To configure [Command Control in PAM \(Getting Start Guide\)](#)

## Command Control Policies

Command Control offers Administrators the ability to limit commands that can be executed via a [whitelist](#) or [blacklist](#) in both Windows and Unix remote in-browser sessions.

In addition to the command restrictions themselves, *Command Control* can also place restrictions on command Arguments and what can, cannot or is required to be “piped” to commands.

Special forbidden sequences and meta-commands are run under Command Control policies.

## Create Command Control Policies

Any user who has been granted the global System Administrator role may access and modify the Command Control policies, located at Administration > Command Control.

To create a new policy, navigate to Administration > Command Control and click the **Create** button.

Create your policy by entering the values as required.

Name	Enter a unique, but descriptive name of your policy. When applying the policy, the user will be selecting your policy by name only from a dropdown menu.
Description	Enter a description for your policy.
Control Type	Select either <i>Whitelist</i> or <i>Blacklist</i> .

Next, click the **Add Command** button to begin configuring your white- or blacklist policy.

Command	Enter the command to be included in this policy.
Add/Remove Argument	Optionally, add or remove argument(s) to be included with the command.
Type	Select the <i>Include</i> or <i>Exclude</i> option that will pertain to the above argument.

For example, if you want to restrict commands for your Cisco device so that the user may only execute *show version* (i.e. whitelist), the following configuration can be used:

Command	show
Add/Remove Argument	version
Type	Include

You may repeat the process to add additional commands to this policy or click **Save** to complete the policy creation.

## Edit or Delete Command Control Policies

To edit or delete an existing policy, navigate to Administration > Command Control and click the **Edit** or **Delete** button next to your desired policy.

If editing a policy, be sure to click the **Save** button when you are finished with your modifications.

# Apply Command Control Policies

Command Control policies are applied to Record Types or individual Records to ensure user commands are limited when remote sessions are active.

## *Apply Policies to Record Types*

Applying the Command Control policy to a Record Type allows for the policy to be inherited down to all records that make use of this type. To apply the policy to a Record Type:

1. Navigate to Administration > Record Type and click the **Edit** button for the desired *Record Type*.
2. On the Record Type's Edit page, click the **Command** button.
3. On the Command Control page, click the **Add** button.
4. Enter a principal(s) that should have the policy applied and then click the **Add** button.
5. Select the desired policy by name from the **Command Control** dropdown menu.
6. Click the **Select** button to apply the policy.
7. Review the policy as configured and finally click the **Save** button to apply it to the *Record Type*.  
To remove a policy, select the applied Policy by checking the box to its left and then clicking the **Remove** button.  
Finally, click the **Save** button to finalize the update.

## *Apply Policies to Records*

Applying the Command Control policy to an individual Record allows for the policy to be relevant for a specific host or user rather than for all hosts.

### **To apply the policy to a Record:**

1. Navigate to the record and choose the option Manage > Command Control.
2. If the inheritance is not already broken, then click the **Make Unique** button.
3. On the Command Control page, click the **Add** button.
4. Enter a principal(s) that should have the policy applied and then click the **Add** button.
5. Select the desired policy by name from the **Command Control** dropdown menu.
6. Click the **Select** button to apply the policy.
7. Review the policy as configured and finally click the **Save** button to apply it to the *Record*.  
To remove a policy, select the applied Policy by checking the box to its left and then clicking the **Remove** button.  
Finally, click the **Save** button to finalize the update.

# Getting Started with Command Control Policies

This guide is designed for System Administrators to learn about PAM Command Control and how it can be used to govern which commands can or cannot be executed by users during remote sessions.

To complete the guide be sure that you have access to a PAM System Administrator account.

This Guide will be broken into two parts.

The first part will describe how to setup a basic whitelist command policy and the second part will describe how to setup a blacklist command policy.

In the attempt to keep this guide short and quick, we will demonstrate the functionality and provide screenshots using a Windows Host remote session, but please keep in mind that the same setup can be applied to a Unix Host remote session as well.

[Jump to Whitelist Command Policy](#)

[Jump to Blacklist Command Policy](#)

## Whitelist Command Policy

In the whitelist scenario, we want to permit a user to login to a production server, but limit their ability to execute only certain commands.

For this, we are going to implement a whitelist policy to include the command **iisreset** and then apply this policy to both this user and the production server.

Finally, we will login to this policy controlled remote session to demonstrate how it will work from a user's perspective.

[1. Creating a Command Control Policy](#)

[2. Applying the Policy to a Record](#)

[3. Executing Commands in a Policy Controlled Session](#)

### *Stage 1: Creating a Command Control Policy*

Command Control policies are used to define which command(s) and arguments are to be added to either a whitelist or blacklist.

1. Login to PAM as a System Administrator and navigate to Administrator > Command Control.
2. Click the **Create** button.
3. Enter a user recognizable name in the **Name** field (required).
4. Enter a description into the **Description** field (optional).
5. In the *Control Type* dropdown menu, select *Whitelist*.
6. Click the **Add Command** button.
7. In the Command field, type the command *iisreset*.

- Click the **Save** button.

Command Control Details: IIS Reset Policy

Save Cancel

Name IIS Reset Policy

Description Whitelist iisreset

Control Type Whitelist

Command iisreset Add Argument Remove Command

Type Include Include Exclude

Add Command

Your Command Control Policy is now created.

## Stage 2: Applying the Policy to a Record

Command Control policies are applied to records to ensure user commands are controlled when remote sessions are active.

- Navigate and open a Windows Host or Unix Host record that you wish to apply this policy to. *You must be a PAM Administrator or an Owner on the record to assign or configure Command Controls.*
- Click the **Manage** dropdown menu and then select the **Command Controls** option.
- Click the **Add** button.
- Enter your PAM Administrator (or another test account) in the Principal field and click **Add**.
- In the Command Control dropdown menu select the Command Control Policy by name that was created in Stage 1 of this guide.
- Click the **Select** button.

## Assign Command Control

### Principal ?

Add

### Selected Principals

John Williams ▾

### Command Control

IIS Reset Policy ▾

CancelSelect

7. The Command Control Policy will appear in the list. If you had another policy, you could repeat this process as many times as needed. When complete, click the **Save** button to assign the policy to this record.

### Commands Controls for Windows Host (internal)

Inherit from ParentSaveAddRemove↺

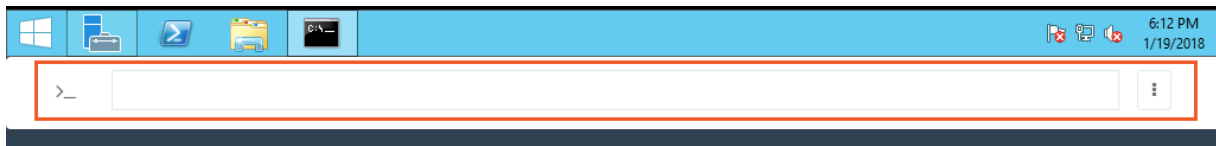
Principal	Principal Type	Policy
<input type="checkbox"/> John Williams (john)	User	IIS Reset Policy

Your record now has the Command Control Policy assigned to it.

## Stage 3: Executing Commands in a Policy Controlled Session

Now that we created the policy and assigned it to both our user and a record, it's time to Connect to this remote session and see how Command Control actually works.

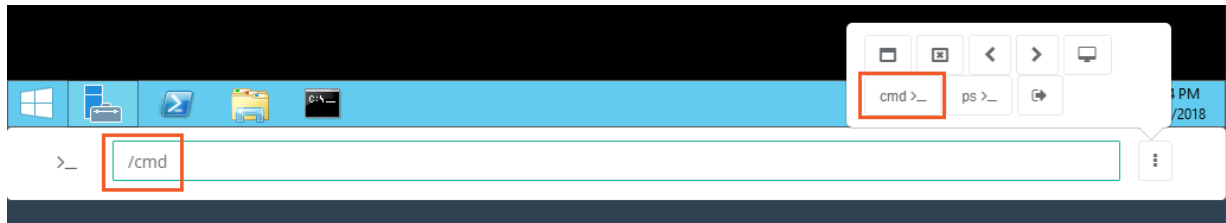
1. Return back to the record used in Stage 2 and click the *Connect* button. *Command Control is supported in sessions with or without recording enabled.*
2. Once successfully connected to your Windows session, you should immediately realize that mouse control is disabled. This is to prevent the user from interfacing with the host outside of our whitelisted command(s). When a session is being controlled using a Command Control Policy, the user will only be able to issue commands using the PAM's command input field located at the bottom of the session window and the actual session will be used to provide feedback.



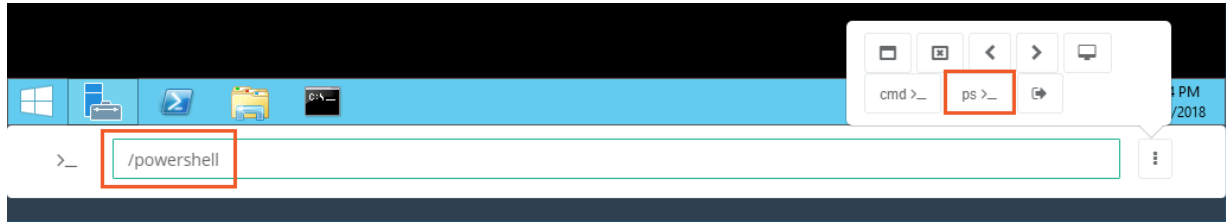
3. To open a command prompt or PowerShell prompt, either enter the following commands or use the following quick launch options.



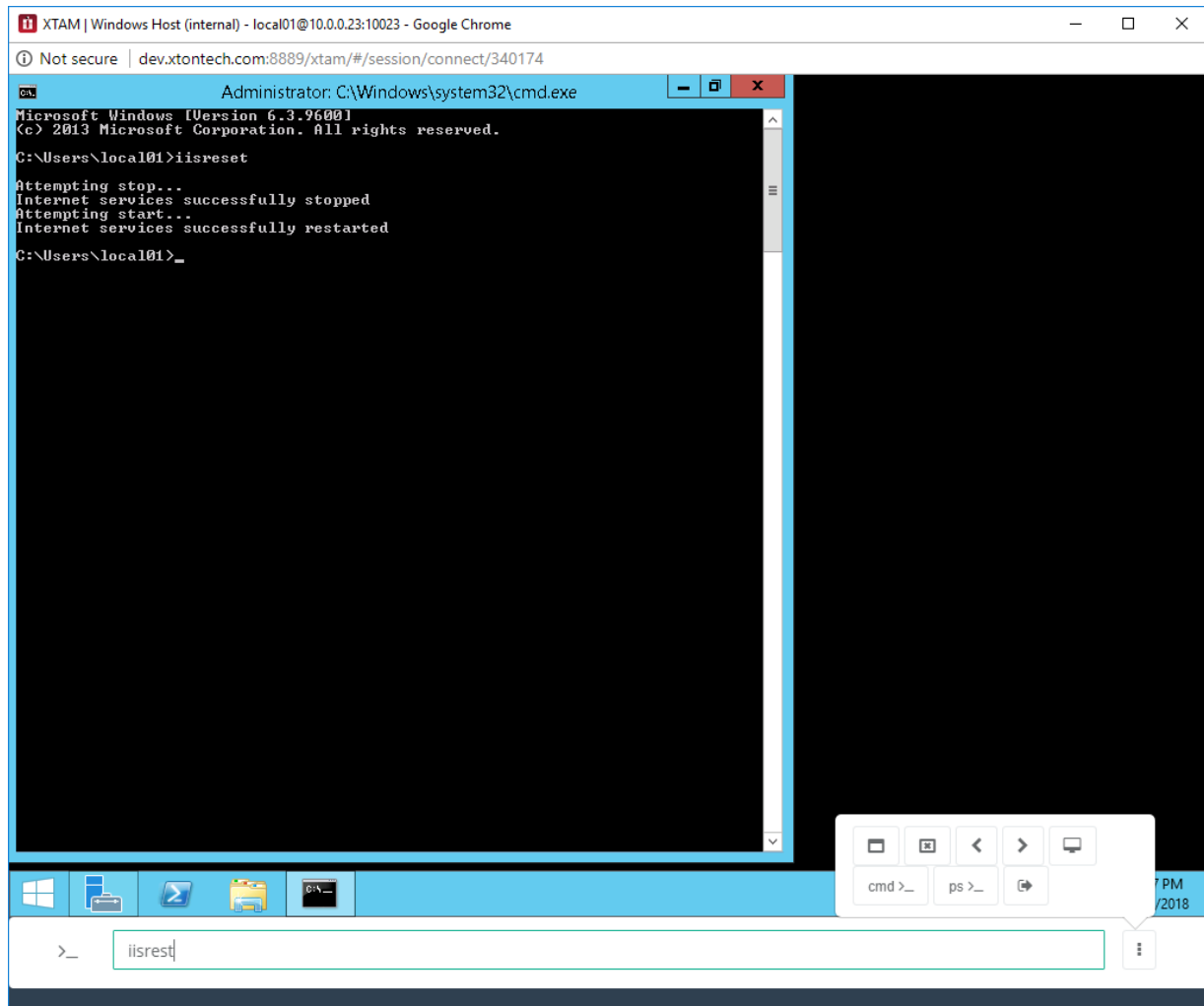
- a. For Command Prompt, type the command `/cmd` or select the `cmd >_` option from the command menu.



- b. For PowerShell, type the *command* `/powershell` or select the `ps >_` option from the command menu.



4. When the application opens, enter your whitelisted command (`iisreset`) into the input field and hit the Enter key to execute the command. The command will be sent to command prompt or PowerShell and be executed. The results will display in the application just as if you typed them natively. The command was sent and executed because it was included in our Whitelist policy.

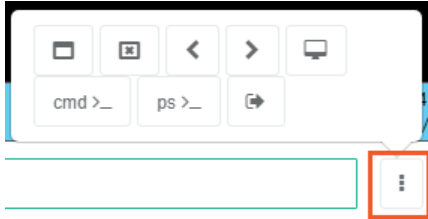


- Commands not included in Whitelist will naturally be forbidden, so let's now test that. Enter any command besides `iisreset` into the input field and hit the **Enter** key. Rather than sending and executing your typed command, the input field clears the command and displays the message *Command forbidden by policy*.

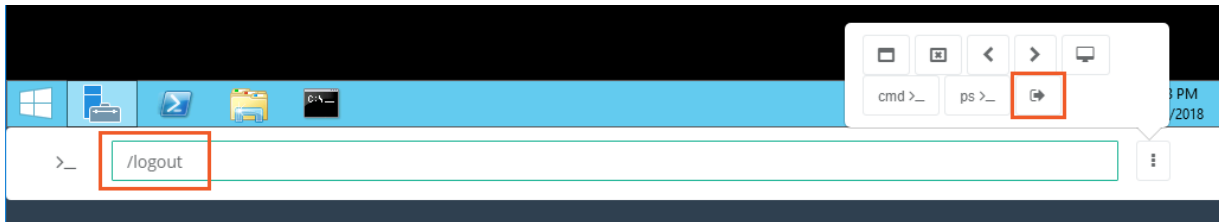
>\_

Command forbidden by policy

- Before disconnecting the session, explore the other options displayed in the Command menu to become familiar with the Quick Launch options.



- When you are finished, you can disconnect your remote session by either executing the `/logout` command or select the *logout* option from the command menu.



## Blacklist Command Policy

In the blacklist scenario, we want to permit a user to login to a production server, but limit their ability to open a remote desktop session to another server (commonly referred to as Server Jumping).

For this, we are going to implement a blacklist policy to include the command `mstsc` and then apply this policy to both this user and the production server.

Finally, we will login to this policy controlled remote session to demonstrate how it will work from a user's perspective.

[1. Creating a Command Control Policy](#)

[2. Applying the Policy to a Record](#)

[3. Executing Commands in a Policy Controlled Session](#)

### Stage 1: Creating a Command Control Policy

Command Control policies are used to define which command(s) and arguments are to be added to either a whitelist or blacklist.

- Login to PAM as a System Administrator and navigate to Administrator > Command Control.
- Click the **Create** button.
- Enter a user recognizable name in the **Name** field (required).
- Enter a description into the **Description** field (optional).
- In the **Control Type** dropdown menu, select *Blacklist*.
- Click the **Add Command** button.

7. In the **Command** field, type the command `mstsc`.
8. In the **Type** dropdown menu select *Include/Exclude* (optional).
9. Click the **Save** button.

---

Command Control Details: Server Jumping

---

Save Cancel

---

Name	Server Jumping	
Description	Prevent RDP sessions	
Control Type	Blacklist ▼	

---

Command	mstsc	Add Argument
		Remove Command
Type	Include ▼	

Add Command

Your Command Control Policy is now created.

## Stage 2: Applying the Policy to a Record

Command Control policies are applied to records to ensure user commands are controlled when remote sessions are active.

1. Navigate and open a Windows Host or Unix Host record that you wish to apply this policy to. *You must be a PAM Administrator or an Owner on the record to assign or configure Command Controls.*
2. Click the **Manage** dropdown menu and then select the **Command Controls** option.
3. Click the **Add** button.
4. Enter your PAM Administrator (or another test account) in the Principal field and click **Add**.
5. In the Command Control dropdown menu select the Command Control Policy by name that was created in Stage 1 of this guide.
6. Click the **Select** button.

## Assign Command Control

### Principal ?

Add

### Selected Principals

John Williams ▾

### Command Control

Server Jumping ▾

CancelSelect

7. The Command Control Policy will appear in the list. If you had another policy, you could repeat this process as many times as needed. When complete, click the **Save** button to assign the policy to this record.

Commands Controls for Windows Host (internal)

Inherit from ParentSaveAddRemove

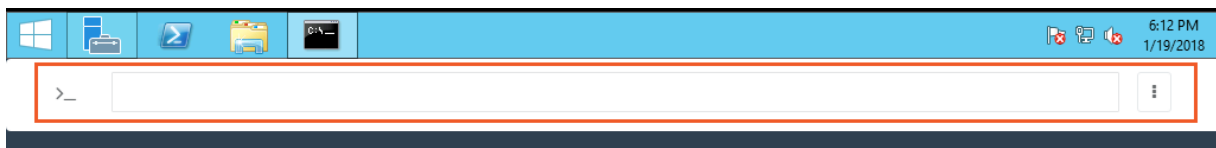
Principal	Principal Type	Policy
<input type="checkbox"/> John Williams (john)	User	Server Jumping

Your record now has the Command Control Policy assigned to it.

### Stage 3: Executing Commands in a Policy Controlled Session

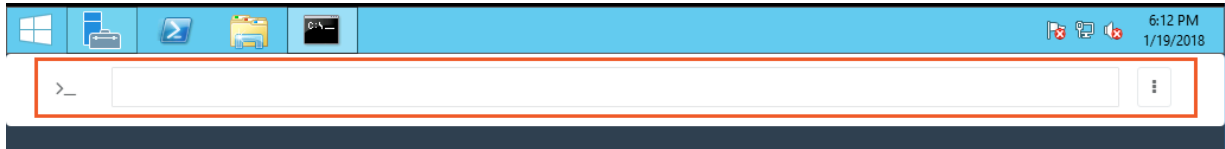
Now that we created the policy and assigned it to both our user and a record, it's time to Connect to this remote session and see how Command Control actually works.

1. Return back to the record used in Stage 2 and click the **Connect** button. *Command Control is supported in sessions with or without recording enabled.*
2. Once successfully connected to your Windows session, you should immediately realize that mouse control is disabled. This is to prevent the user from interfacing with the host outside of our whitelisted command(s). When a session is being controlled using a Command Control Policy, the user will only be able to issue commands using the System's command input field located at the bottom of the session window and the actual session will be used to provide feedback.

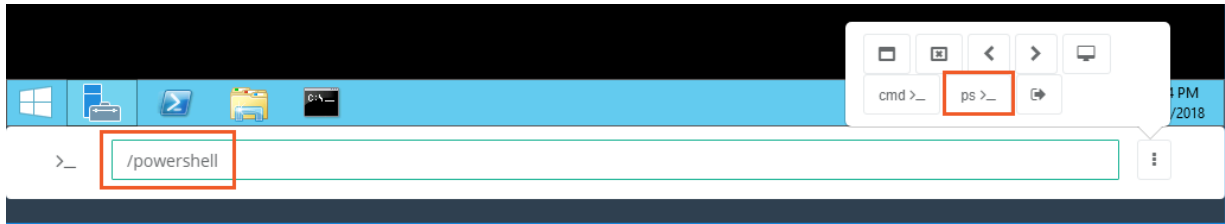


3. To open a command prompt or PowerShell prompt, either enter the following commands or use the following quick launch options.

- a. For Command Prompt, type the command `/cmd` or select the `cmd` option from the command menu.



- b. For PowerShell, type the command `/powershell` or select the `ps` option from the command menu.

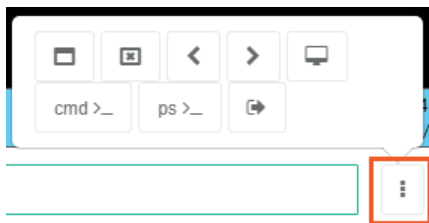


4. When the application opens, enter your blacklisted command (`mstsc`) into the input field and hit the **Enter** key to execute the command.

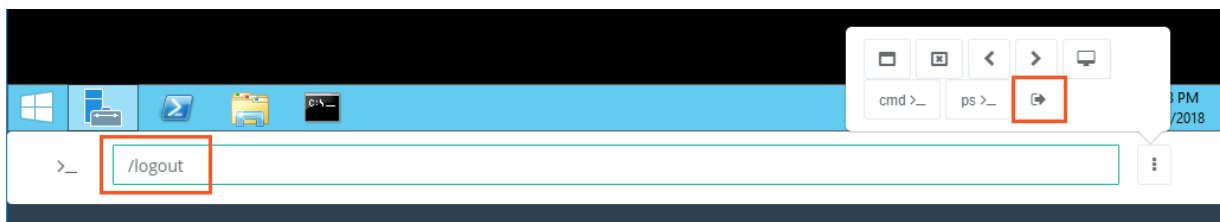
Rather than sending and executing your typed `mstsc` command, the input field clears the command and displays the message *Command forbidden by policy*. The command was not sent and executed because it was included in our Blacklist policy.



5. Commands not included in Blacklist will naturally be permitted, so let's now test that. Enter any command besides `mstsc` into the input field and hit the **Enter** key. The command will be sent to command prompt or PowerShell and be executed. The results will display in the application just as if you typed them natively. The command was sent and executed because it was not included in our Blacklist policy.
6. Before disconnecting the session, explore the other options displayed in the Command menu to become familiar with the Quick Launch options.



7. When you are finished, you can disconnect your remote session by either executing the `/logout` command or select the *logout* option from the command menu.



# MFA Configuration

This Multi-factor Authentication (MFA) page allows System Administrators to enable specific, possibly different, MFA providers on an individual user or group basis.

Additionally, a *default* MFA provider can be configured that requires all users to authenticate using that same provider with the option to exclude individuals (direct login without requiring MFA).

NOTE: The general use of MFA authentication in PAM requires certain **pre-requisites** to be installed and configured on the host server. Please review the MFA guides located on our website for information regarding these requirements.

**To assign an MFA provider to a user or group:**

1. Navigate to Administration > MFA and click the **Add** button.

## Multi-factor Authentication


Home / Multi-factor Authentication

MFA Configuration

Found 1 entries.

Add

Delete



Show 

50

 entries

CSV PDF XLSX PDF Protected CSV Protected XLSX Protected

Search:

Showing 1 to 1 of 1 entries

User	Provider	Enabled	Actions
<input type="checkbox"/> Service Administrator (pamadmin) /Local	none		<div>...</div>

First

Previous

1

Next

Last

2. On the New Multi-factor Authentication page, configure your MFA as required.

Default	When selected, this specific configuration becomes the default MFA provider for all users or groups. In turn, the specific users or groups added separately then become exceptions to this default provider.
Principals	User or Group to assign to this provider.  This Principals option is removed when the <i>Default</i> option is enabled because default applies to all principals.

Provider	<p>Select the MFA provider from those available in the dropdown list.</p> <p>The list of providers in this menu is populated based on the MFA integration(s) that have been established with PAM.</p> <p>Of note, the <i>none</i> option will result in no MFA authentication being required for the selected principals and the <i>mfa-generic</i> option is used exclusively for token enforcement during SSH Proxy sessions only.</p>
----------	--

New

☐
Default ?

Brian Williams (bwilliams) /Local ▼

Provider ?

Select Provider ▼

Select Provider  
mfa-azuread  
mfa-confirmid  
mfa-duo  
**mfa-gauth**  
mfa-generic  
mfa-radius  
mfa-yubikey  
none

3. Click the **Save** button to complete your MFA configuration.

#### To edit an MFA provider assignment for a user or group:

1. Navigate to Administration > MFA, locate the entry you want to update, open its *Actions* menu and select the **Edit** option.
2. On the Edit Multi-factor Authentication page, update the configuration as needed.
3. Click the **Save** button to complete your updated MFA configuration.

Success!

MFA method successfully updated.

OK

#### To delete an MFA provider assignment for a user or group:

1. Navigate to Administration > MFA, locate the entry you want to delete, open its *Actions* menu and select the **Delete** option. For a bulk delete option, check the box next to each entry you want to delete and then click the **Delete** button located above the Search box.
2. Click the **OK** button on the confirmation dialog to complete the removal of the selected MFA configuration.

## Defining MFA per User or Group

If you want to enable different MFA providers for different users or groups, please review the following guide for configuration steps.

A common scenario, would be that you want internal users to use your default Duo MFA provider (or no MFA requirement at all), while external contractors are forced to use a free alternative like [Google Authenticator](#).

### To Configure Unique MFA Provider Requirements

For the purposes of this article, it is assumed that you have already configured the required [Federated Sign-in Module](#) and integrated with your [MFA provider\(s\)](#). If you have not yet performed these required steps, please read the appropriate articles and return here when ready.

1. Login to PAM with a System Administrator account.
2. Navigate to Administration > MFA.
3. Configure your user and group mapping as required. Use the *Add*, *Edit* and *Delete* option to manage the list of users or groups. For each user or group, select the desired MFA option from the dropdown. For ease of use, if you wish to apply the same MFA provider for all users, simply check the **Default** option and then your single Provider.

Note that the System pre-populates this table with all current system administrators (users or groups) with *Provider*: none meaning that system admins will not require MFA. You might want to change or retain this default configuration depending on your requirements.

4. Login to PAM host server and open the file `$PAM_HOME/web/conf/catalina.properties` in a text editor.
5. Locate and comment out (put a # before the line) all the line(s) that begin with the below:

Please note that this may include several lines.

```
1 | cas.authn.mfa.globalProviderId=mfa-
```

6. Enable granular MFA configuration in the `$PAM_HOME/web/conf/catalina.properties` by uncommenting the line for parameter:



- a. for Federated Sign in v5.2x:

```
1 | cas.authn.mfa.groovyScript=.../web/webapps/pam/WEB-INF/mfa/xtam-  
   | mfa.groovy
```

- b. for Federated Sign in v6.5:

```
1 | cas.authn.mfa.groovyScript.location=.../web/webapps/pam/WEB-INF/mfa/xtam-  
   | mfa.groovy
```

Depending on PAM host server, the path above (shortened to ...) will be different.

7. **Save and close** the file `$PAM_HOME/web/conf/catalina.properties`
8. **Restart** the **PamManagement** service (Windows) or the **pammanager** service (Linux) to complete the configuration.

## Reset a User's GAuth MFA Token

If you need to reset a user's GAuth MFA token because they failed to complete or they wish to redo the registration process, please perform the following procedure.

Please note that this option is only supported for user's that have been configured to use the default MFA Provider **mfa-gauth**.

1. Login to PAM with a System Administrator account.
2. Navigate to Report Center > Users.
3. Locate this user in the report (you should see a value in their MFA Token column), then from the actions menu (...) select the option **Reset GAuth Token**.
4. Ask the user to log in to rerun the MFA registration process.

Object	Event	MFA Token	Directory	
All	444	gauth	Local	...
13	26			View Audit Log
All	3			Personal Vault
1	8			Remove Duplicate Entries
	8			Reset GAuth Token
				Block User

If questions remain or issues arise while using PAM, please contact the Support team:

<https://support.imprivata.com/communitylogin>.

# Google Authenticator

How to login to Privileged Access Management as a User.

The experience for users who must use Google multi-factor authentication (MFA) to login is slightly different than the traditional style of username and password entry that they are probably accustomed to.

Although not drastically different, the following procedure must be performed by every user whose account is configured to use Google MFA in PAM.

In order to use Google MFA, you will need to download and install the Google Authenticator to your mobile device.

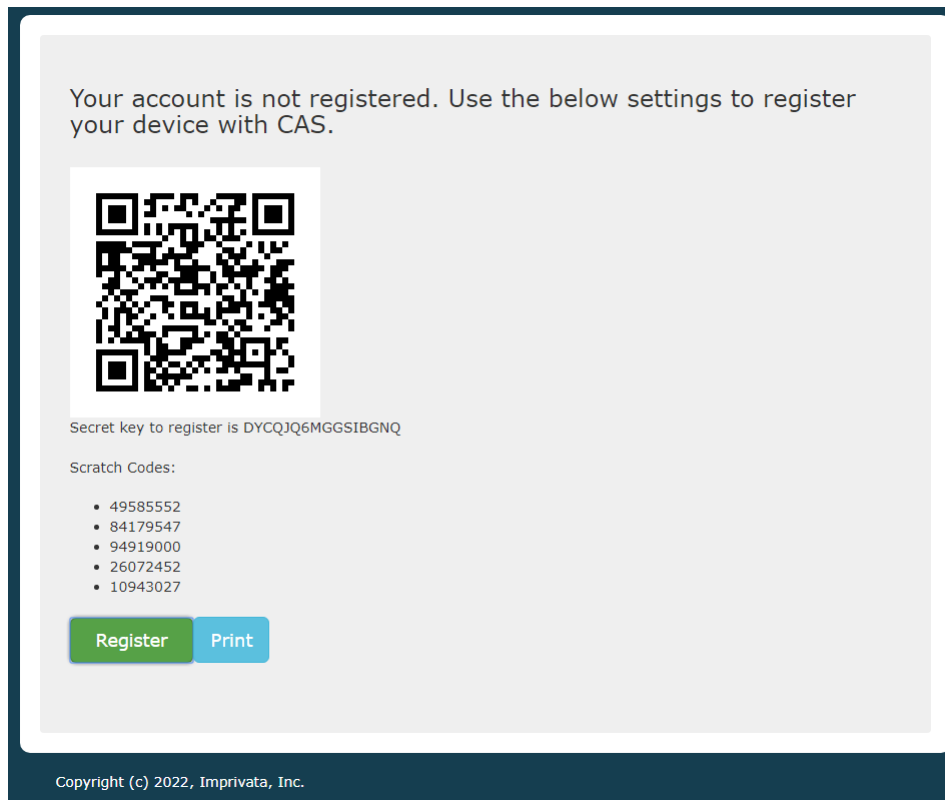
Please do this before continuing.



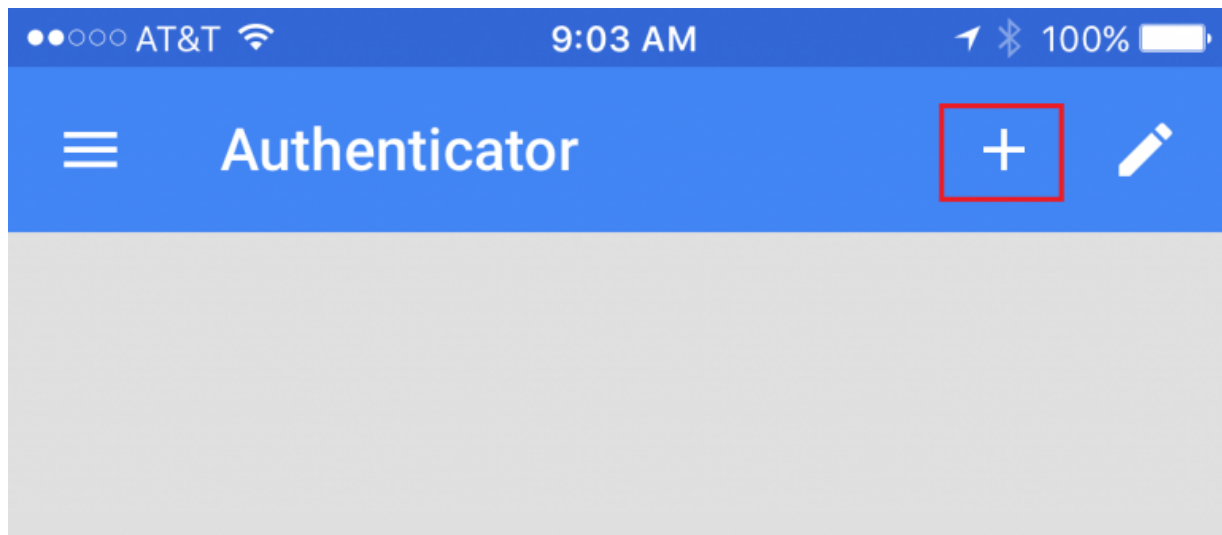
1. Open your browser to Imprivata Privileged Access Management's login page.
2. Enter your username and password into their login fields and click **Login** when ready to continue. If you are unsure of your login, try your default network login. If that does not work, please contact your PAM System administrator for further assistance.

A screenshot of the Imprivata Privileged Access Management login page. The page has a dark blue background. On the left, there is a light gray login form. At the top of the form, it says "Log in to Imprivata Privileged Access Management" with a lock icon below it. The form contains two input fields: "Username:" with the text "chrisk" and "Password:" with masked characters. Below these fields is a green "Log in" button. Under the button is a link "Forgot your password?". At the bottom of the form, there is a security notice: "For security reasons, please log out and exit your web browser when you are done accessing services that require authentication!". On the right side of the page, there is a light gray box titled "Links to Additional Resources" containing two links: "Documentation" and "Contact Imprivata Support". At the bottom left of the page, the copyright notice "Copyright (c) 2022, Imprivata, Inc." is displayed.

3. After clicking **Login**, a new page in your browser will display the necessary information required to configure your Google Authenticator app for the first time.



4. Open the Google Authenticator app on your mobile device now. Click the **Add** button in the Google Authenticator mobile app.



5. Select either the **Scan barcode** or **Manual entry** option along the bottom.



- a. If you selected the **Scan barcode** option, simply point your phone's camera at the barcode in your computer's browser. In a second or two, the App will scan the barcode and automatically configure your app.

- b. If you selected the **Manual entry** option, enter your PAM username into the Account field and enter the **Secret Key** into the app's **Key** field. Click the **Done** button when it is complete.

●●○○ AT&T 9:05 AM 100%

← Manual entry ✓

Account

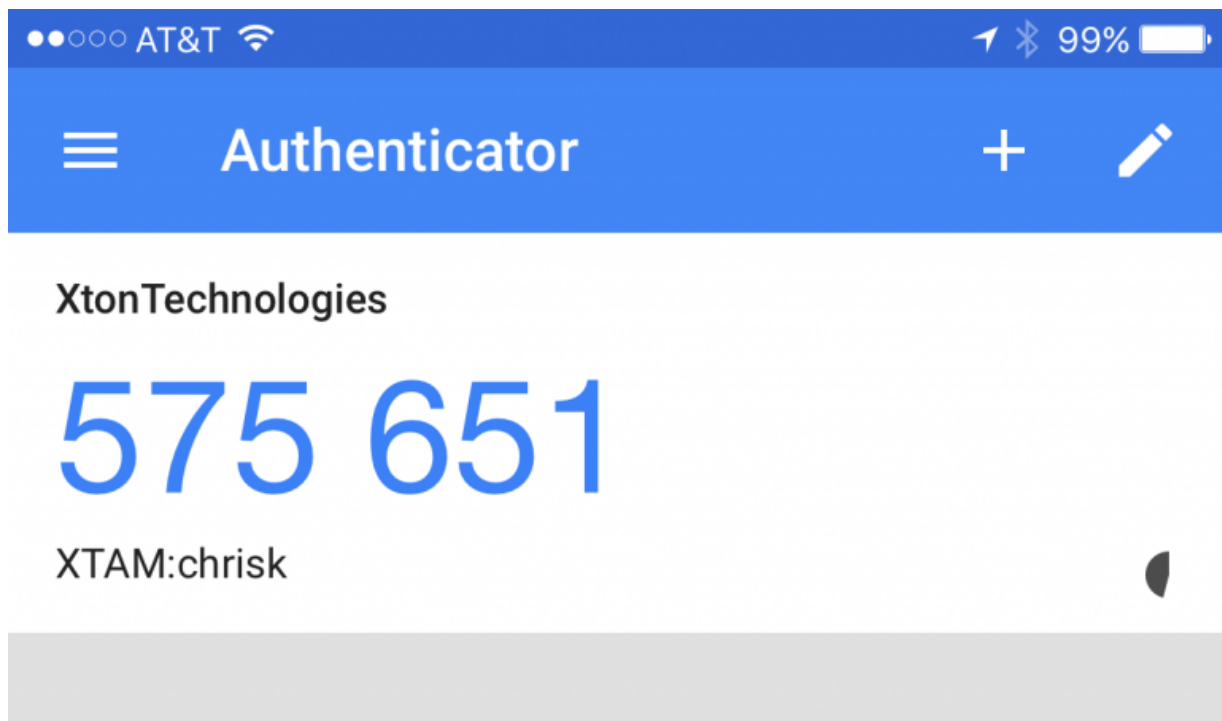
chrisk

Key

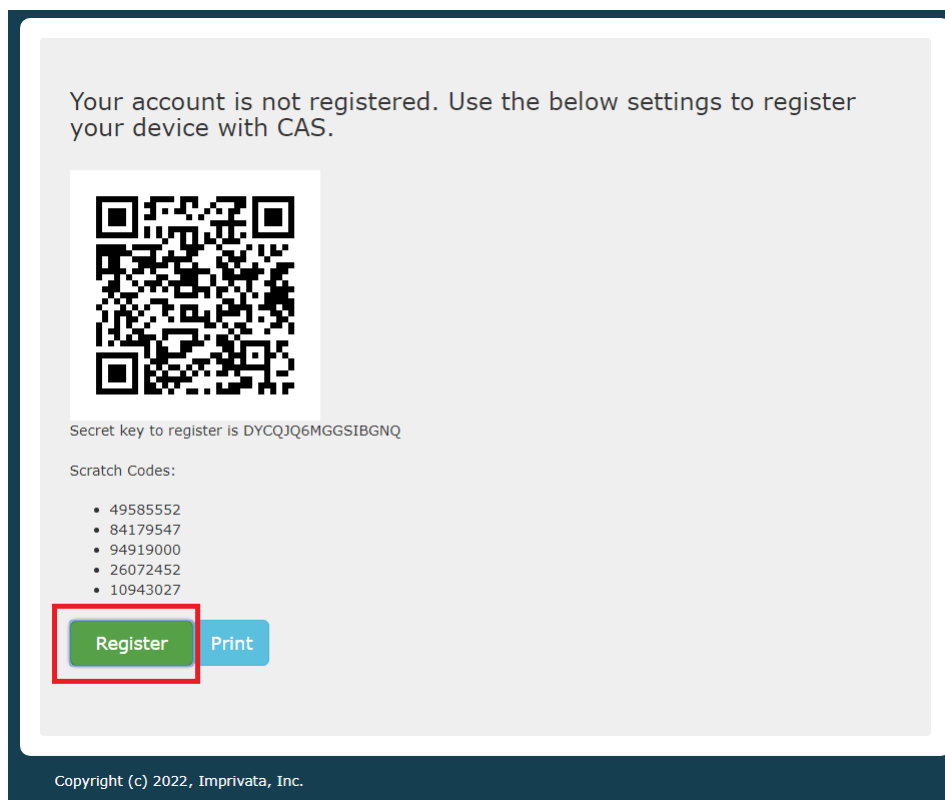
DYCQJQ6MGGSIBGNQ

Time based ☒

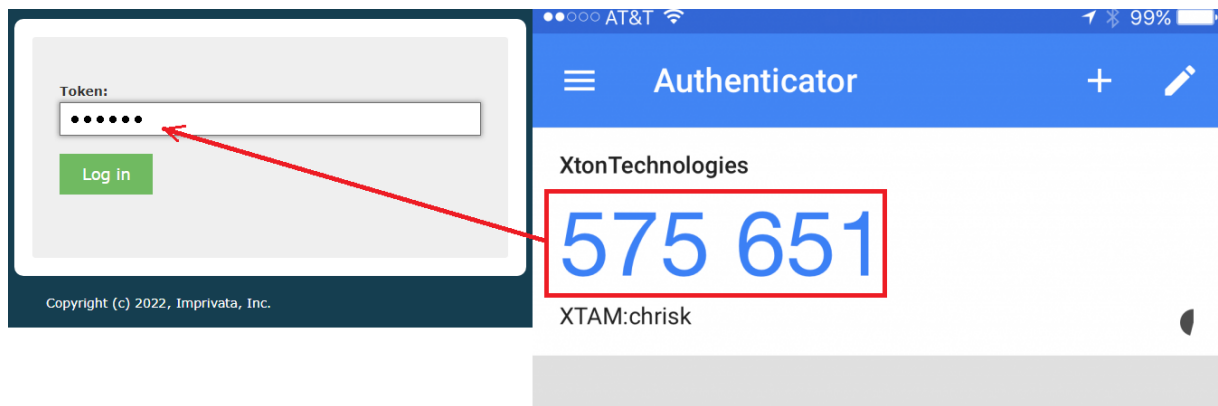
6. The app will now redirect back to its main page where your connection to PAM will be displayed.



7. Return to your computer's browser that is displaying the Barcode and click the **Register** button.



8. On the next page, enter the 6 digit code that is displayed on your mobile device's Google Authentication app into the **Token** field in your browser.



9. Click **Login** when complete. Please note that these 6 digit codes are time based, so if you take too long to enter and login, the code in the App will refresh and you will then need to enter the new one in order to login successfully.
10. You are now logged into your PAM.  
For subsequent logins, you will not need to re-register your mobile device, but you will be required to open the Google Authenticator app and enter the 6 digit code into the Token field in order to login.

## MFA Configuration Options

### Integration

PAM supports RADIUS for authentication which most MFA providers utilize in their own solutions; therefore many MFA products can be successfully integrated with Imprivata Privileged Access Management.

If you have a specific MFA or 2FA provider that you would like to inquire about, have questions or need guidance, please contact us using the information provided in our documentation site.

If questions remain or issues arise while using PAM, please contact our Support team:

<https://support.imprivata.com/communitylogin>.

Privileged Access Management integrates with your existing MFA provider, it does not provide its own service. Therefore, you will need to follow the configuration guides below before you can configure your MFA usage in PAM. This includes deploying the required [Federated Sign-In Module](#) as well as having an Administrative account with your MFA provider.

**For specific MFA providers**, please review the links below:

[Duo Security MFA – How to Configure \(Admin\)](#)

[Duo Security MFA – How to Login \(Users\)](#)

[Google Authenticator \(or other TOTP providers\) – How to Configure \(Admin\)](#)

[Google Authenticator \(or other TOTP providers\) – How to Login \(Users\)](#)

[RADIUS – How to Configure \(Admin\)](#)

### Configuration Options

The MFA Configuration Options allows a PAM System Administrator to determine which users or groups will have to authenticate using their MFA provider in order to login.

The following options are available:

To start using MFA, please first read [enabling granular control over MFA configuration for different users or groups of users](#) article to configure PAM to support this feature.

**Add:** Select a user or group that will be added to PAM MFA configuration.

**Edit:** Modify PAM MFA configuration of the selected user or group.

**Delete:** Remove the selected user or group from PAM MFA configuration.

**Default:** When selected, this specific configuration becomes the default MFA provider for all users or groups. In turn, the specific users or groups added then become exceptions to this default.

**Principal:** The user or group that will be bound to this configuration. Principal is removed when the *Default* option is enabled because default applies to all principals.

**MFA Provider:** The selected provider that will be bound to this principal. The list of providers is populated based on the MFA integration(s) that have been established with PAM. Select the *none* option, if you want the principal to login without requiring MFA authentication.

# Multi-factor Authentication ?

Home / Multi-factor Authentication

MFA Configuration

Found 1 entries.

Add

Delete

Show 50 entries

CSV PDF XLSX PDF Protected CSV Protected XLSX Protected

Search:

Showing 1 to 1 of 1 entries

User	Provider	Enabled	Actions
<input type="checkbox"/> Service Administrator (pamadmin) /Local	none		...

First

Previous

1

Next

Last

The mfa-generic provider option enforces the requirement of a mfa token when a user establishes a [desktop client SSH Proxy](#) , RDP Proxy, and Oracle Proxy sessions only; it does not generate mfa tokens for any other login or connection purposes. These mfa generic tokens are generated in Management > My Profile > Preferences > MFA Code and have a 3 minute expiration time.



By default, all principals with the *System Administrator* role are added with no (*none*) MFA provider configured. This is done to prevent accidental lock out if the MFA integration or configuration is mis-configured. You may change this default behavior if needed.

## MFA Grace Period

PAM can be configured to allow for a grace period when a user does not receive a native MFA challenge after their initial successful authentication. For security reasons, it is not recommended to enable this *MFA Grace Period*, however there are some Use Cases and Administrators that may wish to support the user convenience benefits over the security benefits of MFA.

When MFA Grace Period is enabled, the following scenarios will only require a first successful MFA token, after which, the user will not be prompted to provide it again during the time of their defined Grace Period:

- MFA required Workflow actions like *Unlock* or *Connect*
- Proxy Session authentication like *SSH* and *RDP*.

When MFA Grace Period is enabled, the following scenarios will still require a successful MFA token during every attempt:

- Logins to PAM Web Portal
- SSO (SAML) logins to PAM will enforce their defined MFA policy as configured in the SSO provider.

To enable **MFA Grace Period** the following configuration parameters are available and must be configured identically on each Master node in your PAM deployment. In the `catalina.properties` file, add the following new lines and configure each **<parameter>** to meet your requirements. After each file is updated, a PAM service restart of each node is required.

```
1 | #MFA Grace Period
2 | xtam.cas.mfa.bypass.enabled=<true or false>
3 | xtam.cas.mfa.bypass.seconds=<Grace Period Time in Seconds>
4 | xtam.cas.mfa.bypass.ipRange=<Bypass Only for Connections from the Comma Separated
   | Specified IP Ranges>
5 | xtam.cas.mfa.bypass.sharedIp=<disabled or enabled>
```

**xtam.cas.mfa.bypass.enabled**=*true* or *false*

Use *true* to enable MFA Grace Period and *false* to disable. This parameter is required.

**xtam.cas.mfa.bypass.seconds**=<Grace Period Time in Seconds>

Define the amount of time, in seconds, that limits the Grace Period. The grace period begins after the user successfully provides their initial MFA token in the supported scenarios described above. For example, a defined value of **28800** would mean after the user's first successful MFA validation, they would not be prompted again for 8 hours. This parameter is required.

**xtam.cas.mfa.bypass.ipRange**=<Bypass Only for Connections from the Comma Separated Specified IP Ranges>

Define a comma separated list of IP ranges that will enforce the Grace Period. Users from within these IP ranges will fall into the defined Grace Period parameters, while others outside of these ranges will continue to be prompted for MFA. This parameter is optional and if not needed, may be removed, or commented out.

**xtam.cas.mfa.bypass.sharedIp=disabled** or **enabled**

MFA Grace Period uses a combination of the username and their IP address (at the time of their initial authentication) to determine if this user has previously provided a successful MFA authentication. In the scenario where all users are reported from the same IP address to PAM, this option will allow an Administrator to enable the shared IP configuration. It is not recommended to enable this option unless absolutely necessary. This parameter is required.

When **enabled**, multiple users presenting from the same IP address will be included in the Grace Period.

When **disabled**, multiple users presenting from the same IP address will be prompted for MFA regardless of the enabled Grace Period configuration.

## MFA Login as a User

The experience for users who must use Duo multi-factor authentication (MFA) to login is slightly different than the traditional style of username and password entry that they are probably accustomed to.

Although not drastically different, the following procedure must be performed by every user whose account is configured to use Duo MFA in Imprivata Privileged Access Management.


In order to use Duo MFA, you will need to download and install the Duo Mobile app to your device.

Please do this before continuing.



1. Open your browser to the Imprivata Privileged Access Management's login page.
2. Enter your username and password into their login fields and click **Login** when ready to continue. If you are unsure of your login, try your default network login. If that does not work, please contact your System administrator for further assistance.

## Log in to Imprivata Privileged Access Management



**Username:**

**Password:**

Log in

[Forgot your password?](#)

For security reasons, please [log out](#) and exit your web browser when you are done accessing services that require authentication!


### Links to Additional Resources

[Documentation](#)

[Contact Imprivata Support](#)

Copyright (c) 2022, Imprivata, Inc.

- After clicking Login, a new page in your browser will display the beginning of the setup process. Click the **Start setup** button to begin.



[What is this?](#) [Need help?](#)

Powered by Duo Security

## Protect Your Xton Technologies Account

Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. This prevents anyone but you from accessing your account, even if they know your password.

This process will help you set up your account with this added layer of security.

Start setup

- Select the type of device you will be adding to your Duo account that in turn will be used to authenticate and login to PAM. Click the **Continue** button to continue.

**XT**

[What is this?](#) [Need help?](#)

Powered by Duo Security

### What type of device are you adding?

- ☒ **Mobile phone** RECOMMENDED
- ☐ **Tablet** (iPad, Nexus 7, etc.)
- ☐ **Landline**
- ☐ **U2F token**

**Continue**

5. Assuming you selected Mobile Phone in the previous step, select your country and then enter your phone number. Click **Continue** to continue.

**XT**

[What is this?](#) [Need help?](#)

Powered by Duo Security

### Enter your phone number

United States ▼

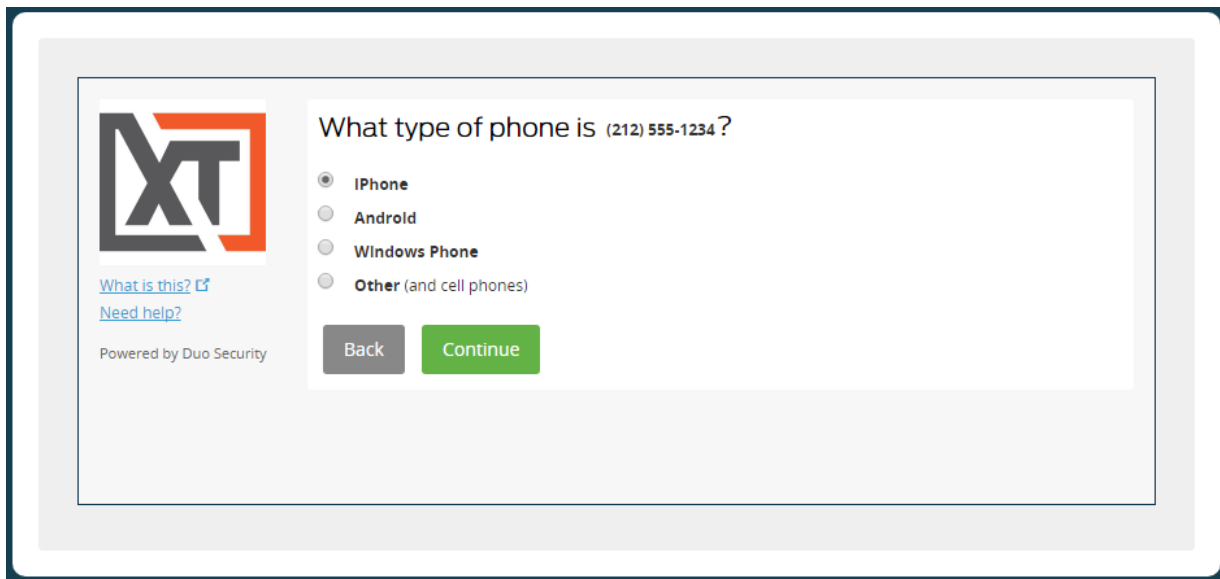
+1 2125551234 ✓

ex: (201) 234-5678

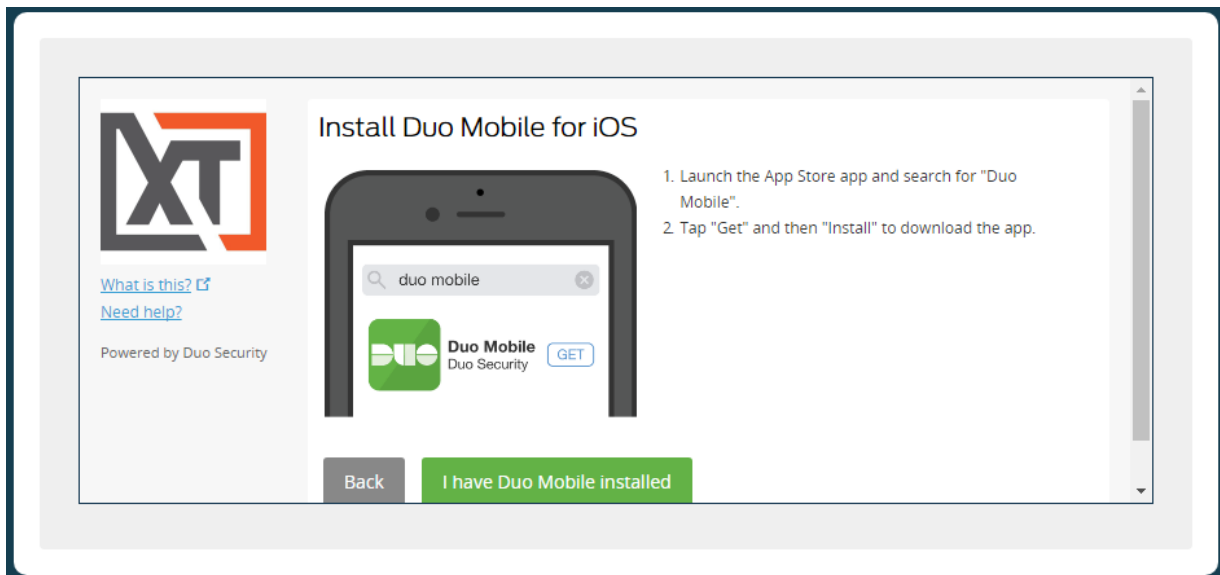
☒ **(212) 555-1234** This is the correct number.

**Back** **Continue**

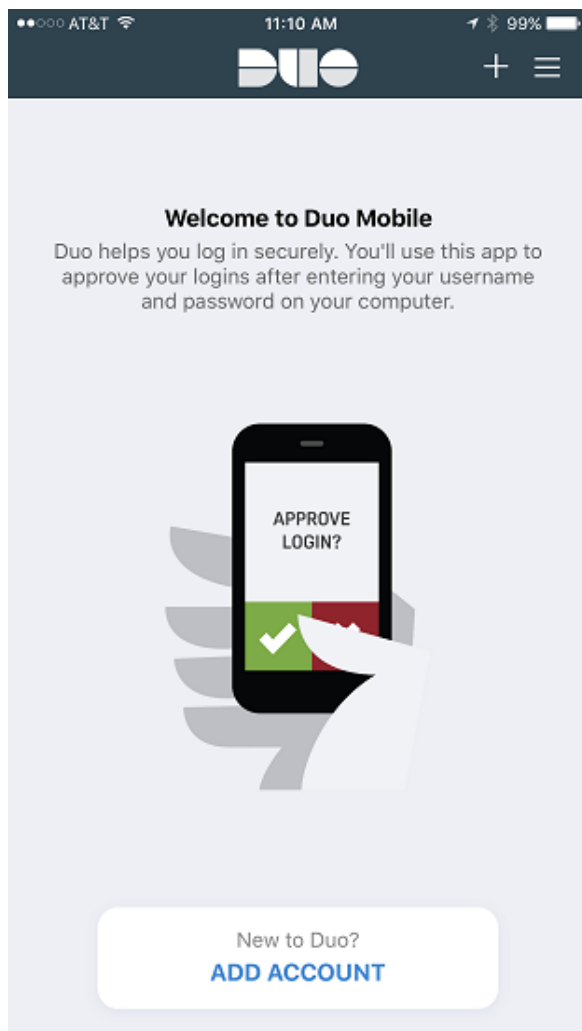
6. Select the type of phone that is associated with your phone number that was entered previously. Click **Continue** to continue.



7. If you have not already, download and install the Duo Mobile app to your device now. When the app is installed, click the **I have Duo Mobile installed** button to continue.



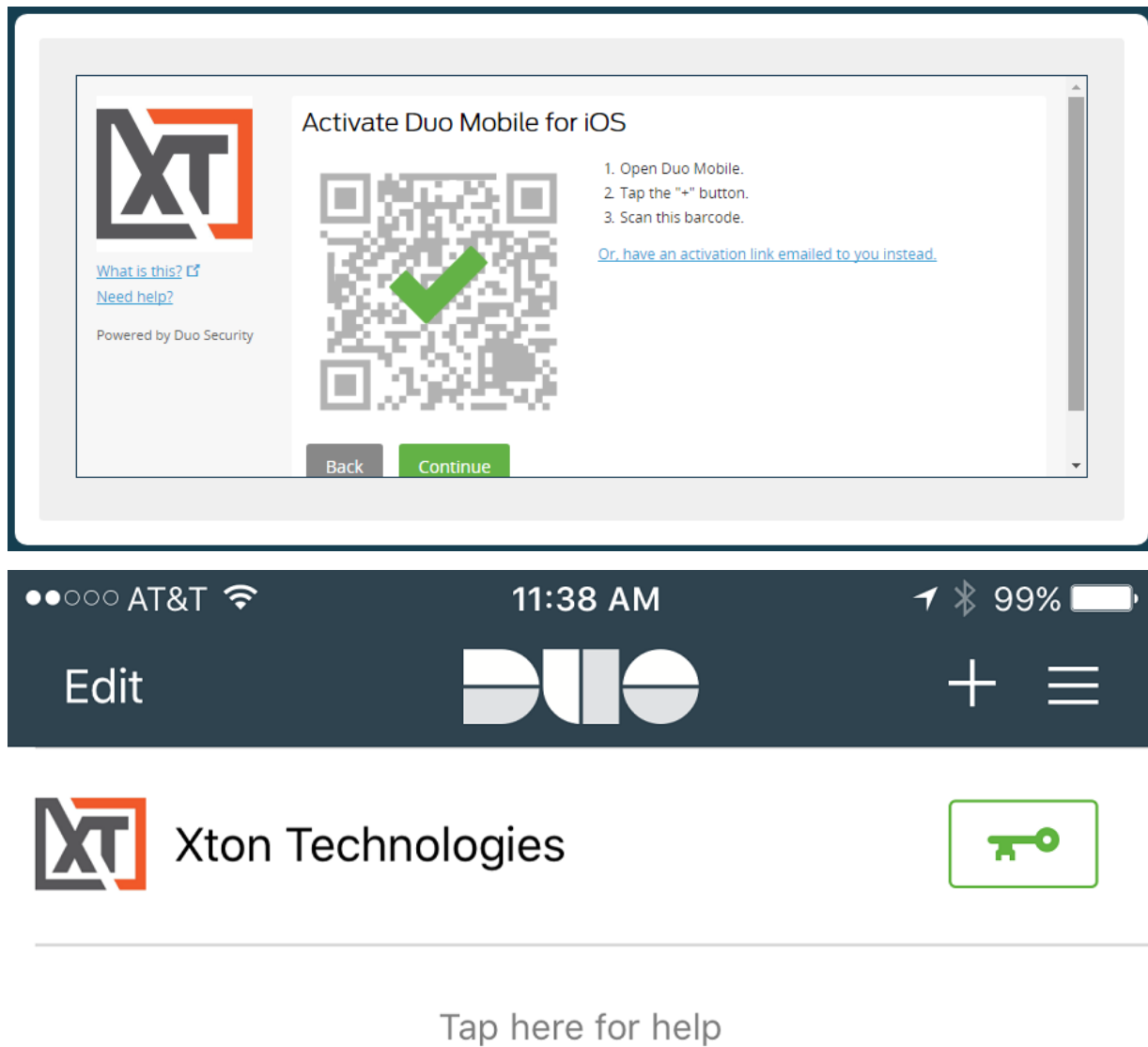
8. This next screen will display the barcode that is required to configure MFA with your device. Before we continue on your computer, open the Duo Mobile app on your device and click the **Add Account** button along the bottom or click the + button to add another account to the app.



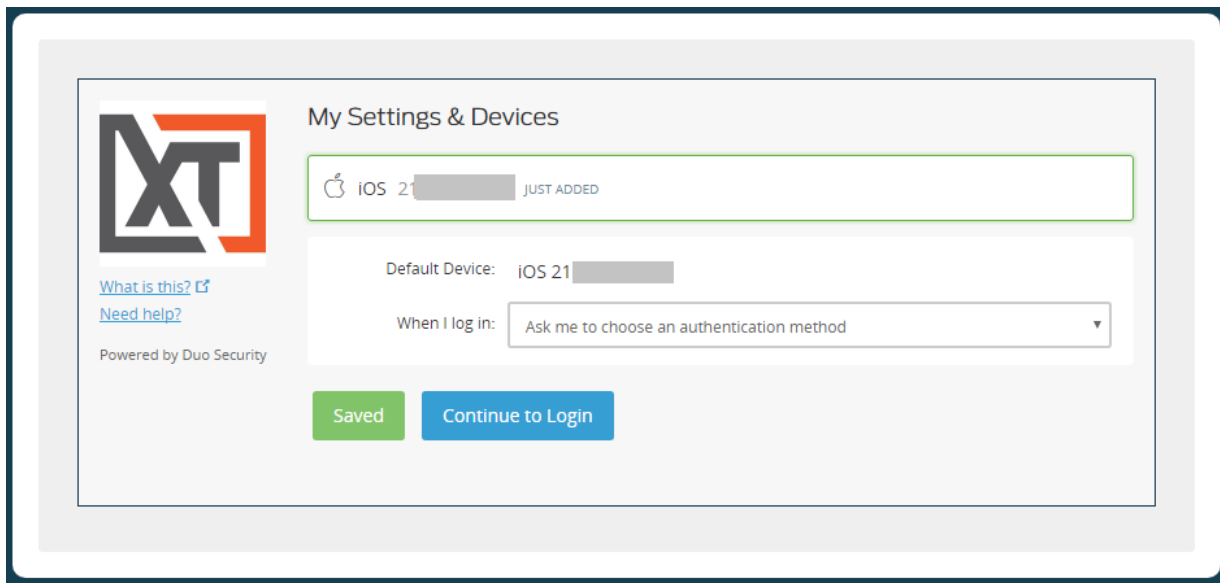
9. Point your device's camera at the barcode in your computer's browser to scan and configure the app.



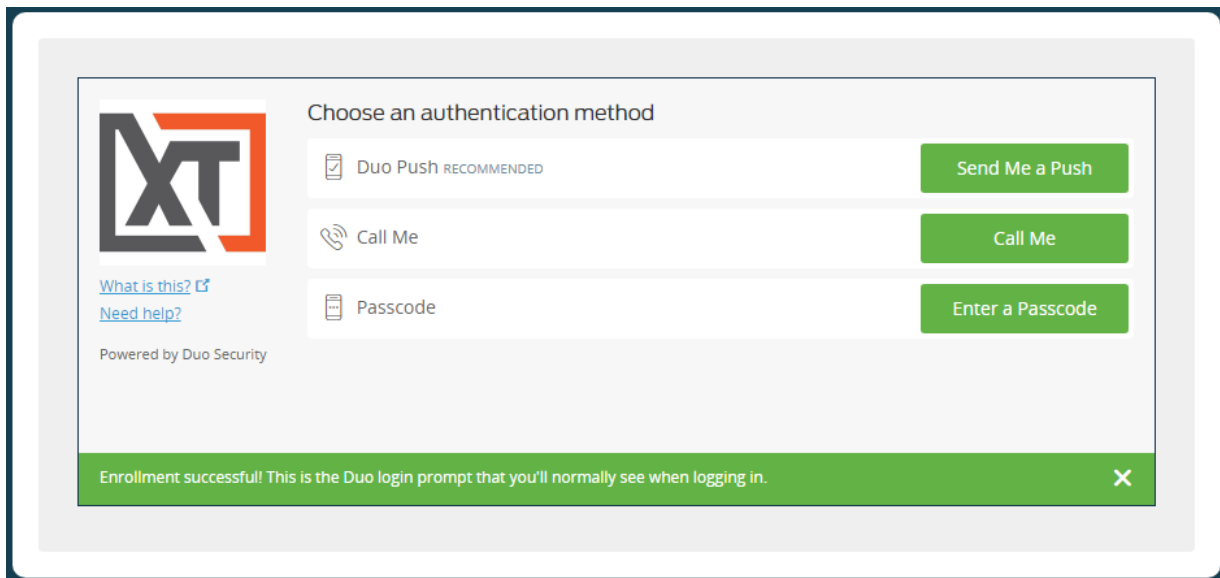
10. After a few seconds, the device and browser will recognize the barcode and show the following success image.



11. Once configured, choose your login options on this page and click **Continue to Login** to continue.



12. Duo Mobile MFA is now configured. This screen will now be your normal login prompt whenever logging into PAM. Select your authentication method by clicking the green button to the right.



13. In this example, we will select the Passcode option by clicking the **Enter a Passcode** button. Open the Duo Mobile app and then press the **Key** button located to the right of your new connection.





Xton Technologies



152694 ⓘ

Tap here for help

14. Enter this *six digit code* from your device's Duo Mobile App into the Log In prompt shown in your computer's browser. Click the **Log In** button to continue.

Choose an authentication method

☒ Duo Push RECOMMENDED Send Me a Push

☐ Call Me Call Me

Log In

[What is this?](#) [Need help?](#)

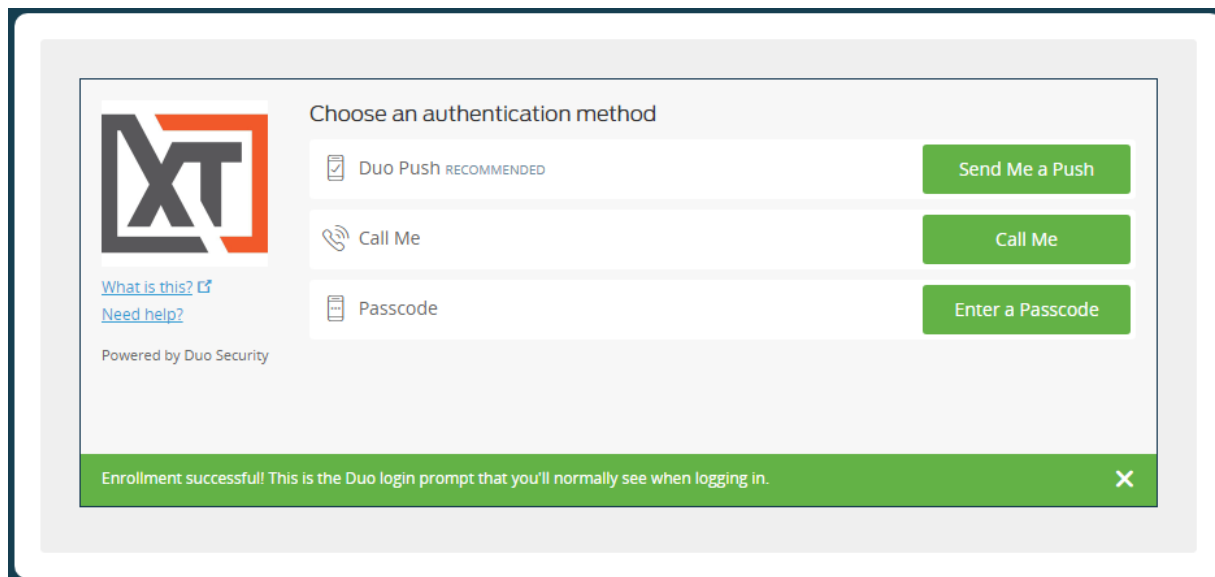
Powered by Duo Security

Enter a passcode from Duo Mobile or a text. Text me new codes ×

15. You are now logged into PAM.

For subsequent logins, you will not need to re-register your mobile device, but you will be required to open the Duo Mobile app and authenticate in order to login.

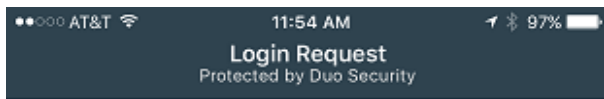
If *Duo Push* is used, then click the Duo Push button **Send Me a Push** at the login prompt and simply click the **Accept** button in the Duo Mobile app to authenticate and login to PAM. You will be automatically logged in to PAM.



The screenshot displays a Duo login prompt interface. On the left, there is a logo with the letters 'XT' in a stylized font, with 'X' in black and 'T' in orange. Below the logo are two links: 'What is this?' and 'Need help?'. Underneath these links, it says 'Powered by Duo Security'. To the right of the logo, the heading 'Choose an authentication method' is displayed. Below this heading, there are three authentication options, each with a corresponding icon and a green button to its right:

- Duo Push** (with a checkmark icon and the word 'RECOMMENDED' in all caps) with a green button labeled 'Send Me a Push'.
- Call Me** (with a telephone handset icon) with a green button labeled 'Call Me'.
- Passcode** (with a document icon) with a green button labeled 'Enter a Passcode'.

At the bottom of the interface, a green banner contains the text: 'Enrollment successful! This is the Duo login prompt that you'll normally see when logging in.' followed by a close button (an 'X' icon).



Xton Technologies



11:54:05 AM EDT  
September 13, 2023



If questions remain or issues arise while using PAM, please contact the Support team:

<https://support.imprivata.com/communitylogin>.

## YubiKey MFA Login as a User

YubiKey MFA: how to login to Privileged Access Management as a User.

The experience for users who must use YubiKey multi-factor authentication (MFA) to login is slightly different than the traditional style of username and password entry that they are probably accustomed to.

Although not drastically different, the following procedure must be performed by every user whose account is configured to require YubiKey MFA in Access Manager.

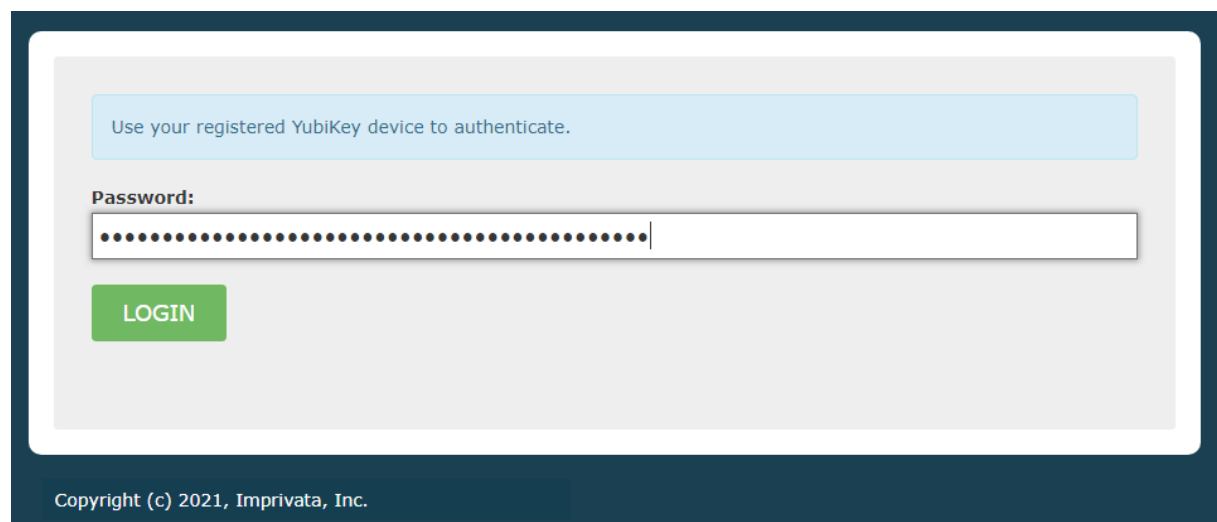
In order to use YubiKey MFA, you will need access to your physical YubiKey device. The following procedure has been tested with both YubiKey version 4 and 5 devices.

1. Open your browser to the Privileged Access Management's login page.
2. Enter your username and password into their login fields and click **Login** when ready to continue. If you are unsure of your login, try your default network login. If that does not work, please contact your PAM administrator for further assistance.

3. After clicking Login, a new page in your browser will display the beginning of your YubiKey registration process. *This is a one-time registration process and you will not be required to perform this step again after your YubiKey is registered.* Click your mouse cursor to the **Token** field and then touch your YubiKey. YubiKey should automatically populate the token value and advance to the next step. If it does not advance, click the **Register** button to continue.

4. After your YubiKey is registered, this next screen will authenticate you into Privileged Access Management. Click your mouse cursor to the **Password** field and then touch your YubiKey. YubiKey

should automatically populate the one time password value and log you into Privileged Access Management. If it does not log you in, click the **Login** button to continue.



Use your registered YubiKey device to authenticate.

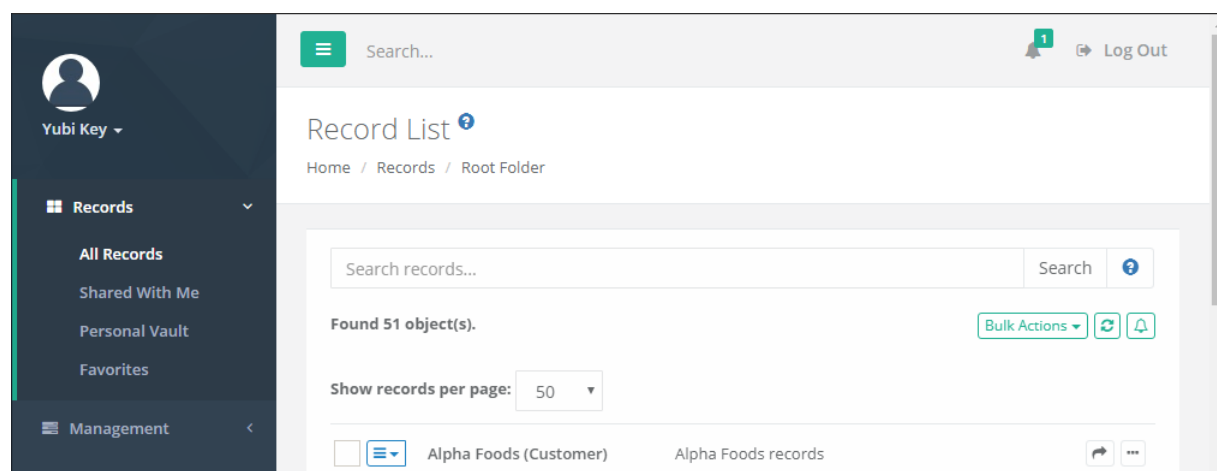
**Password:**

.....

**LOGIN**

Copyright (c) 2021, Imprivata, Inc.

5. You are now logged into the PAM.



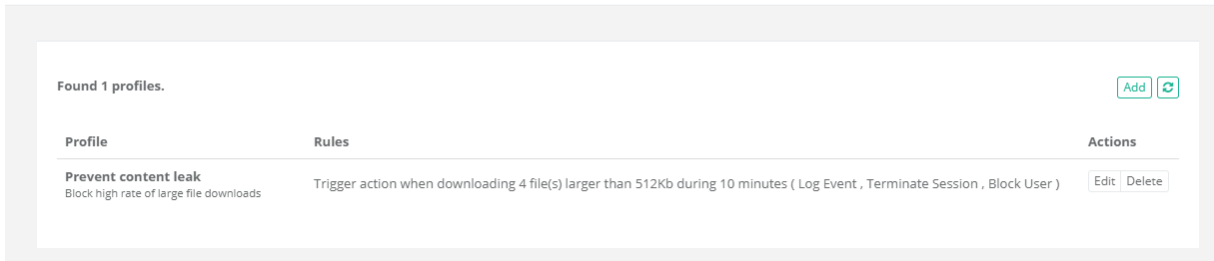
For subsequent logins, you will not need to re-register your YubiKey device, but you will be required to use your YubiKey device in order to login with its one time password (OTP).


## Behavior Profiles and Event Analytics

Behavior profiles allow System Administrators to create custom configurations to take automatic actions based on the behavior profiles of users.

Common examples would be a *Behavior Profile* where a user unlocks too many secrets in a short amount of time or a user frequently downloads files during a remote session.

These behavioral events could then trigger actions such as blocking the user's access or terminating their session, allowing PAM to perform self-monitoring with automated actions.



Found 1 profiles.			<a href="#">Add</a> 
Profile	Rules	Actions	
<b>Prevent content leak</b> Block high rate of large file downloads	Trigger action when downloading 4 file(s) larger than 512Kb during 10 minutes ( Log Event , Terminate Session , Block User )	<a href="#">Edit</a>	<a href="#">Delete</a>

## Create Behavior Profiles

How to create Behavior Profiles:

1. Login to PAM with a System Administrator account. *Only System Administrators may create and manage behavior profiles.*
2. Navigate to Administration > Behavior Profiles.
3. Click the **Add** button to create a new profile.
4. Enter a Name (required) and a Description (optional) for your new profile.
5. Click the **Add Rule** button to create a new rule for this profile.
6. Configure your rule using the below descriptions as guidelines.
  - **Trigger:** Defines the behavior that will automatically trigger the rule's action.
    - *Rule Type:* Select the rule from dropdown menu that will be used to trigger the action.

Please note that depending on the rule type selected, the remaining parameters may contain more or less options.

- *Threshold Count:* This parameter specifies the number of times the selected type of a user's behavior should occur before it triggers execution of the rule's actions.
- *Threshold Size (Kb):* This parameter specifies the minimum size of the content (in kilobytes) involved in the user behavior to count as a trigger condition for the rule's actions to execute. You may leave this parameter blank or specify -1 to indicate that this rule applies to content of any size.
- *Rate (min):* This parameter defines the duration (in minutes) of the user behavior event should happen to trigger the rule action. For example, it might be acceptable for a user to transfer 50 files during an entire session; however, transferring 50 files in the course of 5 minutes should cause a session termination. For events related to remote sessions, leave this parameter blank or specify -1 to indicate that the system should count user behavior threshold for the duration of the current session.
- *Rule Description:* This read only field provides human readable feedback describing the current rule configuration to confirm the expectations of the rule's behavior.
- **Rule Actions:** This section describes the rule actions that execute in response to a user behavior condition defined in the previous section. You can disable a behavior profile by unchecking all options in this Rule Actions section.

Please note that depending on the rule type selected, the Rule Actions parameters may contain more or less options.

- *Log Event:* This action causes the system to generate an Audit Log event (using the audit category Analytics) in response to the specified user behavior. Interested parties could subscribe to daily or weekly reports as well as to real-time notifications related to the analytics events to monitor behavior of system users or to fine tune user behavior configuration. The events from the audit log could also be streamed to a SIEM systems for correlation analysis.
- *Terminate Session:* This action causes the system to terminate the user's current session to the remote endpoint in response to the specified user behavior.
- *Block User:* This action causes the system to block a user in response to the specified user behavior from all system activities. A blocked user may still login to PAM; however, until they are unblocked, they will not have access to any objects or settings, this includes all permissions and roles applying even to System Administrators. Blocked users can only be unblocked by System Administrators from the Administration > **Global Roles** screen by removing the blocked role or from the Users report by selecting the Unblock option for this user.

We strongly recommend having at least 2 System Administrator accounts for PAM, but if you only have 1 and you have blocked its access, you will need to run the DBUnblock command from the PAM host server to manually unblock this account. To run this command you will need access to the PAM host server, permissions to execute commands and access to the PAM Master Password. We highly recommend having at least 2 System Administrator accounts to avoid these types of scenarios.

- *Reset Password:* This action causes the system to schedule a password reset task for the asset(s)

involved in the specified user behavior.

**User Behavior Rule**

**Trigger** ?

**Rule Type** ? Frequent or Large Files Download

**Threshold Count** ? 4

**Threshold Size (Kb)** ? 512

**Rate (min)** ? 10

**Rule Description** ? Trigger action when downloading 4 file(s) larger than 512Kb during 10 minutes

**Rule Actions** ?

**Log Event** ? ☒

**Terminate Session** ? ☒

**Block User** ? ☒

**Reset Password** ? ☐

Close Save

7. Click the **Save** button to finish creating your rule for this profile.
8. You may add additional rules to this Behavior Profile using the **Add Rule** and repeating the process or you may click the **Save** button to finish creating this profile.

## Apply Behavior Profiles to User or Records

How To Apply Behavior Profiles to User or Records.

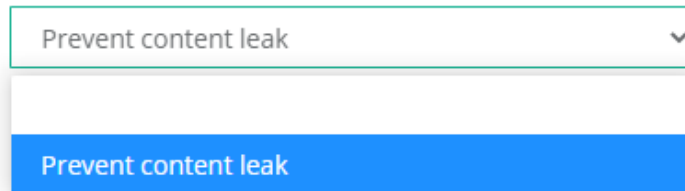
Behavior Profiles are applied to PAM Users or Records as Workflow Binding objects thus allowing the profile to be uniquely customized to specific containers, records, IP addresses, time of day and more.

1. Navigate to the container or object where the profile is to be applied and select the Manage > **Workflows** option from the menu.
2. Select Actions > **Edit** for the existing binding that you wish to apply this profile. If you do not have any bindings, please review our Approval Workflows article for additional information about Workflows and their Bindings.



3. For the **Behavior Profile** option, select the profile name from the dropdown menu.

**Behavior Profile** ?

A screenshot of a web interface showing a dropdown menu. The dropdown is open, displaying a list of options. The top option is "Prevent content leak" with a downward arrow icon. Below it, there is a blue button with the text "Prevent content leak".

Prevent content leak

Prevent content leak

4. Click the **Save** button to save your updated workflow binding.

Now you may test the applied Behavior Profile with the User that is associated to this binding.

## Edit Behavior Profiles and their Rules

How To Edit Behavior Profiles and their Rules.

1. Login to PAM with a System Administrator account. Only System Administrators may manage behavior profiles.
2. Navigate to Administration > Behavior Profiles.
3. Click the **Edit** button corresponding to the *Behavior Profile* you wish to edit.
4. On the Behavior Profile's edit page, you may update the Name, Description or add additional rules as needed.
5. If you wish to edit an existing rule in this profile, click the **Edit** button corresponding to the rule, make the required changes and finally click its **Save** button to complete the rule change.
6. Click the **Save** button on the Behavior Profile screen to save all your changes.

## Delete Behavior Profiles and their Rule

How To Delete Behavior Profiles and their Rules.

1. Login to PAM with a System Administrator account. Only System Administrators may manage behavior profiles.
2. Navigate to Administration > **Behavior Profiles**.
  - If you wish to delete a Behavior Profile entirely, click the **Delete** button next to the corresponding profile. Click **OK** in the confirmation dialog to complete the deletion of your selected profile.
  - If you wish to delete a Rule within a Behavior Profile, click the Behavior Profile's **Edit** button and once in the Profile, click the **Delete** button next to the corresponding rule that you wish to remove from the profile. Click **OK** in the confirmation dialog to delete the selected rule. Once the rule has been deleted, you must click the Profile's **Save** button to complete this process.

## Calendar style weekly access analytics report

The calendar style weekly access analytics report identify deviations in users behavior accessing assets during the week. The report displays the distribution of sessions during the hours of the day and day of the week in a concise chart.

This report identify peak access as well as *deviations* in users behavior such as unexpected access at night or during the weekend.

The report is available on the Reports > **Statistics** screen and covers users access activity during last week.

# Behavior Profiles

Behavior profiles allow PAM System Administrators to create custom configurations to take automatic actions based on the behavior profiles of users.

Common examples would be a Behavior Profile where a user unlocks too many secrets in a short amount of time or a user frequently downloads files during a remote session.

These behavioral events could then trigger actions such as blocking the user’s access or terminating their session, allowing PAM to perform self-monitoring with automated remediation.

## Create Behavior Profiles

Any user who has been granted the global System Administrator role may access and modify the Command Control policies, located at Administration > Behavior Profiles.

To create a new profile, navigate to Administration > Behavior Profiles and click the **Add** button.

Create your policy by entering the values as required.

Name	Enter a unique, but descriptive name for your profile.  When applying the policy, the user will be selecting your policy by name only from a dropdown menu.
Description	Enter a description for your profile.

Next, click the **Add Rule** button to begin configuring your behavior profile rules.

Behavior Profile Rules are comprised of two components; first the *Trigger* which are the user actions or events that are being monitored and the second is the *Rule Actions* which are the automatic remediation actions performed.

Your rule may only include a single Trigger; however, this same rule may include multiple Rule Actions.

The available **Triggers** are described below.

Please note that depending on the selected *Rule Type*, there may be more or less options are available.

Rule Type	Select the rule from dropdown menu that will be used to trigger the action.
Threshold Count	This parameter specifies the number of times the selected type of a user’s behavior should occur before it triggers execution of the rule’s actions.

Threshold Size (Kb)	<p>This parameter specifies the minimum size of the content (in kilobytes) involved in the user behavior to count as a trigger condition for the rule's actions to execute.</p> <p>You may leave this parameter blank or specify -1 to indicate that this rule applies to content of any size.</p>
Rate (min)	<p>This parameter defines the duration (in minutes) of the user behavior event should happen to trigger the rule action.</p> <p>For example, it might be acceptable for a user to transfer 50 files during an entire session; however, transferring 50 files in the course of 5 minutes should cause a session termination.</p> <p>For events related to remote sessions, leave this parameter blank or specify -1 to indicate that the system should count user behavior threshold for the duration of the current session.</p>
Rule Description	<p>This read only field provides human readable feedback describing the current rule configuration to confirm the expectations of the rule's behavior.</p>

The available **Rule Actions** are described below.

You can disable a behavior profile by unchecking all options in this *Rule Actions* section.

Please note that depending on the rule type selected, the *Rule Actions* parameters may contain more or less options.

Log Event	<p>This action causes the system to generate an Audit Log event (using the audit category Analytics) in response to the specified user behavior.</p> <p>Interested parties could subscribe to daily or weekly reports as well as to real-time notifications related to the analytics events to monitor behavior of system users or to fine tune user behavior configuration.</p> <p>The events from the audit log could also be streamed to a SIEM systems for correlation analysis.</p>
Terminate Session	<p>This action causes the system to terminate the user's current session to the remote endpoint in response to the specified user behavior.</p>

Block User	<p>This action causes the system to block a user in response to the specified user behavior from all system activities.</p> <p>A blocked user may still login to PAM; however, until they are unblocked, they will not have access to any objects or settings, this includes all permissions and roles even <i>System Administrators</i>.</p> <p>Blocked users can only be unblocked by System Administrators from the Administration &gt; Global Roles screen by removing the blocked role or from the Users report by selecting the Unblock option for this user.</p>
Reset Password	<p>This action causes the system to schedule a password reset task for the asset(s) involved in the specified user behavior.</p>

When you are finished, click the **Save** button to complete the rule creation. This new rule will be added to the Behavior Profile.

If you wish to add more rules to this profile, click the **Add Rule** button and repeat the process.

Each Behavior Profile can contain multiple rules.

When you are finished creating your *Behavior Profile*, click the **Save** button to complete the profile creation.

## Edit or Delete Behavior Profiles

To edit or delete an existing profile, navigate to Administration > Behavior Profiles and click the **Edit** or **Delete** button next to your desired profile.

If editing a profile, be sure to click the **Save** button when you are finished with your changes.

## Edit or Delete Behavior Profiles Rules

To edit or delete an existing profile's rules, navigate to Administration > Behavior Profiles and click the **Edit** button next to your desired profile.

When you are on the Behavior Profile's Edit page, click the **Edit** or **Delete** button next to your desired rule.

Make the required changes and click the **Save** button when finished.

## Applying Behavior Profiles

Behavior Profiles are applied to Records through the use of Workflow Bindings.

When you configure Workflow Bindings, you will have the option to select one Behavior Profile that will be applied to all users that are bound to this object's workflow.

The Profile will then be applied to their interactions related to this Record.

Please visit [Workflows](#) article for additional information and configuration options.

# Settings and Configurations

The Settings menu is used to consolidate Global and Administrative configuration options to be implemented and maintained by System Administrators.

## Application Nodes

Provides an overview of all found nodes within the system configuration. Use the appropriate **Edit** button to modify an individual node's configuration.

A link to the [API Documentation](#) is also available on this page.

## Proximity Groups

Proximity Groups are used for system configurations that include multiple Session Manager components.

A Proximity Group is used to define which Session Manager is to be used when brokering connections for remote Sessions.

Use the **Add Group** button to add additional Proximity Groups and configure as required.

When Proximity Groups are added their connection status will be shown as a specific font color in the *Servers* column of the list.

- **Green** indicates the service is online and secured.
- **Blue** indicates the service is online and insecure.
- **Grey** with strikethrough indicates the service is not online.

Use the **Edit** button next to each Proximity Group to update its configuration.

For more information about multiple or isolated Session Manager deployments, please read our [Article Deployment Architecture to Scale Session Manager](#) article.

## Database

The Database page shows your current database connection information as well as a listing of all exported database volumes.

Use the options **Export Encrypted** or **Export Decrypted** to generate an on-demand system export with or without encryption.

Use the **Import** button next to the appropriate export to import that volume into the system.

**CAUTION: A database import will remove all current objects, settings and configurations from the system and replace it with those from the imported volume only. This action cannot be undone.**

## Registration

Enter your system Activation code here to register the software or to update your current key.

Once the code has been entered in the **Activation code** field, click the **Automatic Registration** button and when the Status indicates *License is Valid*, click the **Save License** button to complete the activation process.

If your system cannot communicate with PAM's activation server, then use the **Manual Registration** button and follow the onscreen steps to complete the activation process.

## Parameters

The Parameters page provides several options that can be used to configure the system.

Use the Help button (  ) available for each parameter for a brief description of its function and usage.

After any parameter is updated, be sure to click its **Save** button to save the change.

## Mail Server

The Mail Server page is used to configure and test your Email Server integration.

Mail server integration is required to send email notifications and scheduled reports to users with a defined email address in their account profile.

## AD

The AD page is used to configure and test your Active Directory integration. Enter your Active Directory connection parameters and account that will be used by the system to create an integration point.

The account provided will be used to execute AD queries, read AD group membership, read AD user profiles and to reset passwords when using the *Active Directory User* record type.

## Syslog

The Syslog page is used to configure your syslog output so that PAM's audit events can be sent to your external SIEM or Syslog product.

## System Properties Reference Guide

[Download \(docx\)](#)

### Backend Database

Property	Default	Description
derby.system.home		Embedded database home folder
hibernate.connection.driver_class		Backend database driver class
hibernate.dialect		Backend database dialect
pam.db.password		Backend database Password
pam.db.url		Backend database URL
pam.db.user		Backend database User
pam.db.validationQuery		Test backend database query to validate connection

# LDAP Authentication

Property	Default	Description
ldap.authn.searchFilter		Main integrated LDAP user search filter
ldap.baseDn		Main integrated LDAP base DN
ldap.domain		Main integrated LDAP domain
ldap.groupSearch		Main integrated LDAP groups search query
ldap.managerDn		Main integrated LDAP service account
ldap.managerPassword		Main integrated LDAP service account password
ldap.roleBase		Main integrated LDAP base tree node for groups
ldap.roleName	cn	Main integrated LDAP attribute name for a group name
ldap.roleSearch		Main integrated LDAP role search query
ldap.rootDn		Main integrated LDAP root DN
ldap.url		Main integrated LDAP URL
realm.apacheds.local.baseDn		Local user directory service account DN
realm.apacheds.local.bindCredentials		Local user directory service account password
realm.apacheds.local.connectionURL		Local user directory URL
realm.apacheds.local.groupSearch		Local user directory group search query
realm.apacheds.local.roleBase		Local user directory group base
realm.apacheds.local.roleName		Local user directory attribute for group name
realm.apacheds.local.roleSearch		Local user directory membership search query
realm.apacheds.local.userBase		Local user directory user base
realm.apacheds.local.userSearch		Local user directory user search query
realm.apacheds.local.userSearch.cas		Local user directory user search for CAS
ldap[2].name		Integration name
ldap[2].url		LDAP URL
ldap[2].managerDn		Service account DN
ldap[2].managerPassword		Service account DN password

Property	Default	Description
ldap[2].rootDn		Root DN
ldap[2].baseDn		Base DN
ldap[2].domain		Domain
ldap[2].authn.searchFilter		User search filter
ldap[2].userName	uid	User name attribute
ldap[2].userSearch		User search filter
ldap[2].roleBase		Role base DN
ldap[2].roleName	cn	Role name attribute
ldap[2].roleSearch		Search query for roles by user
ldap[2].groupSearch		Search query for roles

## MFA

Property	Default	Description
cas.authn.mfa.duo[0].duoApiHost		Duo MFA integration Duo Security API URL
cas.authn.mfa.duo[0].duoApplicationKey		Duo MFA integration application or secret key
cas.authn.mfa.duo[0].duoIntegrationKey		Duo MFA integration API key
cas.authn.mfa.duo[0].duoSecretKey		Duo MFA integration secret key
cas.authn.mfa.duo[0].id		Duo MFA integration ID (mfa-duo)
cas.authn.mfa.duo[0].name		Duo MFA integration name
cas.authn.mfa.duo[0].rank	0	Duo MFA integration rank
cas.authn.mfa.duo[0].trustedDeviceEnabled	False	Duo MFA integration flag to enable trusted devices option
cas.authn.mfa.gauth.codeDigits	6	TOTP MFA number of digits in the code
cas.authn.mfa.gauth.issuer		TOTP MFA issuer



Property	Default	Description
cas.authn.mfa.gauth.jpa.database.dataSourceName		TOTP MFA database connection (usually java:comp/env/jdbc/PamDB)
cas.authn.mfa.gauth.jpa.database.dataSourceProxy	true	TOTP MFA data source proxy
cas.authn.mfa.gauth.jpa.database.ddlAuto	update	TOTP MFA database pre-creation option
cas.authn.mfa.gauth.jpa.database.dialect		TOTP MFA database dialect (usually {hibernate.dialect})
cas.authn.mfa.gauth.jpa.database.driverClass		TOTP MFA database driver class (usually {hibernate.connection.driver_class})
cas.authn.mfa.gauth.label		TOTP MFA screen label
cas.authn.mfa.gauth.timeStepSize	30	TOTP MFA time step size
cas.authn.mfa.gauth.trustedDeviceEnabled	False	TOTP MFA flag to enable trusted devices option
cas.authn.mfa.gauth.windowSize	3	TOTP MFA window size
cas.authn.mfa.globalProviderId		Global MFA provider
cas.authn.mfa.radius.client.accountingPort		Radius MFA accounting port
cas.authn.mfa.radius.client.authenticationPort		Radius MFA authentication port
cas.authn.mfa.radius.client.inetAddress		Radius MFA host name or IP address
cas.authn.mfa.radius.client.sharedSecret		Radius MFA secret
cas.authn.mfa.radius.server.protocol		Radius MFA server protocol
cas.authn.mfa.yubikey.clientId		Yubikey MFA client ID
cas.authn.mfa.yubikey.jpa.dataSourceName		Yubikey MFA data source name (usually java:comp/env/jdbc/PamDB)
cas.authn.mfa.yubikey.jpa.dataSourceProxy	true	Yubikey MFA data source proxy
cas.authn.mfa.yubikey.jpa.ddlAuto	update	Yubikey MFA database pre-creation option

Property	Default	Description
cas.authn.mfa.yubikey.jpa.dialect		Yubikey MFA database dialect (usually {hibernate.dialect})
cas.authn.mfa.yubikey.jpa.driverClass		Yubikey MFA database driver class (usually {hibernate.connection.driver_class})
cas.authn.mfa.yubikey.name		Yubikey MFA integration name
cas.authn.mfa.yubikey.secretKey		Yubikey MFA secret key
cas.authn.mfa.groovyScript		Path to Groovy script to enable granular MFA integration

## CAS

Property	Default	Description
cas.audit.alternateClientAddrHeaderName		HTTP Header for client address (X-Forwarded-For)
cas.audit.jdbc.dataSourceName		CAS audit data source name (usually java:comp/env/jdbc/PamDB)
cas.audit.jdbc.dataSourceProxy		CAS audit MFA data source proxy
cas.audit.jdbc.ddlAuto	update	CAS audit database pre-creation option
cas.audit.jdbc.dialect		CAS audit database dialect (usually {hibernate.dialect})
cas.audit.jdbc.driverClass		CAS audit database driver class (usually {hibernate.connection.driver_class})
cas.authn.accept.users	Empty	Hard coded users for authentication
cas.clearpass.cacheCredential	False	Flag to enable using the password of the current user for system operations such as session connect
cas.clearpass.cacheCredential	true	Flag to enable pass-through credentials capture
cas.clearpass.crypto.enabled	true	Flag to enable pass-through credential encryption

Property	Default	Description
cas.clearpass.crypto.encryption.key		Pass-through credentials encryption key
cas.clearpass.crypto.signing.key		Pass-through credentials signing key
cas.logout.confirmLogout	true	Confirms CAS logout
cas.logout.followServiceRedirects	true	Flag to enable service provider logout for SAML integrated providers
cas.managed.path		Application Access URL stem (https://xtam.company.com/)
cas.metrics.loggerName		
cas.metrics.refreshInterval	86400	
cas.server.name		Managed path of CAS server URL (for example, https://xtam.company.com)
cas.server.prefix		CAS URL for SAML integration (for example, https://xtam.company.com/xtam/)
cas.serviceRegistry.initFromJson	true	Flag for CAS registry DB initialization
cas.serviceRegistry.jpa.dataSourceName		CAS service registry data source name (usually java:comp/env/jdbc/PamDB)
cas.serviceRegistry.jpa.dataSourceProxy	true	CAS service registry MFA data source proxy
cas.serviceRegistry.jpa.ddlAuto	update	CAS service registry database pre-creation option
cas.serviceRegistry.jpa.dialect		CAS service registry database dialect (usually {hibernate.dialect})
cas.serviceRegistry.jpa.driverClass		CAS service registry database driver class (usually {hibernate.connection.driver_class})
cas.standalone.config.security.alg		Algorithm for CAS parameters encryption
cas.standalone.config.security.psw		Master password to encrypt CAS parameters
cas.tgc.crypto.enabled	true	Flag to enable CAS TGC encryption

Property	Default	Description
cas.tgc.crypto.encryption.key	generated	CAS TGC encryption key
cas.tgc.crypto.signing.key		CAS ticket granting signing key. SRF token signing key
cas.tgc.crypto.signing.key	generated	CAS TGC signing key
cas.ticket.registry.cleaner.schedule.enabled		CAS ticket registry cleaner schedule enable flag
cas.ticket.registry.cleaner.schedule.repeatInterval		CAS ticket registry cleaner repeat interval
cas.ticket.registry.cleaner.schedule.startDelay		CAS ticket registry cleaner start delay
cas.ticket.registry.jpa.crypto.alg	AES	CAS ticket registry encryption algorithm
cas.ticket.registry.jpa.crypto.enabled	true	Flag to enable CAS registry encryption
cas.ticket.registry.jpa.crypto.encryption.key	generated	CAS ticket registry encryption key
cas.ticket.registry.jpa.crypto.encryption.keySize	16	CAS ticket registry encryption key size
cas.ticket.registry.jpa.crypto.signing.key	generated	CAS ticket registry signing key
cas.ticket.registry.jpa.crypto.signing.keySize	512	CAS ticket registry signing key size
cas.ticket.registry.jpa.dataSourceName		CAS ticket registry data source name (usually java:comp/env/jdbc/PamDB)
cas.ticket.registry.jpa.dataSourceProxy	true	CAS ticket registry MFA data source proxy
cas.ticket.registry.jpa.ddlAuto	update	CAS ticket registry MFA database pre-creation option
cas.ticket.registry.jpa.dialect		CAS ticket registry database dialect (usually {hibernate.dialect})
cas.ticket.registry.jpa.driverClass		CAS ticket registry database driver class (usually {hibernate.connection.driver_class})
cas.ticket.registry.jpa.jpaLockingTimeout	3600	CAS ticket locking timeout
cas.ticket.registry.jpa.ticketLockType	NONE	CAS ticket lock shared among nodes
cas.ticket.st.timeToKillInSeconds	10	

Property	Default	Description
cas.view.defaultRedirectUrl		Application Access URL such as <a href="https://xtam.company.com/xtam/">https://xtam.company.com/xtam/</a>
cas.webflow.crypto.alg	AES	
cas.webflow.crypto.enabled	true	
cas.webflow.crypto.encryption.key		CAS webflow encryption key
cas.webflow.crypto.encryption.keySize	16	
cas.webflow.crypto.signing.key		CAS webflow signing key
cas.webflow.crypto.signing.keySize	512	

## CAS Authentication

Property	Default	Description
cas.authn.ldap[0].type	DIRECT	Local user directory type
cas.authn.ldap[0].ldapUrl		Local user directory URL
cas.authn.ldap[0].useSsl		Local user directory SSL enabling
cas.authn.ldap[0].useStartTls		Local user directory StartTLS enabling
cas.authn.ldap[0].connectTimeout		Local user directory connect timeout
cas.authn.ldap[0].baseDn		Local user directory base DN
cas.authn.ldap[0].userFilter		Local user directory filter to search users
cas.authn.ldap[0].subtreeSearch		Local user directory enable subtree search
cas.authn.ldap[0].usePasswordPolicy	false	Local user directory use password policy
cas.authn.ldap[0].dnFormat		Local user directory DN format pattern based on user entry
cas.authn.ldap[0].principalAttributeId	uid	Local user directory attribute for user
cas.authn.ldap[0].principalAttributeList		Local user directory list of attributes to retrieve from the directory
cas.authn.ldap[1].type		Integrated LDAP user directory type (AUTHENTICATED AD DIRECT ANONYMOUS)

Property	Default	Description
cas.authn.ldap[1].ldapUrl		Integrated LDAP user directory URL
cas.authn.ldap[1].useSsl		Integrated LDAP user directory use SSL option
cas.authn.ldap[1].useStartTls		Integrated LDAP user directory use StartTLS option
cas.authn.ldap[1].connectTimeout		Integrated LDAP user directory connection timeout
cas.authn.ldap[1].baseDn		Integrated LDAP user directory base DN
cas.authn.ldap[1].userFilter		Integrated LDAP user directory user query
cas.authn.ldap[1].subtreeSearch		Integrated LDAP user directory enable subtree search
cas.authn.ldap[1].usePasswordPolicy	false	Integrated LDAP user directory password policy use
cas.authn.ldap[1].dnFormat		Integrated LDAP user directory DN format pattern
cas.authn.ldap[1].principalAttributeId		Integrated LDAP user directory attribute for user name (for example, sAMAccountName or UserPrincipalName)
cas.authn.ldap[1].principalAttributeList		Integrated LDAP user directory list of attributes to retrieve from directory
cas.authn.pac4j.saml[x].clientName		SAML integration client name
cas.authn.pac4j.saml[x].keystorePassword		SAML integration keystore password
cas.authn.pac4j.saml[x].privateKeyPassword		SAML integration
cas.authn.pac4j.saml[x].serviceProviderEntityId		SAML integration service provider entity ID
cas.authn.pac4j.saml[x].serviceProviderMetadataPath		SAML integration URL to service provider metadata
cas.authn.pac4j.saml[x].keystorePath		SAML integration path to keystore
cas.authn.pac4j.saml[x].identityProviderMetadataPath		SAML integration path to provider metadata file

Property	Default	Description
cas.authn.pac4j.saml[x].maximumAuthenticationLifetime		SAML integration maximum authentication lifetime
cas.authn.pac4j.saml[x].forceAuth	false	SAML integration

## XTAM

Property	Default	Description
ide	False	Flag to avoid 1-minute delay starting up worker processes
java.io.tmpdir		OS temporary folder
java.net.useSystemProxies	true	Flag to disable use of OS proxy configuration for HTTP queries such as check for latest version. False in OOB configuration.
mail.smtp.timeout	10000	Timeout in milliseconds for SMTP operations
pam.language	en_US	Default language to initialize the system
user.home		Temporary folder base for the playback rendering
xtam.ad.members.search	true	Flag to enable dynamic reference from local groups to external LDAP members to allow entry reorganization in the external user directory without breaking local groups membership. When set to False, the system will use entry DN to reference external entry instead of search
xtam.api.token.verification	true	Flag to disable XSRF token verification
xtam.aws.sts.endpoint		AWS STS Endpoint for temporary ticket generation. The value defaults to sts.amazonaws.com and could be overwritten by record field STSEndpoint.
xtam.aws.sts.region		AWS STS Region for temporary ticket generation. The value defaults to us-east-1 and could be overwritten by record field STSRegion.
xtam.cas.mfa.token		Authentication token from CAS login process to XTAM granular MFA service

Property	Default	Description
xtam.cas.mfa.default	none	Default MFA service to use in case of failure to detect user or group based MFA service
xtam.cas.registry.sqlCasJwtSigningKey		SQL statement for CAS registry
xtam.cas.registry.sqlCasJwtupdateService		SQL Statement for CAS registry update
xtam.cert.password		WEB Server SSL Certificate password
xtam.cert.path		Path to WEB Server SSL Certificate
xtam.config.recording.encrypt	False	Flag to enable encryption of session recordings
xtam.driver.wsman.delay	1	WS-Management protocol delay in seconds between commands
xtam.driver.wsman.timeout	30	WS-Management protocol timeout in seconds
xtam.ha[0].url		Second node URL for node replication
xtam.http.proxy	False	Flag to enable HTTP Proxy in remote node to tunnel RDP, SSH and HTTP proxy connections from master node as a session manager
xtam.http.proxy.port		Port number overwrite for remote node HTTP Proxy serving as a session manager for master node proxy servers
xtam.http.proxy.upstream.auth.alg	SHA256	Encryption algorithm for remote Proxy session manager communication for SSH, RDP, HTTPs proxies
xtam.import.unique	False	Flag to enable enforcement of unique record names in folder during import process
xtam.integration.duo.apiHost		Overwrite for cas.authn.mfa.duo[0].duoApiHost
xtam.integration.duo.integrationKey		Overwrite for cas.authn.mfa.duo[0].duoIntegrationKey
xtam.integration.duo.secretKey		Overwrite for cas.authn.mfa.duo[0].duoSecretKey
xtam.integration.sms.password		
xtam.integration.sms.script		SMS integration Groovy script from script library
xtam.integration.sms.url		SMS integration URL



Property	Default	Description
xtam.integration.sms.user		
xtam.integration.ticketing.password		Service account password for ticketing system integration
xtam.integration.ticketing.pattern		Request reason pattern indicating a message to ticketing system (SN #)
xtam.integration.ticketing.script		Groovy script from the script library to integration with ticketing system
xtam.integration.ticketing.url		URL of ticketing system
xtam.integration.ticketing.user		Service account for ticketing system integration
xtam.item.name.length	3996	Max length of form fields
xtam.item.ref.credential.only	False	Flag to use only credential fields for reference records
xtam.mfa.mock	False	Flag enabling mock MFA controller (allow first time use, deny second time use)
xtam.perflog.dump_attributes	False	Flag to log operating system attributes to performance logging
xtam.perflog.enabled	False	Flag to enable internal performance logging
xtam.perflog.logging.file	Perf.log	File name for the internal performance logging if not redirected to system log
xtam.perflog.logging.level	INFO	Level of the system log message for internal performance log
xtam.perflog.logging.system	False	Flag to redirect internal performance logging to regular system logging instead of custom file perf.log
xtam.perflog.period.seconds	60	Period of internal performance logging
xtam.proxy.cli.mfa.disabled	False	Flag to disable capability to pass MFA token with RDP, SSH proxy user attribute
xtam.proxy.host		XTAM Proxy host if different from cas.managed.path (for example, for geo-distributed systems)

Property	Default	Description
xtam.proxy.http.trustAllServers	False	Flag to enable HTTP Proxy to trust SSL Certificates of all endpoint WEB Portals
xtam.rdp.proxy	False	Flag to enforce RDP proxy startup
xtam.rdp.proxy.port		RDP Proxy port overwrite
xtam.rdp.proxy.trace_cleartext_credentials	False	Flag to enable tracing of credential capturing by the system
xtam.remote.enabled	False	Flag to switch the node to remote node mode
xtam.remote.node		Node name to overwrite default host name as a node name
xtam.remote.password		Remote node user password
xtam.remote.token		Remote node authentication token as an alternative to user and password
xtam.remote.url		Master node URL
xtam.remote.user		Master node user to connect to master node
xtam.remote[0].enabled	false	Flag to enable master node configuration for multi-master node deployment
xtam.remote[0].url		Master node URL in multi-master node deployment
xtam.remote[0].user		Master node user in multi-master node deployment
xtam.remote[0].password		Master node password in multi-master node deployment
xtam.remote[0].token		Master node password token in multi-master node deployment to use instead of user and password
xtam.replication.signingKey		Signing key for node-to-node replication exchange
xtam.report.daily.hours	0	Hour for the daily report schedule
xtam.report.monthly.days	1	Day of the month for monthly report schedule
xtam.report.weekly.days	SUN	Day of the week for weekly report schedule

Property	Default	Description
xtam.secured.ids	False	Flag to enable Secure-IDs
xtam.secured.ids.strict	False	Flag to enable strict check for Secure-IDs
xtam.session.command.input.wait	1000	Time in milliseconds to wait before issuing blocking command (such as sudo) at the start of remote session
xtam.shadow.crossvault.disable	False	Flag to disable restriction to make reference, shadow and dynamic credential records in another vault
xtam.proxy.mfa.disable	False	Flag to disable MFA for proxy sessions (SSH, RDP, HTTP). This parameter replaced now deprecated but still valid parameter xtam.ssh.proxy.mfa.disable with the same meaning.
xtam.ssh.session.idle	0	Default idle timeout for SSH sessions
xtam.transport.security.bc	false	Flag to enable Bouncy Castle installed as a preferred security provider
xtam.ueba.enabled	true	Flag to enable business analytics processing
xtam.user.guest.enabled	false	Flag to enable auto-creating guest accounts authenticated using external SSO services
xtam.user.guest.group		Local group to add auto-created guest user
xtam.user.guest.ttl	0	Expiration time in milliseconds (0 – infinite) for auto-created guest user
xtam.web.mfa.disable	false	Flag to disable MFA for WEB Login (as oppose to Proxy Servers)
xtam.ssh.proxy.connect_retry_count	2	Number of times SSH Proxy will retry connecting to remote server
xtam.ssh.proxy.auth_retry_count	5	Number of times SSH Proxy will retry authenticating XTAM user

Property	Default	Description
xtam.ssh.proxy.connect_retry_timeout	10	Number of seconds SSH Proxy waits before retrying to connect to remote server progressively increasing with each retry (10 seconds after first failed attempt, 20 seconds after seconds one, 30 seconds after third one)
xtam.ssh.proxy.auth_retry_timeout	10	Number of seconds SSH Proxy waits before retrying to authenticate XTAM user progressively increasing with each retry (10 seconds after first failed attempt, 20 seconds after seconds one, 30 seconds after third one)
xtam.ssh.exec.su.mode	1	SSH su command execution mode: 1 - su - user -c 'command' 2 - su -c 'command' - user
xtam.ssh.exec.verify.feedback	false	Default SSH execution strategy password reset verification only checks successful connectivity with new password. Set this option to true to verify password reset by checking the output from the echo command to confirm successful command execution.
xtam.ssh.channel.connect.timeout	20000	Timeout opening SSH job execution channel in milliseconds. Default is defined by the library and is about 20 seconds (20000 ms)
xtam.session.command.expect.su	password	Expected output for su command to type password
xtam.reverse.tunnel[0].remoteHost		Master node host for SSH connection for reverse tunnel configuration
xtam.reverse.tunnel[0].remotePort		Master node port for SSH connection for reverse tunnel configuration
xtam.reverse.tunnel[0].remoteUser		Master node user for SSH connection for reverse tunnel configuration
xtam.reverse.tunnel[0].remotePassword		Master node user password or Private Key password for SSH connection for reverse tunnel configuration

Property	Default	Description
xtam.reverse.tunnel[0].remoteKey		Optional path to master node Private Key for SSH connection as an alternative for remoteUser for reverse tunnel configuration
xtam.reverse.tunnel[0].forwardHost		Session manager host in the isolated network in the local isolated network space for reverse tunnel configuration
xtam.reverse.tunnel[0].forwardPortLocal		Session manager port in the isolated network for reverse tunnel configuration
xtam.reverse.tunnel[0].forwardPortRemote		Session manager port on the master node to use in the proximity group for reverse tunnel configuration
xtam.reverse.tunnel[0].forwardBindingAddress		Binding address on the master node to expose the port to other interfaces
xtam.reverse.tunnel[0].enabled	true	Flag to enable or disable reverse tunnel configuration
xtam.forward.tunnel[0].remoteHost		Master node host for SSH connection for reverse tunnel configuration
xtam.forward.tunnel[0].remotePort		Master node port for SSH connection for reverse tunnel configuration
xtam.forward.tunnel[0].remoteUser		Master node user for SSH connection for reverse tunnel configuration
xtam.forward.tunnel[0].remotePassword		Master node user password or Private Key password for SSH connection for reverse tunnel configuration
xtam.forward.tunnel[0].remoteKey		Optional path to master node Private Key for SSH connection as an alternative for remoteUser for reverse tunnel configuration
xtam.forward.tunnel[0].forwardHost		Host in the master node network to forward tunnel to
xtam.forward.tunnel[0].forwardPortLocal		Forwarded port on the remote node to map as a master node port
xtam.forward.tunnel[0].forwardPortRemote		Master node port to forward traffic to

Property	Default	Description
xtam.forward.tunnel [0].forwardBindingAddress		Binding address on the remote node to expose the port to other interfaces
xtam.forward.tunnel[0].enabled	true	Flag to enable or disable forward tunnel configuration
xtam.ssh.proxy.banner		SSH Proxy banner to override banner defined in the system parameter
xtam.job.selfCheckStatus	false	This parameter makes Check Status job execution to run by the account on record instead of the shadow account
xtam.session.web.audio	false	Enables audio channel support for WEB Sessions
xtam.replication.sequence		Indicator of node sequence in multi-node High Availability setup. The parameter is given in the form of sequence/total where the sequence (1, 2, 3, ...) is the sequence of the node in HA cluster and total is the total number of nodes in the cluster. Among other options, the node will only send notifications about event generated by this node to avoid duplication of alerts.
xtam.ssh.proxy.auth.rest	false	Flag indicating whether SSH Proxy user authentication should fall back to REST authentication after failed attempts to authenticate using integrated LDAP directories.
xtam.web.version.disable	false	Flag disabling automatic version check by the WEB GUI
xtam.export.page.size	500	Page size for export process to control balance between memory consumption and speed of system export
xtam.api.config.check_groups.threads_per_request	5	If many proximity groups are configured and users are experiencing slowness when loading the proximity group page, the value of this property can be increased to a number greater than 5. PAM Manager needs to be restarted if this property is updated

Property	Default	Description
xtam.ldap.cert.auto-import	true	Auto-import AD certificates for internal directory service (on replication) and AD records (on periodical jobs when using LDAPS connection)
xtam.web.cert.auto-import	true	CAS certificate auto import performed on application startup if set to true, disabled if false

[System properties reference guide \(docx\)](#)

## Command Line Utility Reference Guide

### Terminology

PAM – Privileged Access Management

CLU – PAM Command Line Utility

CLI – command line interface

\$PAM\_HOME – PAM Server deployment folder

ADS – internal user directory service

CDN – content distribution network for PAM binaries

### Introduction

PAM Command Line Utility (CLU) is a helper utility to simplify and to facilitate PAM Server configuration and deployment activities.

This guide expects CLU will be launched from the `$PAM_HOME` folder by providing full or relative path to the utility launcher. *A typical issue with launching CLU is running it from a location other than the `$PAM_HOME` folder (typically `$PAM_HOME/bin` which is incorrect).*

Example of the launch command for **Linux hosts** is given below:

Linux host

```
1 | ./bin/PamDirectory.sh COMMAND PARAMETER1 PARAMETER2 ...
```

Example of the launch command for **Windows hosts** is given below:

#### Windows host

```
1 | .\bin\PamDirectory.cmd COMMAND PARAMETER1 PARAMETER2 ...
```

Below are several examples of the command run on a **Linux host to integrate with Active Directory** prompting for the user's password:

```
1 | ./bin/PamDirectory.sh ADConnect web dc-server ad-service-user -
```

```
1 | ./bin/PamDirectory.sh ADConnect web ldaps://dc-server:636 ad-service-user -
```

## Common Parameters

- **catalina.home** is the folder where PAM Server WEB Container is located. Typically, it is **\$PAM\_HOME/web** folder. When the CLU is launched from the **\$PAM\_HOME** folder it could be specified using a relative **path: web**
- **password** – in the majority of the cases it is possible to specify dash ( - ) instead of the password in the command line to make the CLU to allow a user to type the password in a secure input prompt. This option masks the password during CLU execution and to simplify the entry of special characters.

- **File PATH\_TO\_THE\_INSTRUCTION\_FILE** – parameter File allows one to provide CLU the text file with the list of parameters instead of providing command parameters using command line.

The parameters file is a regular properties file with all parameters defined under the same section called: **instruction**.

Command parameter is specified using property **command**.

All other parameters are specified as properties with the property name as it is defined in this guide.

Note that unlike the ordered unnamed command line parameters, parameters given by file specification are unordered and named with the required names defined in this document in the Parameters section.

Example of the File properties file for the command **SetAdminPassword** is given below:

[instruction]



catalina.home=web  
admin.password=pam-generate

## Configuration Commands

This section describes the commands mostly used to manage the deployment configuration. Parameters in the commands in this section could be specified as positional command line parameters or using the instruction file using single **File** parameter.

### SetAdminPassword

The command replaces the password of the service account (DN: uid=admin,ou=system) in the local user directory services. The current password is obtained from the existing configuration. The command also updates this password encrypted in the PAM Server configuration file. A service restart is required after executing this command.

#### Parameters

- **catalina.home**
- **admin.password** - New administrator password parameter might be a password itself, a dash to prompt a user to enter a password, or one of the keywords *<generate>* or *pam-generate* to generate new password. The generated password will be printed on the console after the command execution

### SetMasterPassword

The command sets a new master password used to encrypt and decrypt sensitive data in the PAM Vault. Note that the command does not re-encrypt existing records so updating master password might cause existing records to become unreadable by the system in case they were encrypted by different master password.

The command is useful in cases like deploying new node to the existing farm or to migrate back-end database to another system.

#### Parameters

- **catalina.home**
- **master.password** - New master password parameter might be a password itself, a dash to prompt a user to enter a password, or one of the keywords *<generate>* or *pam-generate* to generate new password. The generated password will be printed on the console after the command execution

### SetDBPassword

This command replaces the password of a service account for the embedded database in cases when the system is deployed with the internal Apache Derby database. The command also updates this password encrypted in the PAM Server configuration file. A service restart is required after executing this command.

#### Parameters

- **catalina.home**
- **db.home** is a folder where the internal Apache Derby database is deployed. Typically, it is `$PAM_HOME/db` folder. When the CLU is launched from the `$PAM_HOME` folder it could be specified using the relative path: `db`
- **db.password** – New database administrator password parameter might be a password itself, a dash to prompt a user to enter a password, or one of the keywords *<generate>* or *pam-generate* to generate new password. The generated password will be printed on the console after the command execution

## Init

The command initializes new local user directory service with the LDAP structure required for PAM operations.

Note that the software initializes the directory services during installation. The command is useful to build a new directory service structure. It is not recommended to use this command on an existing, functional deployment.

#### Parameters

- **catalina.home**

## CreateUser

This command creates a local user in the local user directory.

#### Parameters

- **catalina.home**
- **user.login** is the login name of the newly created account
- **user.firstName** is the first name
- **user.lastName** is the last name
- **user.password** is a new user password that might be a password itself, a dash to prompt a user to enter a password, a keyword *GENERATE* to generate new password. The generated password will be printed on the console after the command execution. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

## CreateGroup

This command creates a local group in the local user directory optionally with one specified group member.

#### Parameters

- **catalina.home**
- **group.name** is the name of a new group
- **group.description** is a description of a new group
- **group.member** is the optional member of a new group given as the login name of the account

## RenameGroup

The command renames a local group in the local user directory.

Parameters

- **catalina.home**
- **group.name** is the existing group name
- **group.newName** is the new group name

## SetUserPassword

This command sets a new password for an existing local user.

Parameters

- **catalina.home**
- **ads.password** is a local user directory service account password
- **user.login** is the user login
- **user.password** is the new user password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

## ADConnect

This command sets up integration with [Microsoft Active Directory](#). The result of the successful execution of this command is the set of AD connection properties defined in the `$PAM_HOME/web/conf/catalina.properties` file. The PAM service needs to be restarted after executing this command. This command establishes connection to one Active Directory server. Establishing another connection will replace the previous connection. To manage integration with multiple LDAP / AD servers use the [LdapConnect](#) command.

Read more about [integration with MS Active Directory](#) in the application's help system.

Parameters

- **catalina.home**
- **ldap.server** is the AD Domain Controller server or URL. When just server is specified the CLU attempts to connect to the AD Global Catalogue first and then to the AD Domain Controller itself using LDAPS protocol. Custom protocols or ports could be specified using full URL notation like in the example, [ldaps://ad-server.company.com:port](#).

Note that for the secure communications using LDAPS protocol the AD server certificate should be imported into the PAM Server keystore (see the command `SSLImport`) and the name on the certificate should match the name of the AD-server host in the URL.

- **ldap.user** is the service account in MS Active Directory
- **ldap.password** is the service account password that might be a password itself or a dash to prompt a user to enter a password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

### Example

Configure a new AD connection requesting the command to prompt for the service user password

```
1 | ./bin/PamDirectory.sh ADConnect web ldaps://eu-dc-server pam-service-eu -
```

## ADQuery

This command executes a provided LDAP Query in the first integrated MS Active Directory to test the connection and to test the query.

### Parameters

- **catalina.home**
- **ldap.query** is the LDAP query to execute
- **-v** is the optional parameter to enable additional logging information printed during the query execution.

Note that for the File method to pass parameters this parameter in the properties file should be called *verbose*

## LdapConnect

This command manages integrations with multiple LDAP user directories. Specifically, the command can either add new or delete existing integrations. The result of the successful execution of this command is the set of LDAP connection properties defined in the `$PAM_HOME/web/conf/catalina.properties` file. The PAM service needs to be restarted after executing this command. To manage integration with a single AD server,

administrators might use the **ADConnect** command.

Read more about [integration with multiple LDAP user directories](#) in the application's help system.

#### Parameters

##### **catalina.home**

**ldap.name** is the friendly name of the integrated LDAP server. This name is used in the consequent LDAP management commands as well as in the PAM system as a reference point for the external users. Use alphanumeric characters only.

**ldap.server** is LDAP server or URL. Custom protocols or ports could be specified using full URL notation like in the example, *ldaps://ldap-server.company.com:port*.

Note that for the secure communications using LDAPS protocol the LDAP server certificate should be imported into the PAM Server keystore (see the command `SSLImport`) and the name on the certificate should match the name of the LDAP server host in the URL. Alternatively, this parameter might contain the keyword **DISABLE** to remove integration with this LDAP server referenced by name parameter. When **DISABLE** keyword is specified in this parameter no further positional parameters are required.

**ldap.user** is the service account in LDAP server

**ldap.password** is the service account password that might be a password itself or a dash to prompt a user to enter a password. The password might be started with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

#### Examples

Configure new LDAP connection assigning it new name EU-DC requesting the command to prompt for the service user password:

```
1 | ./bin/PamDirectory.sh LDAPConnect web EU-DC ldaps://eu-dc-server pam-service-eu -
```

Delete configured LDAP connection with the name EU-DC:

```
1 | ./bin/PamDirectory.sh LDAPConnect web EU-DC DISABLE
```

## ADSCONNECT

This command establishes a connection with the internal user directory service (ADS). The connection with the local internal user directory is established during installation. The command is useful to connect to a

remotely deployed internal user directory.

#### Parameters

- **catalina.home**
- **ads.server** is ADS server or URL. Custom protocols or ports could be specified using full URL notation like in the example, *ldaps://ldap-server.company.com:port*.
- **ads.password** is the service account (for the account DN: uid=admin,ou=system) password that might be a password itself or a dash to prompt a user to enter a password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

## ADSReplicate

This command establishes a local user directory replication with the other node of a two-node deployment. Executing this command with a different server will replace the previously established replication. To manage replication for more than two node deployments use the **ADSReplication** command.

Read more about [the internal user directory replication in high availability deployments](#) in the help system.

#### Parameters

- **catalina.home**
- **ads.remote.server** is the host of the replicating system
- **ads.remote.password** is the service account (for the account DN: uid=admin,ou=system) password that might be a password itself or a dash to prompt a user to enter a password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

## ADSReplication

This command manages internal user directory replication between multiple nodes. Each replication process in the local node is associated with the numerical index (1, 2, 3, ...) used in this command. For example, in three-node deployment each node will maintain two replication processes indexed by numbers 1 and 2 on each node with each of the other nodes.

Read more about [the internal user directory replication in high availability deployments](#) in the help system.

#### Parameters

- **catalina.home**
- **ads.remote.index** is the replication process index on this node to apply below parameters to. Alternatively, this parameter might have a keyword list. This list command will list parameters of all configured replication processes on this node. When list command is specified, no other parameters are needed.

- **ads.remote.server** is the host of the replicating system. Alternatively, this parameter might contain keyword **delete** to delete this replication process from the local node.
- **ads.remote.password** is the service account (for the account DN: uid=admin,ou=system) password that might be a password itself or a dash to prompt a user to enter a password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

## Examples

List configured replication slots:

```
1 | ./bin/PamDirectory.sh ADSReplication web list
```

Delete configured replication slots number 3:

```
1 | ./bin/PamDirectory.sh ADSReplication web 3 delete
```

Configure replication slot number 3 requesting the command to prompt for the password:

```
1 | ./bin/PamDirectory.sh ADSReplication web 3 pam-node-d -
```

## ADSExport

This command exports content of internal local user directory service to an external XML file.

### Parameters

- **catalina.home**
- **file** is the file path
- **encrypted** is a true or false parameter indicating whether the export file should contain sensitive data encrypted

## ADSImport

This command imports the content of the exported file to the internal user directory service.

### Parameters

- **catalina.home**
- **file** is the file

# DBConnect

This command changes connection to a new back-end database. The command expects the database server to exist with the appropriate instance and the data-storage with the name PamDB pre-created. A service restart is required after successful execution of this command.

## Parameters

- **catalina.home**
- **db.type** is the vendor of the back-end database with possible values: Derby, MySql, MSSQL, Oracle, PostgreSQL
- **db.server** is the host name of the back-end database. The command will try the port default for the vendor in case the port is not specified. Otherwise, specify port in *host:port* notation.
- **db.user** is the service account for the database integration.
- **db.password** is the service account password that might be a password itself or a dash to prompt a user to enter a password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

# XTConnect

This command runs on the remote PAM node and establishes a connection with the master node. The communication between remote and master node is done using the https protocol.

## Parameters

- **catalina.home**
- **pam.server** is the host of the master node in the form of host, *host:port* or *https://host:port*.
- **pam.user** is the service account with the Service role in the master node.
- **pam.password** is the service account password that might be a password itself or a dash to prompt a user to enter a password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

# ConfigureRealms

This command manages single server integration with [MS Active Directory](#) services. The PAM service should be restarted after successful execution of this command. The command is used by the installation process leaving the configuration complete after the successful installation. The command modifies properties in `$PAM_HOME/web/conf/server.xml` that could be otherwise managed directly without this command.

## Parameters



- **catalina.home**
- **auth.catalina.enable** is an indicator with possible true or false values to manage combined user realm.
- **auth.ad.enable** is an indicator with possible true or false values to manage Active Directory pool connector as a part of the combined realm.

## EnableSso

This command manages configuration of the [Federated Sign-In](#) module. The command is used by the installation process, leaving the configuration complete after a successful installation. The command modifies properties in `$PAM_HOME/web/conf/server.xml` that could be otherwise managed directly without this command. A service restart is required after successful execution of this command.

### Parameters

- **catalina.home**
- **managed.path** is the expected managed path of the PAM WEB Application it will be accessed by its WEB users.
- **sso.enable** enable is an indicator with possible true or false values to enable or disable the Federated Sign-In configuration.

## GenerateSSL

This command generates a new self-signed SSL certificate to secure the PAM server WEB application traffic and applies it to the PAM WEB container. A service restart is required after successful execution of this command.

### Parameters

- **catalina.home**

## CheckWebStatus

This command checks PAM system logs to detect whether PAM service had started up.

### Parameters

- **catalina.home**

## CheckAdsStatus

This command checks ADS system logs to detect whether ADS service had started up.

### Parameters

- **catalina.home**
- **ads.check.timeout.ms** is the delay in milliseconds.

## GenerateCASKeys

This command generates unique encryption and signature keys for use by the [Federated Sign-In](#) module. Each installation procedure runs this command to generate unique keys for each deployment. A service restart is required after successful execution of this command.

Read more about synchronizing encryption and signature keys for high availability deployments in the help system.

Parameters

- **catalina.home**

## GenerateCASCipher

This command encrypts provided sensitive password using the algorithm used by the [Federated Sign-In](#) module to put to the configuration file so that sensitive password would not be stored in the configuration files unencrypted.

Read more in the system help for the information about the technique to use encrypted [Federated Sign-In](#) module passwords in the configuration files.


Parameters

- **catalina.home**
- **password** might be a password itself or a dash to prompt a user to enter a password.

## GenerateCertificate

This command generates a unique certificate bundle for use by the WEB Session manager to protect traffic between the PAM master node and the WEB Session Manager. The command also uploads the bundle into the ADS storage.

Parameters

- **catalina.home**
- **bundle.file.name** is the file name for the generated new  bundle.

## ExportCertificate

This command extracts the WEB Session Manager certificate bundle from the ADS storage to the local file system.

Parameters

- **catalina.home**
- **bundle.file.name** is the file name for the extracted new ZIP bundle. For example, `pamcert.zip`

## File

This command allows one to replace all positional command line parameters with the instruction file that contains all these parameters named with the names given in this guide. This option provides better control over the command execution by automated scripts and over special characters that can appear in the parameter.

See more details about the instruction file structure with the example in the Common Parameters File description in this guide.

## EnableNonOpenMode

This command enables non-open mode in [Federated Sign-In module](#) that forbids logins to the PAM WEB application with the unapproved destination service provided in the login URL.

Note that the only method to change managed service on the application login is to edit the login URL in the browser. The attempt to login to the unapproved destination service is not a security risk but it may resolve some audit findings

Parameters

- **catalina.home**

## Tool Commands

This section describes the utility commands to test various connections, certificates, encryptions, to establish trusts, and help to understand deployment environments and relationships between system components.

Parameters for commands in this section could only be specified as positional command line parameters.

## Sign

This command signs a binary file with the signature key from the provided key store. PAM Server can verify the signature using the public key certificate included with every deployment.

Parameters

- **KEYSTORE\_PATH** – path to the keystore with the signature private key
- **KEYSTORE\_PASSWORD** – password to the keystore
- **FILE\_PATH** – binary file to sign

## Encrypt

This command encrypts a provided text string so it could be used in the configuration file `$PAM_HOME/web/conf/catalina.properties` for sensitive data. PAM Server internally decrypts passwords in the configuration files encrypted by this command.

### Parameters

- **SECRET** is the secret sensitive data to decrypt. Alternatively, it is possible to type dash (-) instead of the data itself for the command to prompt user to type the data in the hidden prompt.

## TestCertificate

This command attempts to connect to the provider HTTPS URL to test the validity of the certificate securing this URL endpoint. The command issues a connection error in case of issues.

### Parameters

- **URL** is the HTTPS URL to connect

## SSLPoke

This command attempts to connect to the TCP endpoint given by host and port parameters. After connection the command obtains a certificate from the connected endpoint and analyzes its validity.

### Parameters

- **Host** is the endpoint host
- **Port** is the endpoint port

## SSLImport

This command connects to the specified TCP endpoint, validates its SSL certificate and imports it to the PAM Server keystore. After successful connection, the command lists all certificates from the certificate chain retrieved from the connected endpoint allowing a user to import selected certificates into the PAM Server keystore. The command also generates errors of certificate validation and trust in case of the detected certificate or trust issues.

The command is useful to establish trust for PAM Server with various components connected using various protocols in case the protocols are secured by the self-signed SSL certificate generated in-house as oppose to

well-known Internet certificate authorities. Examples of such components include: MS Active Directory, external LDAP server (eDirectory, OpenLDAP), PAM Remote Session Manager, PAM ADS, PAM WEB Container, PAM Load Balancer, etc

#### Parameters

- **Host** is the endpoint host
- **Port** is the endpoint port
- **in-place** is an optional parameter with true (default) or false values that allows to import the certificate into the temporary local file instead of directly to the PAM Server keystore

#### Example

```
1 | ./bin/PamDirectory.sh SSLImport remote-session-manager-host 4822
```

## ADTest

This command tests connection to the provided LDAP server without making configuration changes in the system.

#### Parameters

- **LDAP\_SERVER** is an LDAP server host or URL
- **LDAP\_USER** is an LDAP server user
- **LDAP\_PASSWORD** is an LDAP server password or a dash to prompt a user to enter a password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

## DecryptFile

This command decrypts a file (such as session recording stored on the file system) encrypted by PAM Server using provided master password.

#### Parameters

- **encrypted.file** is path to the source encrypted file
- **unencrypted.file** is path to the destination decrypted file

## PublishedVersion

This command downloads the last published PAM Server version from PAM binaries content distribution network. The command allows to test the connection from the server hosting PAM deployment to the PAM CDN. The command also allows to test connection established through HTTP proxy in case direct traffic to

PAM CDN is blocked but proxy traffic is allowed.

#### Parameters

- **pam.edition** is the optional parameter with the possible values product (default) for production version or qa for QA version.
- **proxy** is the optional parameter to specify proxy host and port in the notation proxy:port to test indirect proxied connection to PAM CDN. Alternatively, specify dash (-) in this parameter to indicate that direct connection should be used instead of proxy to allow to use next positional parameter to test protocol security.
- **security.level** is the optional parameter to specify different levels of protocol security with possible values SSLv3, TLSv1, TLSv1.1, TLSv1.2.

## Break Glass Commands

This section describes summary to break glass commands. Refer to the PAM system help for more information about [break glass scenarios](#) and [workflows](#).

Parameters for commands in this section could only be specified as positional command line parameters.

## ListExport

This command lists records from the system export that match the provided criteria.

#### Parameters

- **export.file** is the full path to the export file or to the export file base: a file name without extension and export index to include all export files into the archive search.
- **match** is the criteria to search for records. The command will perform a case insensitive search for a match criterion as a substring of record name, description or host. Alternatively, a criterion might be a record ID.

## Extract

This command extracts sensitive information of the specified records from the system export and prints it on the screen. The command requires the [master password](#).

#### Parameters

- **export.file** is the full path to the export file or to the export file base: a file name without extension and export index to include all export files into the archive search.
- **name** is the criteria to search for records. The command will perform a case insensitive search for a match criterion as a substring of record name, description or host. Alternatively, a criterion might be a record ID.
- **master** is a master password to decrypt the records sensitive data. The master password might be a password itself or a dash to prompt a user to enter a password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

# Database Configuration Commands

This session describes commands that allow admins to manipulate database configuration usually performed using the application [WEB GUI](#). However, there are situations that require direct intervention to the database mostly caused by configuration mistakes that are difficult to recover. Commands in this section require master password as the authentication method.

## DBReleaseLockedAdmins

This command removes Administrator block from all workflow bindings in the system to unlock system administrators who accidentally locked themselves by applying workflow bindings they could not pass (blocking, interactive approval with missed required approvers). The command requires a valid master password.

### Parameters

- **catalina.home**
- **master** is a master password to decrypt the records sensitive data. The master password might be a password itself or a dash to prompt a user to enter a password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

## DBListUsers

This command lists cached users for further analysis. The command requires a valid master password.

### Parameters

- **catalina.home**
- **master** is a master password to decrypt the records sensitive data. The master password might be a password itself or a dash to prompt a user to enter a password. The password might start with **base64-** prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

## DBUnblock

This command unblocks the user by provided login. The command requires a valid master password.

The command is useful to unlock locked administrators in cases of single system administrator present in the system.

Note that the user block might happen because of various circumstances such as in the result of a behavior analytics rules.

### Parameters

- **catalina.home**
- **user** is the user login to unlock
- **master** is a master password to decrypt the records sensitive data. The master password might be a password itself or a dash to prompt a user to enter a password. The password might start with base64-prefix. In this case the command will treat the string after the prefix as a Base64 decoded password.

## Appendix A: Summary of commands

- SetAdminPassword catalina.home admin.password | <generate> | pam-generate
- SetMasterPassword catalina.home master.password | - | <generate> | pam-generate
- SetDBPassword catalina.home db.home db.password | <generate> | pam-generate
- Init catalina.home
- CreateUser catalina.home user.login user.firstName user.lastName user.password | GENERATE
- CreateGroup catalina.home group.name group.description [group.member]
- RenameGroup catalina.home group.name group.newName
- SetUserPassword catalina.home ads.password user.login user.password
- ADConnect catalina.home ldap.server ldap.user ldap.password
- ADQuery catalina.home ldap.query [-v]
- LdapConnect catalina.home ldap.name ldap.server ldap.user ldap.password
- LdapConnect catalina.home ldap.name DISABLE
- ADSConnect catalina.home ads.server ads.password
- ADSReplicate catalina.home ads.remote.server ads.remote.password
- ADSReplication catalina.home ads.remote.index | list ads.remote.server | delete ads.remote.password
- ADSExport catalina.home file encrypted:{true|false}
- ADSImport catalina.home file
- DBConnect catalina.home db.type:{Derby|MySQL|MSSQL|Oracle|PostgreSQL} db.server db.user db.password
- XTConnect catalina.home pam.server pam.user pam.password
- ConfigureRealms catalina.home auth.catalina.enable:true|false auth.ad.enable:true|false
- EnableSso catalina.home managed.path sso.enable:true|false
- GenerateSSL catalina.home
- CheckWebStatus catalina.home
- GenerateCASKeys catalina.home
- GenerateCASCipher catalina.home {SECRET|-}
- CheckAdsStatus catalina.home ads.check.timeout.ms
- GenerateCertificate catalina.home bundle.file.name
- ExportCertificate catalina.home bundle.file.name
- File PATH\_TO\_INSTRUCTION\_FILE



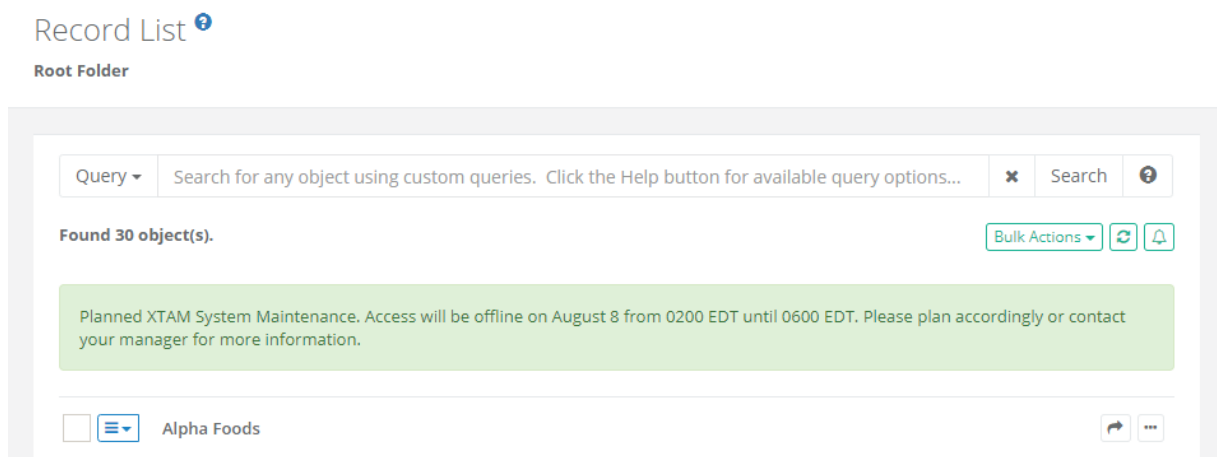
- Sign KEYSTORE\_PATH KEYSTORE\_PASSWORD FILE\_PATH
  - Encrypt SECRET
  - TestCertificate URL
  - SSLPoke host port
  - SSLImport host port [in-place:true|false]
  - ADTest LDAP\_SERVER LDAP\_USER LDAP\_PASSWORD
  - Extract export.file name|id master|-
  - ListExport export.file match
  - DecryptFile encrypted.file unencrypted.file
  - PublishedVersion [product|qa] [proxy:port|-] [SSLv3|TLSv1|TLSv1.1|TLSv1.2]
- 
- DBReleaseLockedAdmins catalina.home master|-
  - DBListAdmins catalina.home master|-
  - DBMakeAdmin catalina.home login master|-
  - DBListUsers catalina.home master|-
  - DBUnblock catalina.home user master|-
  - EnableNonOpenMode catalina.home

## Administrative Messages

### How to Display a Message to all PAM Users.

Administrative Messages allows PAM System Admins to easily deliver common messages to all logged in users. Administrative Messages, similar in concept to a message of the day (MOTD) in Unix, will appear when all users log in to PAM or when they navigate to any Records view (All Records, Shared with Me, Personal Vault and Favorites).

These messages can be configured to appear continuously, until they expire or deleted, or to appear only once per user.



## Create or Manage Administrative Messages

1. Login in PAM with a System Administrator account. Only System Administrators can create and manage messages.
2. Navigate to Management > Messages and click the **Create** button.
3. Enter your plain text message into the **Message** field. The maximum message length is 1024 characters, including spaces.
4. Check the **Show Once** box to have it appear once per user. Do not check the box to generate a continuous message. Continuous messages will remain visible to users until they expire or until the message itself has been deleted by a System Administrator.
5. Select an **Expiration Date** for when the message will be removed from display (expired messages are not deleted). An expiration date is required.
6. Click the **Create** button to complete the process.

These message will appear immediately for users. Currently logged in users will see the message once their Records page is refreshed.

You can create multiple messages and each will be visible until they expire or are deleted.

Messages				
Found 9 messages.				<a href="#">Create</a> <a href="#">Delete</a> <a href="#">Refresh</a>
	Created	Expiration date	Show once	Message
<input type="checkbox"/>	08/14/2020 11:38	08/21/2020 23:59		Planned XTAM System Maintenance. Access will be offline on August 8 from 0200 EDT until 0600 EDT. Please plan accordingly or contact your manager for more information. <a href="#">...</a>
<input type="checkbox"/>	08/12/2020 08:36	08/17/2020 00:00	<input checked="" type="checkbox"/>	System Maintenance coming soon. Contact your manager for more information. <a href="#">...</a>

To Edit a message, simply select the **Edit** option from the Actions menu to the right of any message.

To Delete a message, simply select the message from this Messages page and click the **Delete** button. Deleted messages will be removed from view.

## View Administrative Messages

All users logged into PAM will see all current Administrative Messages on their Records pages. Additionally, users may also read all non-deleted messages, even Show Once messages, from their Messages page.

1. Login to PAM and navigate to Management > Messages.
2. All messages, including *Show Once* messages, can be read from this page. Deleted messages will not

appear.

Messages			
Found 9 messages.			
Created	Expiration date	Show once	Message
08/14/2020 11:38	08/21/2020 23:59		Planned XTAM System Maintenance. Access will be offline on August 8 from 0200 EDT until 0600 EDT. Please plan accordingly or contact your manager for more information.
08/12/2020 08:36	08/17/2020 00:00	✓	System Maintenance coming soon. Contact your manager for more information.

## Mail Server

The Mail Server page is used to configure integration with an email provider to Send and/or Read emails using PAM. Sending emails uses the SMTP configuration and reading emails uses the IMAP configuration. PAM sends emails for functions including, but not limited to, user notifications, report delivery via email, and workflow notifications. PAM reads emails from an IMAP enabled mailbox for functions including, but not limited to, processing workflow approvals via emails.

Please use this Mail Server page to provide the configuration details required for your intended PAM use.

Note that IMAP Mailbox configuration is not required if you only want to use PAM to send emails.

Administration

Global Permissions

Global Roles

Local Users

Local Groups

Discovery

Scripts

Record Types

Tokens

Workflows

Command Control

MFA

Behavior Profiles

Settings

Updates

Reports

Searches

Management

Application Nodes

Proximity Groups

Database

Registration

Parameters

Mail Server

AD

Syslog

Save

Configuration to Send Emails

SMTP Server

Server

smtp.office365.com

Port

587

Login

test@domain.com

Password

.....

From Address

test@domain.com

Use TLS

✓

Send Test Email

Test Mail Server Setup

OAuth2 Setup

Tenant ID

00000000-0000-0000-0000-000000000000

Client ID

00000000-0000-0000-0000-000000000000

Secret Value

.....

Configuration to Read Emails

IMAP Mailbox

Server

outlook.office365.com

IMAP Port

993

Login

test@domain.com

Password

.....

IMAP Folder

Inbox/Folder1

Use TLS

✓

Test IMAP Mailbox Setup

OAuth2 Setup

Tenant ID

00000000-0000-0000-0000-000000000000

Client ID

00000000-0000-0000-0000-000000000000

Secret Value

.....

## Configuration to Send Emails

This section is required for PAM to use your SMTP server to send emails to users. Please populate the entire **SMTP Server** section with the required values and use the Test button to confirm connectivity.

Optionally, for Office 365 Mail Server integration, check the **OAuth2 Setup** button and populate the required Tenant ID, Client ID, and Secret Value parameters to use Modern Authentication. Please review the OAuth2 Setup section of this guide for more information.

## Configuration to Read Emails

This section is required for PAM to use an IMAP-enabled mailbox to read emails. Please populate the entire IMAP Mailbox section with the required values and use the Test button to confirm connectivity.

Optionally, for Office 365 Mail Server integration, check the **OAuth2 Setup** button and populate the required Tenant ID, Client ID, and Secret Value parameters to use Modern Authentication. Please review the OAuth2 Setup section of this guide for more information.

Please note that Microsoft intends to [disable Basic Authentication for IMAP in Office 365 beginning October 2022](#). When Basic Authentication for IMAP is disabled in Exchange Online, it will be required that you enable OAuth2 Setup for the IMAP Mailbox configuration if you are using the Office 365 Exchange Online service.

## Configure OAuth2 Setup for SMTP and IMAP in Microsoft Azure AD

As an alternative or requirement, to basic authentication for IMAP and/or SMTP to connect an Office 365 mailbox in PAM, we can use an OAuth2 access token.

To generate an OAuth2 access token and authenticate Office 365 Mailboxes, the following information needs to be provided from Microsoft Azure AD. This section will help you register the required application in Azure and gather the required values are defined below:

- **Directory (Tenant) ID** – The ID of the Microsoft Azure Active Directory to retrieve information from.
- **Application (Client) ID** – The ID of the application that will connect to Microsoft Azure Active Directory, which in this case is the integration connector.
- **Application (Client) Secret Value** – The key that will be used as the secret in the connection to Microsoft Azure.

Please note that Microsoft intends to disable Basic Authentication for IMAP in Office 365 beginning October 2022. When Basic Authentication for IMAP is disabled in Exchange Online, it will be required that you enable OAuth2 Setup for the IMAP Mailbox configuration if you are using the Office 365 Exchange Online service.


### *Register a new application in the Azure portal*

1. Sign in to the [Azure Portal](#) as a User Administrator role for the organization.
2. In the Azure services panel, select the **Azure Active Directory** service, and then select **App registrations > New registration**.


Microsoft Azure

Welcome to Azure!


Don't have a subscription? Check out the following options.



**Start with an Azure free trial**  
Get \$200 free credit toward Azure products and services, plus 12 months of popular [free services](#).  
[Start](#) [Learn more](#)



**Manage Azure Active Directory**  
Manage access, set smart policies, and enhance security with Azure Active Directory.  
[View](#) [Learn more](#)



**Access student benefits**  
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.  
[Explore](#) [Learn more](#)

**Azure services**

[Create a resource](#)

[Azure Active Directory](#)

[App registrations](#)

[Azure AD Domain...](#)

[Subscriptions](#)

[Cost Management...](#)

[Quickstart Center](#)

[Virtual machines](#)

[App Services](#)

[More services](#)

Home > ISXRUNAS

ISXRUNAS | App registrations

Overview

Preview features

Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations**
- Identity Governance

+ New registration

Endpoints

Troubleshooting

Refresh

Download

Preview features

Got feedback?

All applications

**Owned applications**

Deleted applications

Pam

Add filters

1 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
PA Pam		6/14/2022	Current

Home > ISXRUNAS

ISXRUNAS | App registrations

+ New registration

Endpoints

Troubleshooting

Refresh

Download

Preview features

Got feedback?

All applications

**Owned applications**

Deleted applications

Pam

Add filters

1 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
PA Pam		6/14/2022	Current

3. When the Register an application page appears, enter your application's registration information:
  - a. **Name** - Enter a meaningful application name that will be displayed to users of the app.
  - b. **Supported account types** - Accounts in this organizational directory only.
  - c. **Redirect URI** - '<http://localhost>'.

Microsoft Azure

Home > ISXRUNAS >

## Register an application

**\* Name**  
The user-facing display name for this application (this can be changed later).

Pam ✓

**Supported account types**  
Who can use this application or access this API?

☒ Accounts in this organizational directory only (ISXRUNAS only - Single tenant) ✓  
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)  
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)  
☐ Personal Microsoft accounts only

[Help me choose...](#)

**Redirect URI (optional)**  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web Web http://localhost ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

**Register**

## Locate Tenant ID and Client ID

1. In the Microsoft Azure portal, navigate to the application you created in the previous step.
2. Copy the IDs from **Directory (tenant) ID** and **Application (client) ID** boxes.

Home > ISXRUNAS >

**Pam**

Search (Ctrl+/)

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : Pam

Application (client) ID : [REDACTED]

Object ID : [REDACTED]

Directory (tenant) ID : [REDACTED]

Supported account types : My organization only

Client credentials : 0.certificate\_1.secret

Redirect URIs : 1.web\_0.spa\_0.public.client

Application ID URI : Add an Application ID URI

Managed application in L... : Pam

Get Started Documentation

### Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

## Locate Application Secret Value

1. In the Microsoft Azure portal, navigate to the application you created in the previous step.
2. Select the **Client credentials** parameter.

Home > ISXRUNAS >

**Pam**

Search (Ctrl+/)

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : Pam

Application (client) ID : [REDACTED]

Object ID : [REDACTED]

Directory (tenant) ID : [REDACTED]

Supported account types : My organization only

Client credentials : 0.certificate\_1.secret

Redirect URIs : 1.web\_0.spa\_0.public.client

Application ID URI : Add an Application ID URI

Managed application in L... : Pam

Get Started Documentation

### Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

3. Create a new client secret by navigating to the *Client secrets* tab and click on **New client secret**.

## Pam | Certificates &amp; secrets

Search (Ctrl+/)

Got feedback?

Overview  
Quickstart  
Integration assistant

## Manage

Branding & properties  
Authentication  
Certificates & secrets  
Token configuration  
API permissions  
Expose an API  
App roles  
Owners  
Roles and administrators  
Manifest

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
-------------	---------	-------	-----------

No client secrets have been created for this application.

#### 4. Complete this new client secret process to generate a **Secret Value** for this registered application.

## Pam | Certificates &amp; secrets

Search (Ctrl+/)

Got feedback?

Overview  
Quickstart  
Integration assistant

## Manage

Branding & properties  
Authentication  
Certificates & secrets  
Token configuration  
API permissions  
Expose an API  
App roles  
Owners  
Roles and administrators  
Manifest

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value
-------------	---------	-------

No client secrets have been created for this application.

## Add a client secret

Description Pam Client Secret

Expires Recommended: 6 months

Add

Cancel

## Pam | Certificates &amp; secrets

Search (Ctrl+/)

Got feedback?

Overview  
Quickstart  
Integration assistant

## Manage

Branding & properties  
Authentication  
Certificates & secrets  
Token configuration  
API permissions  
Expose an API  
App roles  
Owners  
Roles and administrators  
Manifest

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

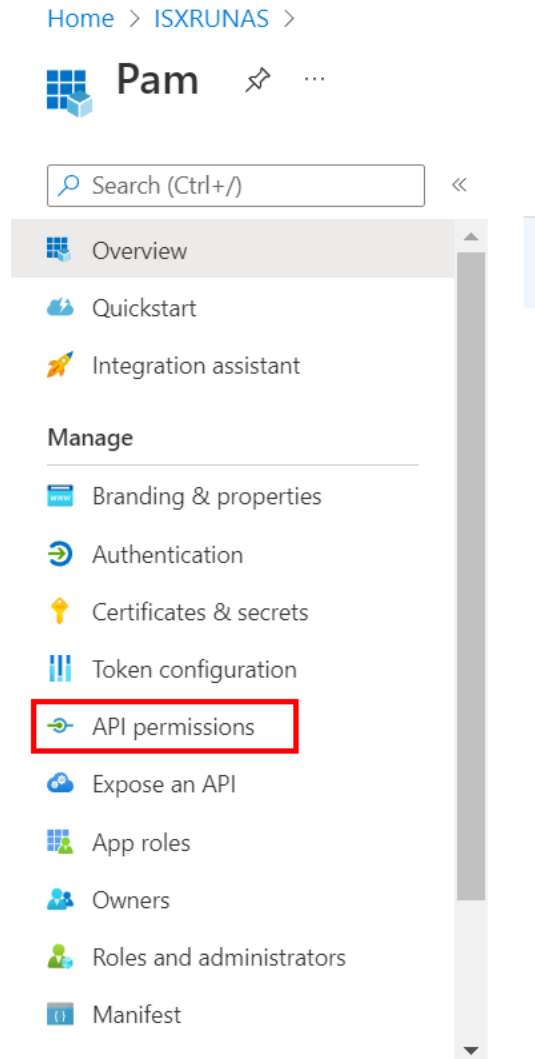
Description	Expires	Value	Secret ID
Pam Client Secret	12/14/2022		



## Configure Required Application Permissions

To authenticate SMTP and IMAP by OAuth2 access token requires certain delegated permissions from the Microsoft Graph section. Set permissions by navigating to the app's API permissions section and clicking Add permission as shown below.

1. Find and select the application you created previously.
2. Select the **API permissions** option and then **Add permission**.



Search (Ctrl+/) Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets
  - Token configuration
  - API permissions**
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest

## Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) ☒ Grant admin consent for ISXRUNAS

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	No	Granted for ISXRUNAS
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	Granted for ISXRUNAS

To view and manage permissions and user consent, try [Enterprise applications](#).

### 3. From the *Microsoft APIs* section, select **Microsoft Graph**.

Search (Ctrl+/) Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets
  - Token configuration
  - API permissions**
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest

The "Admin consent" not reflect the value

## Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs.

[+ Add a permission](#)

API / Permissions name
Microsoft Graph (1)
User.Read

To view and manage permissions and user consent, try [Enterprise applications](#).

### Request API permissions

Select an API

**Microsoft APIs** APIs my organization uses My APIs

Commonly used Microsoft APIs



#### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



#### Azure Communication Services

Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams



#### Azure Rights Management Services

Allow validated users to read and write protected content



#### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal



#### Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data



#### Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination



#### Dynamics 365 Business Central

Programmatic access to data and functionality in Dynamics 365 Business Central

### 4. For the permission type, select **Delegated permissions**.

### Request API permissions

< All APIs



#### Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

#### Delegated permissions

Your application needs to access the API as the signed-in user.


#### Application permissions

Your application runs as a background service or daemon without a signed-in user.

- a. For IMAP, in the **Select permission** parameter, select **IMAP > IMAP.AccessAsUser.All**

## Request API permissions

< All APIs

 Microsoft Graph  
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

**i** The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
IMAP (1)	
<input checked="" type="checkbox"/> IMAP.AccessAsUser.All ⓘ Read and write access to mailboxes via IMAP.	No

Add permissionsDiscard

- b. For SMTP, in the **Select permission** parameter, select **SMTP > SMTP.Send**

## Request API permissions



< All APIs



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

smtp



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
✓ SMTP (1)	
<input checked="" type="checkbox"/> SMTP.Send ⓘ Send emails from mailboxes using SMTP AUTH.	No

Add permissions

Discard

- Back on the **Configured permissions** page, click the **Grant admin consent for <CompanyName>** option.

NOTE: this step must be done by admin user.

Home > ISXRUNAS > Pam

**Pam | API permissions**

Search (Ctrl+/) Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ☒ Grant admin consent for ISXRUNAS

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				
IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	No	Granted for ISXRUNAS
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	Granted for ISXRUNAS

To view and manage permissions and user consent, try [Enterprise applications](#).

## Complete the PAM Mail Server OAuth2 Setup

Return to the PAM Mail Server page, enable the **OAuth2 Setup** checkbox for the SMTP Server and/or the IMAP Mailbox sections and populate the required Tenant ID, Client ID and Secret Value values as generated and configured in the previous steps. Be sure to **Save** and then **Test** your configuration before completing this process.

Additional links for more information:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

<https://docs.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth#get-an-access-token>

## Customizing the Email Templates

If you wish to customize the default email templates that are used for notifications, please perform the following steps.

1. Login to the System host computer and copy the “templates” directory from here `$PAM_HOME/web/webapps/xtam/` to here `$PAM_HOME/content/`.

Please note that the target location `$PAM_HOME/content/` is defined in Administration > Settings > Parameters > Content Location and may differ depending on your configuration.

2. Modify the html files as needed. We recommend you test your updates using the “email\_test.html” template as this is only sent when using the **Test Email** option in the Mail Server configuration. Save and close each when you are done.

3. That's it! Trigger an action that causes an email notification (i.e. **Test Email** in the Mail Server configuration) in your system to test your new templates.

## Email Template Placeholders

The following placeholders are available to be used in your email templates to dynamically populate values in your recipient message bodies.

### *General Placeholders*

Placeholder	Description
{{alert.reason}}	Displays the value from the alert's Message field.
{{item.description}}	Displays the value from the item's Description field.
{{item.id}}	Displays the item's ID.
{{item.name}}	Displays the value from the item's Name field.
{{item.type}}	Displays the value from the item's Type.
{{item.url}}	Displays the URL to the item.
{{log.category}}	Displays the value from the Audit Log's Category field.
{{log.created}}	Displays the value from the Audit Log's Time field.
{{log.event}}	Displays the value from the Audit Log's Event field.
{{log.level}}	Displays the value from the Audit Log's Level field.
{{log.message}}	Displays the value from the Audit Log's Message field.
{{log.ip}}	Displays the value from the Audit Log's IP field.
{{log.object.name}}	Displays the value from the Audit Log's Object field.
{{log.object.type}}	Displays the value from the Audit Log's Type field (hidden).
{{log.user.displayName}}	Displays the first and last name value from the Audit Log's User field.
{{log.user.firstName}}	Displays the first name value from the Audit Log's User field.
{{log.user.lastName}}	Displays the last name value from the Audit Log's User field.
{{log.user.login}}	Displays the login value from the Audit Log's User field.
{{managed.path}}	Displays the value from PAM's Managed Path field. Useful for properly constructing URLs.
{{user.displayName}}	Displays the first and last name of the user which the action was taken for or applied to. For example, a record that was shared with this user.

Placeholder	Description
{{user.firstName}}	Displays the first name of the user which the action was taken for or applied to. For example, a record that was shared with this user.
{{user.lastName}}	Displays the last name of the user which the action was taken for or applied to. For example, a record that was shared with this user.
{{user.login}}	Displays the login name of the user which the action was taken for or applied to. For example, a record that was shared with this user.

## Report Placeholders

Placeholder	Description
{{report.mediaType}}	Displays the format in which the report is generated (CSV or PDF).
{{report.period}}	Displays the time period for which the report covers (Daily, Weekly or Monthly).
{{report.type}}	Displays the type of the report (Audit, Inventory, Job History, etc).
{{report.title}}	Displays the Title of the Report.
{{now}}	Displays current timestamp.
{{all_props}}	Displays additional report properties like Search Filter.

## Workflow Placeholders

Placeholder	Description
{{request.action}}	Displays the action that was requested using the workflow.
{{request.created}}	Displays the timestamp of when the request was made using the workflow.
{{request.ip}}	Displays the last IP address of the user that initiated the request.
{{request.id}}	Displays the request ID of this workflow.
{{request.reason}}	Displays the value that was entered into the Reason field when initiating the request.
{{request.reject.reason}}	Displays the value that was entered into the Reject Request Reason field when the requester's request was rejected.
{{request.requester.displayName}}	Displays the first and last name of the user that initiated the request or with whom it was granted on behalf of.

Placeholder	Description
{{request.requester.firstName}}	Displays the first name of the user that initiated the request or with whom it was granted on behalf of.
{{request.requester.lastName}}	Displays the last name of the user that initiated the request or with whom it was granted on behalf of.
{{request.requester.login}}	Displays the login name of the user that initiated the request or with whom it was granted on behalf of.
{{request.requester.ip}}	Displays the last IP address of the user that initiated the request or with whom it was granted on behalf of.
{{request.status}}	Displays the value from the workflow's Status field.
{{approve.path}}	Adds the browser based Approve shortcut link to the notification message.
{{reject.path}}	Adds the browser based Reject shortcut link to the notification message.
{{anonymous.approve.path}}	Adds the browser based anonymous Approve shortcut link to the notification message. The use of this shortcut does not require the Approver to authenticate to PAM before approving the request.
{{anonymous.reject.path}}	Adds the browser based anonymous Reject shortcut link to the notification message. The use of this shortcut does not require the Approver to authenticate to PAM before rejecting the request.

## Proximity Groups

Privileged Access Management (PAM) can be configured with multiple session manager modules and proximity groups that are used to determine which Session Manager is used to serve each remote endpoint (s).

Proximity groups can use an IP range (i.e. 10.1.1.x/24) or Host Mask (in RegEx form i.e. (.\*)\contoso\.com) or [Vault Name](#) in order to determine where the session communication is sent.

For additional information about why you may consider deploying multiple session managers, please read our blog post on this topic here: [Deployment Architecture to Scale Session Manager](#).

Once you have two or more [Session Manager modules deployed](#), you will then need to create your proximity groups. For example, computers from the network 10.0.0.x/24 will be served by Proximity Group A while computers from the network 10.1.1.x/24 will be served by Proximity Group B.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Proximity Groups.
3. Click the **Add Group** button.
4. Enter a **Group Name** to easily identify this Proximity Group.
5. Choose the **Selector**, either *IP Range*, *Host Mask*, *Vault Based*, *Folder Based* or *Composite*.



6. Click the **Add Server** button.
  - a. Enter the **Host Name** where this remote Session Manager module resides.
  - b. Enter the **Port** value of 4822 (default) or the value that was configured.

Note that you can add multiple session manager servers to a Proximity Group in order to enable PAM load balancing.

7. Click the **Create** button to save this group.
8. Once saved, the Proximity Group will be created and PAM will automatically check its connectivity. If the communication channel is successfully established, the Servers value will be displayed in **blue**, if it is successful and secured it will be displayed in **green** and if it failed to connect it will be crossed-out. Your Proximity Group is working when either blue or green, ~~crossed-out~~ will need to be resolved.

Ensure that port 4822 is open between PAM and your remote session manager server.

9. You can repeat this process as many times as needed to configure additional Proximity Groups.

Found 3 session management proximity groups.

[Add Group](#) 

Name	Filter	Servers	Actions
<b>Default Group</b> Type: Default		localhost:4822	<a href="#">Edit</a>
<b>Remote Office 1</b> Type: IP-Range	10.0.0.1 - 10.0.0.50	10.0.0.20:4822	<a href="#">Edit</a>
<b>Remote Office 2</b> Type: Host Mask	*.contoso.com	<del>192.168.1.4:4822</del>	<a href="#">Edit</a>

## Disabling Proximity Groups

Disabling Proximity Groups or Session Manager Servers is available to help block the service of a session manager to be in use.

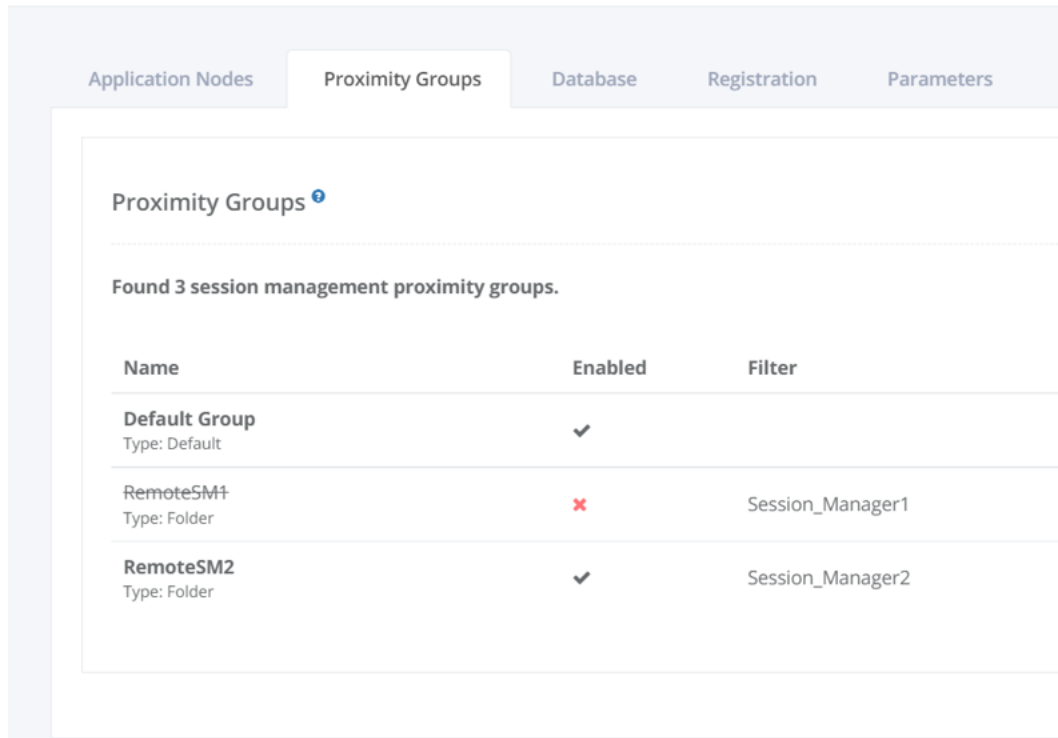
The need to Disable a Proximity Group or Server would be to perform maintenance, troubleshoot, or update the Session Manager components.

Disabling it can ensure no traffic or load will be placed on the session manager, disallowing sessions to connect.

Disabling a Proximity Group will continue to support any existing active sessions but will not have the ability to create new sessions until it is enabled again.

## To Disable a Proximity Group

1. Go to Administration > Setting > **Proximity Groups** and select the **Edit** action for the according proximity group you wish to disable.
2. **Uncheck** the Enabled checkbox section and Save the Proximity Group.
3. The disabled Proximity Group will have a strike through font in its name, as well as a X to indicate it is *disabled*.



### Example scenario with two Proximity groups

One of them being the Default Group (Local Session Manager) and the other being a new Proximity Group (Remote Session Manager):

- If PAM was installed on the master computer with session manager as a selected option during installation, *by default* a Proximity Group named **Default Group** will be set up post installation.
- If this is enabled (it will by default) and another Proximity Group is disabled, any new sessions within the disabled proximity group will automatically be supported by the local PAM (master computer) session manager.
- If a connection issue occurs trying to connect to a session, it could be because of a Proximity Group being disabled.

Navigate to the Audit Log report to verify the connection error being linked to an inactive session manager.

Please double check your Proximity Group configurations to confirm and reconfigure if needed.

Below is an example:

Time	User	IP	Object	Category	Level	Event	Message
08/29/2022 14:05:26	[REDACTED] /Local	[REDACTED]	WinTestSM2	Operation	ERROR	Connect	Cannot find active session manager for [REDACTED]

To **Enable** a proximity group, edit a disabled proximity group and select the *Enabled* checkbox, then save the proximity group.

The strike through font will disappear and a checkmark will indicate it is enabled.

An enabled proximity group will continue supporting existing active sessions and will accept new ones too.

## Disabling Servers

Within Proximity groups you may have multiple Servers supporting sessions.

At any given time, a server may require maintenance, troubleshooting, or updating of the Session Manager components.

Disabling a server (or multiple servers) can be a valid option in this case to bring one server offline while keeping others in the same Proximity Group online.

### *To Disable a Server within a Proximity Group*

1. Go to Administration > Setting > Proximity Groups and select the **Edit** action for the according proximity group you wish to disable the server within.
2. Click on the Server you wish to disable, a dropdown will appear and select **Edit**.

The screenshot shows the 'Proximity Groups' configuration page. At the top, there are tabs: 'Application Nodes', 'Proximity Groups' (selected), 'Database', 'Registration', 'Parameters', 'Mail Server', 'AD', and 'Syslog'. Below the tabs, the page title is 'Proximity Groups' with a help icon. The main content area shows 'Group: RemoteSM2' with 'Cancel', 'Save', and 'Delete' buttons. Below this, there are input fields for 'Group Name' (RemoteSM2), 'Selector' (Folder Based), and 'Folder Name' (Session\_Manager2 (Unix)). At the bottom, there is a 'Servers' section with an 'Add Server' button, a dropdown menu showing '00.000.000.00:4822', and an 'Enabled' checkbox which is checked. A dropdown menu is open for the 'Servers' section, showing 'Edit' (highlighted with a red box) and 'Remove' options.

3. **Uncheck** the *Enabled* checkbox and save. **Save** the proximity group as well, and confirm the server is disabled with a strike through font used for its Host Name.

The screenshot shows the 'Proximity Groups' configuration page. A modal dialog titled 'Add Session Manager' is open. It contains the following fields:

- Host Name:** 00.000.000.00
- Port for WEB Sessions:** 4822
- Port for Native Protocols:** Enter port for native protocols session manager (leave blank if not used or u:)
- Enabled:** ☒ (highlighted with a red box)

At the bottom of the dialog are 'Cancel' and 'Edit' buttons. Below the dialog, the configuration table shows the following entry:

Name	Type	Status	Address	Action
RemoteSM2	Type: Folder	✓	Session_Manager2 00-000-000-00 :4822	Edit

Please note if the Port Number of a Server is struck out, as opposed to its Host Name, that indicates the Server is enabled, but connectivity to it using this defined port was not successful. Check and fix your network connectivity between the PAM Node and the Remote Server using this port to reestablish the connection.

If there is slowness when loading the *Proximity Groups* page, it could be that there are a large number of proximity groups configured. In such cases, please **add** the following property `"xtam.api.config.check_groups.threads_per_request=10"` to `catlina.properties` and set a value **> 5**.

**Restart** Pam manager and verify performance. The default value for this property is 5.

## Export and Import

PAM provides an export option so that your database (configuration, settings, logs and records) can be safely stored for security, import and “break glass” procedures.

The export option can be performed automatically (encrypted) or on-demand (encrypted or decrypted).

If the export is performed with encryption (our recommendation), then your PAM [Master Password](#) will be required in order to decrypt the secured data.

If an Export is being executed inside a Vault Parent. Trying to import this export will give an error and will need to change the type from vault to folder, if importing inside a vault or folder container. Vaults cannot be created inside containers.

Importing your data to PAM from a previously created Export provides a System Administrator with the ability to recover from a loss of data or to rebuild a PAM deployment on a new host.

Some common use cases for Import include:

- Disaster recovery.
- Data loss recovery.
- Populating a test or UAT environment with data.
- Switching to a different PAM database.

And as with all things, the following items must be considered when considering and performing an import:

- This procedure is similar to a database import, meaning all data currently in PAM will be replaced with that from the import. The process will remove all data currently in PAM and import only what is contained in the export.
- If the import is using an encrypted export (which we recommend), then you will need to know the Master Password if importing to a new system.
- The PAM instance that will be importing must be equal or newer in version number to the PAM instance that created the export.

## Automatically export of PAM Database

To export your System Database Automatically:

1. Login to PAM using a System Administrator account.
2. Navigate to Administration > Settings > **Parameters**.
3. Enter or accept the default location in the **Export Location** field to define the export storage location. Use `$PAM_HOME` to define the PAM installation location. Click the **Save** button to its right to save your change.
4. Enter a value (measured in minutes) into the **Export Schedule** field. This value will be the number of minutes between automated exports (enter a zero value to disable the automated export). Click the **Save** button to its right to save your change.
5. An event (Category: Application; Level: Info; Event: Export) will be created in the Audit Log when the export is complete.
6. The export is now saved to your Export Location in a archived zip format, possibly multi-part if the export is large. The naming convention is: `xtamexp-YYYYMMDDHHMMSS-{EventID}-{multipart}.zip`

The first export will be immediately added to the PAM queue. Subsequent exports will take place in intervals based on the value entered into the Export Schedule parameter.

All automated exports will be executed with encryption.

## On-Demand export of PAM Database

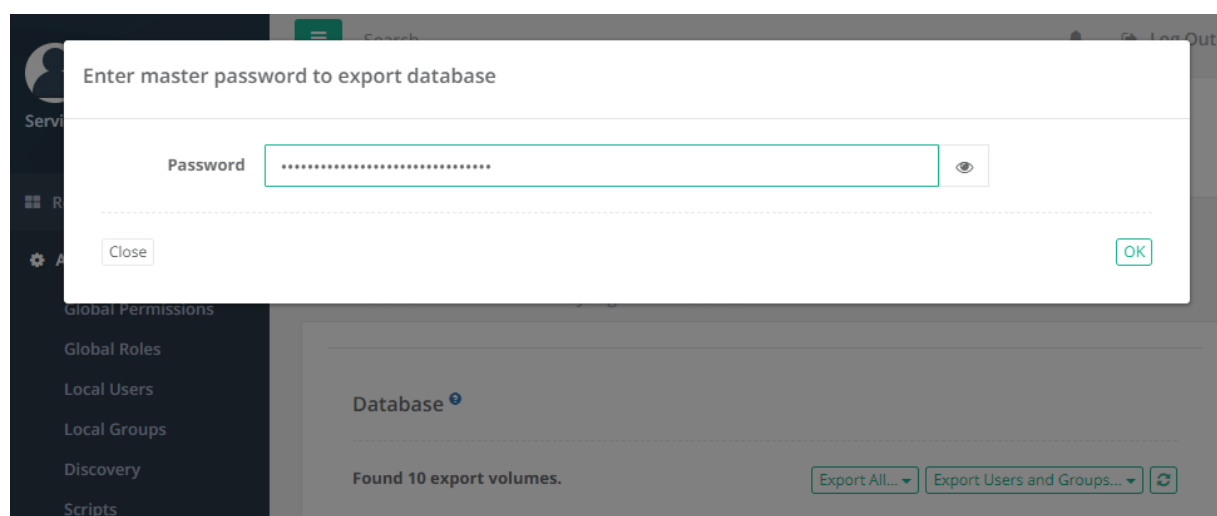
To export your PAM Database On-Demand:

1. Login to PAM using a System Administrator account.
2. Navigate to Administration > Settings > **Parameters**.
3. Enter or accept the default location in the Export Location field to define the export storage location. Use `$PAM_HOME` to define the PAM installation location. Click the **Save** button to its right to save your change.
4. Navigate to Administration > Settings > Database.

5. Choose your desired export option to queue the Export procedure:
  - Export All Encrypted / Decrypted – Performs a full system export including all objects, historical logging and configuration.
  - Express Export Encrypted / Decrypted – Performs a limited system export that includes objects and configuration, but does not include historical log data like Audit, Job, Change History and others.
6. An event (Category: Application; Level: Info; Event: Export or Event: Express export) will be created in the Audit Log when the export is complete.
7. The export is now saved to your **Export Location** in a archived zip format, possibly multi-part if the export is large. The naming convention is: **xtamexp-YYYYMMDDHHMMSS-{EventID}-{multipart}.zip** or **xtamexp\_express-YYYYMMDDHHMMSS-{EventID}-{multipart}.zip**.

The export will be immediately added to the PAM queue and will be performed a single time.

If the export includes encryption (*recommended*), the PAM Master **Password** will be required to access its secured data; however if it is exported decrypted (*not recommended*), then the secured data can be accessed without requiring any passwords.



## System Export Retention

All system exports are stored indefinitely, however if you would like to implement a retention schedule for your exports (includes both Scheduled and On-Demand exports) then please configure the option described below.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Parameters > **System Export Retention**.
3. Enter a value (defined in Days). PAM will delete all system export files after this specified number of days. A value of 0 (zero) will disable the retention schedule.
4. Click the **Save** button next to this option.

Please note that this retention schedule is applied **Globally** for all system exports and exports that have been purged due to this schedule cannot be recovered.

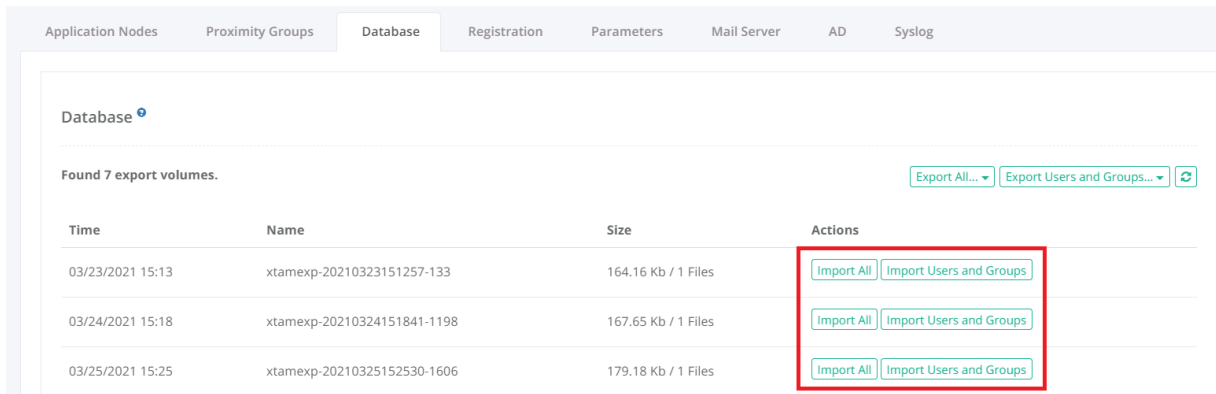
# Import back into the same PAM deployment

## How to Import back into the same PAM deployment using an Encrypted or Decrypted Export.

This procedure details the steps required to import data back into the same PAM system that created the export.

This procedure supports the use of encrypted or decrypted export files.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Database.
3. In the table list of available exported volumes, locate the one you wish to use and click the **Import** button to its right.



4. The Import operation will now be added to the PAM queue and will be executed shortly. Once the import begins, completion time depends on the amount of data that needs to be imported and may take several minutes to finish.

During the import process, the application's GUI may become temporarily unavailable. To check the status of the operation, you should open the PAM log file located at `$PAM_HOME/web/logs/pam.log` and when the message *Importing Complete* appears, the operation is finished.

5. Refresh the *All Records* page to review the imported data.

## Import into a new deployment with Encrypted Export

### How to Import into a new PAM deployment using an Encrypted Export.

This procedure details the steps required to import data into a new PAM system; one that did not create the export.

This procedure supports the use of encrypted export files.

1. Install a new PAM system where and as needed.
2. Once the installation is complete, open a command line on this new host server, navigate to the folder where PAM is installed (`$PAM_HOME`) and issue the following command to update your current PAM Master Password with the one that was used to create your encrypted export.
  - a. For Windows, substitute <MASTER PASSWORD> with the master password used with your export and issue:

```
1 | bin\PamDirectory.cmd SetMasterPassword web <MASTER PASSWORD>
```

- b. For Unix or Linux, substitute <MASTER PASSWORD> with the master password used with your export and issue:

```
1 | bin/PamDirectory.sh SetMasterPassword web <MASTER PASSWORD>
```

- Copy your exported file(s) to your new PAM system and paste them into `$PAM_HOME/export/` or the custom location you defined in Administration > Settings > Parameters > Export Location.
- Login to PAM as a System Administrator.
- Navigate to Administration > Settings > Database.
- In the table list of available exported volumes, locate the one you wish to use and click the **Import** button to its right.

Application NodesProximity GroupsDatabaseRegistrationParametersMail ServerADSyslog

Database

Found 7 export volumes.

Export All...Export Users and Groups...↺

Time	Name	Size	Actions
03/23/2021 15:13	xtamexp-20210323151257-133	164.16 Kb / 1 Files	Import AllImport Users and Groups
03/24/2021 15:18	xtamexp-20210324151841-1198	167.65 Kb / 1 Files	Import AllImport Users and Groups
03/25/2021 15:25	xtamexp-20210325152530-1606	179.18 Kb / 1 Files	Import AllImport Users and Groups

- The Import operation will now be added to the PAM queue and will be executed shortly. Once the import begins, completion time depends on the amount of data that needs to be imported and may take several minutes to finish.

During the import process, the application's GUI may become temporarily unavailable. To check the status of the operation, you should open the PAM log file located at `$PAM_HOME/web/logs/pam.log` and when the message *Importing Complete* appears, the operation is finished.

- Refresh the *All Records* page to review the imported data.

## Import into a new deployment with Decrypted Export

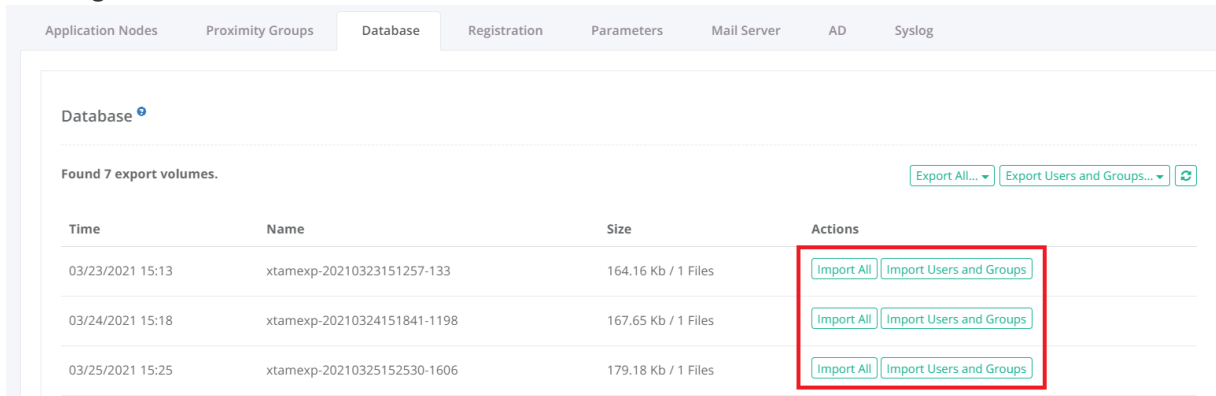
### How to Import into a newPAM deployment using an Decrypted Export.

This procedure details the steps required to import data into a new PAM system; one that did not create the export. This procedure supports the use of decrypted export files.

- Install a new PAM system where and as needed.
- Copy your exported file(s) to your new PAM system and paste them into `$PAM_HOME/export/` or the custom location you defined in Administration > Settings > Parameters > Export Location.
- Login to PAM as a System Administrator.
- Navigate to Administration > Settings > Database.



5. In the table list of available exported volumes, locate the one you wish to use and click the Import button to its right.



6. The Import operation will now be added to the PAM queue and will be executed shortly. Once the import begins, completion time depends on the amount of data that needs to be imported and may take several minutes to finish.

During the import process, the application's GUI may become temporarily unavailable. To check the status of the operation, you should open the PAM log file located at `$PAM_HOME/web/logs/pam.log` and when the message *Importing Complete* appears, the operation is finished.

7. Refresh the *All Records* page to review the imported data.

## Multi Language Support

Changing PAM's Language Settings.

PAM comes with support for translating the GUI (graphical user interface) into multiple languages.

A default is defined on a Global level so that it can be applied to all users'; however there is also a User level setting that can be defined by each PAM user personally.

The "User" level setting takes precedence over the "Global" setting when they are different.

We do our best to make the translations as accurate as possible, however there may be mistakes in spelling or grammatical phrasing. If you notice any issues with the translations or you want to inquire about additional languages, if questions remain or issues arise while using PAM, please contact the Support team: <https://support.imprivata.com/communitylogin>.

## "Global" Language

How to Configure the "Global" Language (System Administrators only):

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Parameters.
3. Locate the parameter **Language** and select your choice from the dropdown menu. *English (US)* is the default mode.
4. When complete, click the **Save** button to its right.

5. Refresh your browser.

A screenshot of a web interface showing a 'Language' dropdown menu. The dropdown is currently set to 'English (US)'. To the right of the dropdown is a question mark icon and a 'Save' button.

All users' will now see PAM in your selected language unless they override it in their User level setting as shown in the next section.


## “User” Language

How to Configure the “User” Language:

1. Login to PAM with your user account.
2. Navigate to Management > My Profile > Preferences.
3. Locate the parameter **Language** and select your choice from the dropdown menu. *English (US) is the default mode.*
4. When complete, click the **Save** button to its right.
5. Refresh your browser.

### User Profile

Home / My Profile

A screenshot of the 'User Profile' page, specifically the 'Preferences' tab. The page has a header with 'Profile', 'Subscriptions', and 'Preferences' tabs. Below the tabs, there is a 'Preferences' section with a green refresh icon. At the bottom of this section, there is a 'Language' dropdown menu set to 'English (US)', a question mark icon, and a 'Save' button.

Your personal login will now see PAM in your selected language regardless of the setting that has been applied at the Global level.

## Registration

### Privileged Access Management Software Registration or Activation.

Privileged Access Management (PAM) can be registered in either online or offline mode.

Online mode is used when the computer where PAM is installed has an open connection to the internet and Offline mode is used when this computer does not.

Below, we will walk-through the registration process for both modes, starting with the most common Online Registration.

## Online Registration

Online (Automatic) registration should be used when the PAM computer has an open connection to the internet.

This process simply verifies the entered activation code against our license server and immediately returns a response.

The following steps should be performed when registering the software in Online or Automatic mode:

1. Login to PAM using a System Administrator account.
2. Navigate to Administration > Settings > Registration.
3. Enter your key into the **Activation Code** field.
4. Click **Automatic Registration**.
5. When the Status displays “License is Valid”, click **Save License**.
6. The software is now activated and ready for use.

If the Status field displays anything other than valid, please double check that the code was entered correctly ensuring that no leading or trailing spaces were accidentally included.

If questions remain or issues arise while using PAM, please contact the Support team using this link:

<https://support.imprivata.com/communitylogin>.

## Offline Registration

Offline (Manual) registration should be used when the PAM computer does not have an open connection to the internet.

This process requires the copying of a unique registration link to another computer that does have an open internet connection, performing the activation on this other computer and then copying back the registration response to the PAM computer.

The following steps should be performed when registering the software in Offline or Manual mode:

1. Login to PAM using a System Administrator account.
2. Navigate to Administration > Settings > Registration.
3. Enter your key into the **Activation Code** field.
4. Click **Manual Registration**.
5. A new browser window will open with a unique URL. Save this URL to a file and copy the file over to another computer with an internet connection. *If the new window does not appear, please disable any pop-up blocker you may have running.*
6. On this internet connected computer, open and load the URL in your browser. When the license response appears, save all the text from this page to a file (ensure that there are no leading or trailing spaces) and copy this file back to the internet disconnected computer.
7. Once back, open the file, copy all the text and paste it the **License** field.
8. When the Status displays “License is Valid”, click **Save License**.
9. The software is now activated and ready for use.

If the Status field displays anything other than valid, please double check that the license text was copied correctly.

If you are still having issues, please contact our Support Team <https://support.imprivata.com/communitylogin> for further assistance.

The image below shows a successfully registered license regardless of the method used.

The screenshot shows the 'Registration' tab in the 'Application Settings' interface. At the top, there are tabs for 'Application Nodes', 'Proximity Groups', 'Database', 'Registration' (selected), 'Parameters', and 'Mail Server'. Below the tabs, there are three buttons: 'Save License', 'Automatic Registration', and 'Manual Registration'. The main content area displays the license status as 'License is Valid'. Below this, there is a section for 'Activation code' showing 'cd' followed by a masked field and '8f'. The 'License' section shows a detailed license string starting with '-----LICENSE BEGIN-----', followed by 'Activation:cd', 'Product:PAM', 'HUB:XtonTech', and 'Client:di@xtontech.com'.

*Please note that if the software is not activated, then it will run in its default “Trial” mode which is limited by both time and record count.*

## Active Directory Integration

To integrate your Active Directory with PAM, you may configure your settings during or after installation.

PAM does not have any limitation on the version or functional level of Active Directory. It is recommended to use a version that uses TLS 1.2.

If you are looking to integrate with additional AD or LDAP domains, please review our [Multi-domain Configuration](#) article.

If you are looking to integrate with NetIQ eDirectory, please review our [NetIQ eDirectory Integration](#) article.

We recommend using an Active Directory account whose password does not change. If the password of this account does change, PAM’s integration with your Active Directory will no longer work resulting in AD users being unable to login to PAM. If your AD integration account password does change, then you can follow the procedure outlined in the section *To configure or update an Active Directory binding After Installation* on this page to update PAM with your new password.

## Active Directory binding During Installation

To configure an Active Directory binding During Installation:

1. When the installation wizard reaches the section named Active Directory enter the following values:
  - a. **LDAP Server:** Enter the host name or IP address of your Active Directory Domain Controller.
  - b. **User:** Enter the user name of the account that can connect to this server.

- c. **Password:** Enter the password of this user.
2. Click the **Connect** button to test your connection.
3. If the test connection was successful, click the **Next** button to continue. If the test connection failed, check your values and try again.

Imprivata Privileged Access Management Setup

**Active Directory**  
Optionally, define connection to the enterprise user directory

LDAP Server: ad.domenexample.com  
User: user@ad.domenexample.com  
Password: [masked]  
Connect

Copyright (c) 2025 Imprivata, Inc.

< Back   Next >   Cancel

## Active Directory binding After Installation

To configure or update an Active Directory binding **After Installation**:

(June 4, 2018) – If you have updated to PAM version 2.3.201806032154 or later, you can now configure Active Directory integration by simply navigating to Administration > Settings > AD within the PAM interface.

1. **Login** to the server where PAM is deployed as an Administrator.
  2. Open a command line and navigate to the folder where PAM is installed (\$PAM\_HOME) and issue the following command:
- for Windows, substitute your **ldap.server**, **ldap.user** and **ldap.password** values and issue:

```
1 | bin\PamDirectory.cmd ADConnect web ldap.server ldap.user ldap.password
```

- for Unix or Linux, substitute your **ldap.server**, **ldap.user** and **ldap.password** values and issue:

```
1 | bin/PamDirectory.sh ADConnect web ldap.server ldap.user ldap.password
```

Please note if your password contains any of the following characters & \ < > ^ | then they must be properly escaped when executing the command by placing a ^ before each like this for ampersand ^&. Alternatively, you can issue the command using a dash – rather than the password in which case you will be prompted to enter the password during execution and in this approach, those special characters do not have to be escaped.

3. If the command returns an *OK* response, then restart the PamManagement (Windows) or pammanager (Linux) service on this computer:

- for Windows:

```
1 | net stop PamManagement
2 | net start PamManagement
```

- for Unix or Linux:

```
1 | service pammanager restart
```

4. If the command returns a *Fail* response, then double check your user and password values. For the {ldap.user} value, be sure to use the **user@domain** format.
5. Active Directory integration is now complete. Objects and permissions may now be shared with AD Users and Groups in PAM.

To support [self-password reset in PAM for your AD users](#), you must configure your AD integration using LDAPS and the defined LDAP binding account must be able to reset the password of other users in this Active Directory

## Unable to Connect to AD services

### Unable to Connect to AD services due to PKIX Path Building Failure when using multiple AD servers behind a Load Balancer.

For the PAM server to communicate with an AD global catalog (GC), the PAM keystore needs to contain a security certificate from this global catalog to establish a trusted connection.

During setup of the integration with AD (whether using GUI or the command ADConnect) PAM automatically imports this certificate from your AD GC server into its PAM keystore so that integration with AD is performed smoothly.

However, in case of multiple GC servers operating behind a load balancer, it is not enough for PAM to include a certificate from a single GC server obtained during initial connection setup because every time PAM needs to communicate with the global catalog, the GC load balancer can route the connection to different GC server set up with a different certificate.

Since PAM does not know how to access each GC server hidden behind the load balancer, the certificates from each GC server should be imported manually into the PAM keystore.

This way, after the integration PAM will trust each GC server no matter which one will be used at any given time by the load balancer.

## Several ways to move forward

First, you need to obtain certificates from GC servers and then these certificates should be imported to the PAM keystore (`$PAM_HOME/jre/lib/security/cacerts`).

Below is the link with the procedure how to import certificates into PAM's keystore.

[Importing Certificates](#)

Please note that the article contains several sections about how to convert your cert to DER format if it is not in der format. You need to run these commands from the `$PAM_HOME` folder to keep all the paths like they are in the article's examples.

**Alternatively**, if you can access each global catalog server directly around the load balancer, you can establish connections with each global catalog server one-by-one using ADConnect.

During every connection PAM will automatically import the certificate from each GC server into its own keystore.

At the end, you can re-establish the connection to the GC load balancer. At this time, PAM will have all certificates loaded into the keystore and will be able to trust any of the connections no matter which one is used.

For both alternative ways to connect it is important to import certificates from all GC servers because GC load balancer might route LDAPS traffic from PAM to any one of them.

## Can't add any new AD users

Can't add any new AD users when logged in as my local pamadmin account.

When I go to the AD tab and test, I get this error:

Active Directory Configuration Failed to Test.: 501: LDAP: error code 49 - 80090308: LdapErr: DSID-0C090447, comment: AcceptSecurityContext error, data 533, v3839.

### *Here are some other reasons for error 49*

The AD-specific error code is the one after "Data":

- 525 user not found
- 52e invalid credentials
- 530 not permitted to logon at this time
- 531 not permitted to logon at this workstation
- 532 password expired
- 533 account disabled
- 701 account expired

- 773 user must reset password
- 775 user account locked

## Syslog

Many companies choose to centralize security and network logging to a single Syslog server or appliance to reduce the burden of log collection, investigation and reporting across many devices.

While PAM does include its own logging engine that captures and stores events, it can also be configured to output this information to your centralized syslog server.

## Syslog server

To output PAM audit log events to your syslog server, please perform the following steps.

You can now configure Syslog integration by simply navigating to Administration > Settings > **Syslog** within the PAM interface.

To understand what types of Audit events are logged by level, please read this [article](#).

1. On the host where PAM is installed, open the file `$PAM_HOME\web\conf\log4j.pam.properties` in a text editor.
2. Modify the second line of this file  
from this: `log4j.rootLogger=INFO, file, stdout`  
to this: `log4j.rootLogger=INFO, file, stdout, SYSLOG`
3. At the end of the file, copy and paste the following lines of code:

```
1 # Syslog Messages
2 log4j.appender.SYSLOG=org.apache.log4j.net.SyslogAppender
3 log4j.appender.SYSLOG.threshold=INFO
4 log4j.appender.SYSLOG.syslogHost={add your Syslog Host name or IP address here}
5 log4j.appender.SYSLOG.facility=LOCAL4
6 log4j.appender.SYSLOG.header=true
7 log4j.appender.SYSLOG.layout=org.apache.log4j.PatternLayout
8 log4j.appender.SYSLOG.layout.conversionPattern=XTAM [%p] %c{3.}:%L - %m%n
```

4. Modify the `log4j.appender.SYSLOG.syslogHost=` line above to add your *Syslog host name* or *IP address*. If you wish to use a non-standard port, then simply add your custom port number to the end of your Syslog name or IP address. `:port`.
5. When finished, **Save** and close this file.
6. The syslog output is delivered over the UDP port by default, so if necessary ensure that port 514 is open.
7. Restart the service **PamManagement** (Windows) or **pammanager** (Linux).

Once the service has completed the restart process, your Syslog server or appliance should immediately begin receiving audit log events from PAM.



# Message Filtering

It is possible to filter messages sent to syslog server to reduce the traffic processed by SIEM server.

To enable filtering, add the following properties at the end of the SYSLOG configuration.

The example below filters all audit log messages generated by PAM about the record Local Unix.

```
1 | log4j.appender.SYSLOG.filter.1=org.apache.log4j.varia.StringMatchFilter
2 | log4j.appender.SYSLOG.filter.1.StringToMatch=Class: Record, Name: Local Unix
3 | log4j.appender.SYSLOG.filter.1.acceptOnMatch=true
4 | log4j.appender.SYSLOG.filter.2=org.apache.log4j.varia.DenyAllFilter
```

These four additional lines in the **log4j** make it possible to SYSLOG only those events that match the *String Match* filter. It takes this value, searches for that in the message and if found, sends it out.

The *DenyAllFilter* class drops the rest of the messages from output.

In our example, it searches for “**Class: Record, Name: Local Unix**” which would send out any events specific to a record (Class:Record) with the name Local Unix (Name: Local Unix).

To include several *String Match* filters, the configuration would be like in the example below.

As above, this configuration will forward Audit Log messages about Local Unix record.

Also, the configuration will forward the messages about system admin account authentications.

```
1 | log4j.appender.SYSLOG.filter.1=org.apache.log4j.varia.StringMatchFilter
2 | log4j.appender.SYSLOG.filter.1.StringToMatch=Class: Record, Name: Local Unix
3 | log4j.appender.SYSLOG.filter.1.AcceptOnMatch=true
4 | log4j.appender.SYSLOG.filter.2=org.apache.log4j.varia.StringMatchFilter
5 | log4j.appender.SYSLOG.filter.2.StringToMatch=Event: Login, User: pamadmin
6 | log4j.appender.SYSLOG.filter.2.AcceptOnMatch=true
7 | log4j.appender.SYSLOG.filter.3=org.apache.log4j.varia.DenyAllFilter
```

Below is another example to demonstrate two *String Match* filters to exclude certain messages from the stream:

```
1 | log4j.appender.SYSLOG.filter.1=org.apache.log4j.varia.StringMatchFilter
2 | log4j.appender.SYSLOG.filter.1.StringToMatch=HTTP\ tunnel\ request\ failed
3 | log4j.appender.SYSLOG.filter.1.acceptOnMatch=false
4 | log4j.appender.SYSLOG.filter.2=org.apache.log4j.varia.StringMatchFilter
5 | log4j.appender.SYSLOG.filter.2.StringToMatch=i-exWj2vOI6R2
6 | log4j.appender.SYSLOG.filter.2.acceptOnMatch=false
```

Note that spaces in the message filter should be escaped by the preceding slash.

Note that filters only work on the message part of the stream event, not on the class or level. To exclude events sent by the certain sources (classes) from the stream (or to change level of the events streamed) use general log configuration line such as `log4j.logger.com.package.package.ClassName=OFF`

After adding these lines, **restart the PAM service** to test the SYSLOG output.

For log4j2, please refer section Adding Syslog configuration to [log4j2](#).

## Audit Log Events

### Event Levels

The levels *Info* and *Error* are used by PAM to communicate information about all events: successful (for level Info) or unsuccessful (for level Error).

The majority of the messages of Info and Error levels come from the Audit Log report at the same time when they appear to the audit log itself.

However, the application communicates some internal states also, such as installing session or key recording for sessions, details of servers startup, etc as Info messages and all internal system errors (these should not happen but sometimes occur) as Error messages.

Additionally, PAM uses *Debug* and *Trace* levels for internal debugging purposes. Sometimes to investigate certain situations with customer deployments, our Support team may ask the customer to enable a higher level debug for troubleshooting purposes.

Some of the application components, especially those related to integration (i.e. LDAP, PowerShell or SSH scripts executing) generate a lot of debug and especially trace messages when enabled.

We do not anticipate users to actually use Trace and Debug message for reasons other than troubleshooting purposes as they do not carry useful business level information.

### Event Categories

- **Analytics:** Relates to events that are generated from the Behavior Analytics service.
- **Application:** Relates to events that the application itself is generating. This includes software updates, health checks, various global configurations and exports.
- **Data:** Relates to the events that are generated when working with the data stored in PAM (containers and records). This includes events like *Create/Update/Delete*, *Lock/Unlock* secured fields, *Copy/Move/Link*, *Record Type* events, *Reports* and Anonymous Link interactions (*create*, *open*).
- **Event:** Relates to events that are generated during sessions. These are the keystrokes, clipboard and file transfer events.
- **Operation:** Relates to events that are generated through the operation of the software, either by users or the service itself. This includes various operations like Authentication into PAM (*login/logout*), *Discovery Query* events, *Queue* events, Session Events (*join*, *left*, *terminate*, *created* and *connect* options).
- **Permissions:** Relates to events that are generated when modifications are made to object permissions, local directory services or public keys. For example, changes to record permissions including make or break inheritance and modifying ACLs. Local directory services includes creating users/groups, modifying groups and locking/unlocking users.

- **Policy:** Relates to events that are generated with regards to the various Policies throughout PAM. This includes Behavior Analytics, Command Control, Password Formula, Scripts, Tasks and MFA. Events include creating, updating and deleting activities.
- **Workflow:** Relates to events that are specific to workflows. Including creating, updating and publishing Bindings and Templates, notifications, approvals and steps.

For logging, PAM uses the industry standard Log4j logging mechanism for processing and filtering of its log messages.

This log configuration is located in the file `$PAM_HOME/web/conf/log4j.pam.properties`, which in turn controls the filtering for log levels for the entire application as well as for individual components.

This file also controls the destination syslog traffic with its own filtering.

Download the PAM [Syslog Messages](#) file for a list of events.

## Migration to Log4j version 2

PAM logging subsystem including integration with SIEM systems or Windows Event logging is based on log4 module.

Default new PAM installation ships with log4j version 2 embedded.

Benefits of migrating the deployment to log4j version 2 include the option to integrate with syslog SIEM systems using TCP protocol and the option to change logging configuration for different system components without restarting of the system.

The following guide described steps needed to complete to switch PAM deployment to log4j version 2. Existing environments using log4j v1 should upgrade all nodes to log4j v2 to maintain compatibility and ensure security compliance.

Please read the entire procedure outlined in the article before beginning. If you have any questions, please contact the Support team: <https://support.imprivata.com/communitylogin>.

## Migration Guide

1. [Update the PAM web module](#) to the current version.
2. **Download** and **uncompress** log4j2 archive: <https://bin.xtontech.com/product/xtam-log4j2-2.24.1.zip>
3. **Stop** PamManagement / pammanager service.
4. **Delete** all files with names starting with **slf4j\*** or **log4j\*** from two folders:

`$PAM_HOME/web/webapps/xtam/WEB-INF/lib/`

`$PAM_HOME/web/webapps/xtamWorker/WEB-INF/lib/`

If a PAM update is done manually, not through the PAM web UI, these deleted files will be added back. Files `slf4j-api-1.7.5.jar` (or `slf4j-api-2.0.7.jar`) & `log4j-1.2.17.jar` will need to be removed again after updating.

5. **Copy** file `conf/log4j2.pam.xml` from the downloaded archive to `$PAM_HOME/web/conf/` folder.
6. **Copy** all files from `lib` folder from the downloaded archive to `$PAM_HOME/web/lib/` folder.
7. ■ For Linux edit file `$PAM_HOME/bin/pammanager`

replace

```
1 | export JAVA_OPTS="$DERBY_OPTS -Dlog4j.configuration=file://$CATALINA_
   | BASE/conf/log4j.pam.properties -
   | Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
```

with

```
1 | export JAVA_OPTS="$DERBY_OPTS -Dlog4j.configurationFile=file://$CATALINA_
   | BASE/conf/log4j2.pam.xml -
   | Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
```

- After making the modifications above, this section will look similar to this example:

```
export JAVA_OPTS="$DERBY_OPTS -Dlog4j.configurationFile=file://$CATALINA_
BASE/conf/log4j2.pam.xml -Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true -
Dlog4j2.formatMsgNoLookups=true --add-opens java.base/java.lang=ALL-UNNAMED --add-
opens java.xml/com.sun.org.apache.xerces.internal.util=ALL-UNNAMED --add-opens
java.base/sun.security.provider=ALL-UNNAMED"
```

- For Windows: edit file `$PAM_HOME/bin/ServiceManagement.cmd`

replace:

```
1 | @set JAVA_OPTS=%DERBY_OPTS% -Dlog4j.configuration=file:/// %CATALINA_
   | BASE%\conf\log4j.pam.properties -
   | Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
```

with

```
1 | @set JAVA_OPTS=%DERBY_OPTS% -Dlog4j.configurationFile=file:/// %CATALINA_
   | BASE%\conf\log4j2.pam.xml -
   | Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
```

- After making the modifications above, this section will look similar to this example:

```
@set JAVA_OPTS=%DERBY_OPTS% -Dlog4j.configurationFile=file:///%%CATALINA_
BASE%\conf\log4j2.pam.xml -Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true -
Dlog4j2.formatMsgNoLookups=true --add-opens java.base/java.lang=ALL-UNNAMED --add-opens
java.xml/com.sun.org.apache.xerces.internal.util=ALL-UNNAMED --add-opens
java.base/sun.security.provider=ALL-UNNAMED
```

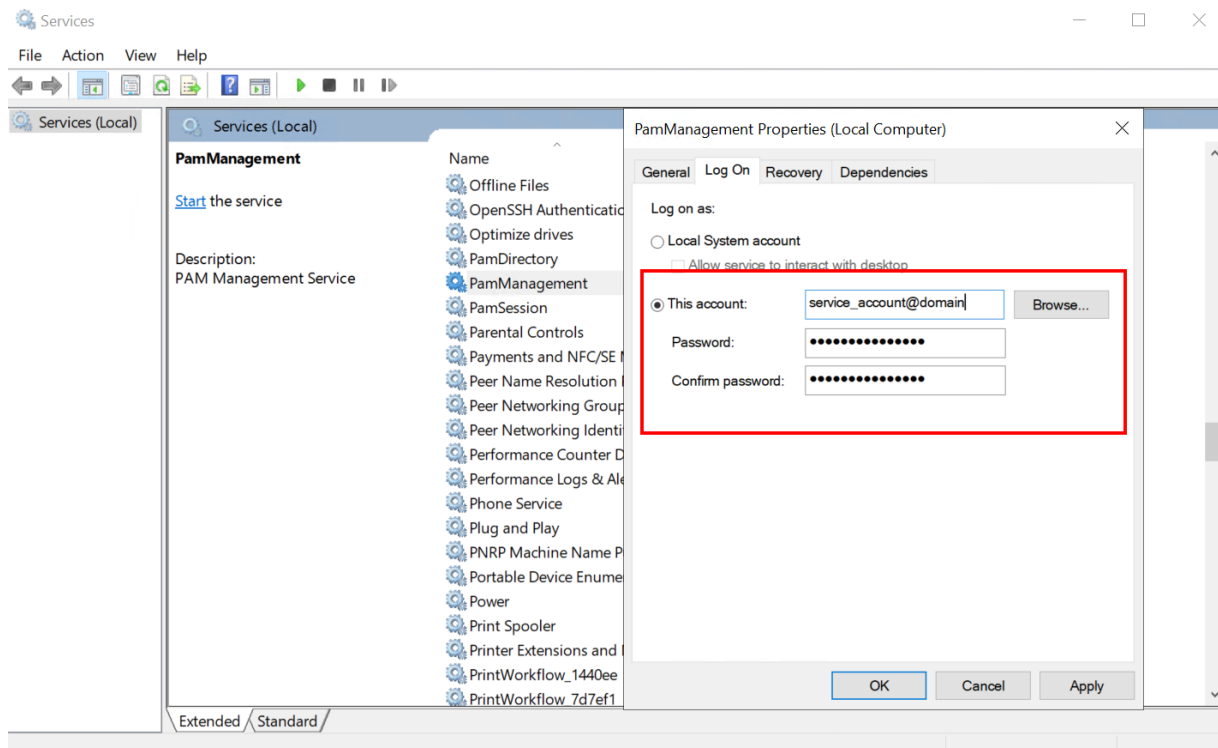
- From an administrative command prompt, navigate to \$PAM\_HOME and run the command:

```
1 | bin\ServiceManagement.cmd remove
```

- When the above command completes successfully, run the command:

```
1 | bin\ServiceManagement.cmd install
```

Note: The **PamManagement** service resets to the default *Local System account* Log on property once this service for PAM is reinstalled. If you are using a Log account other than an Local System account for this service then you must restore it prior to restarting the **PamManagement** service. Navigate to *Services* on Windows and find *PamManagement*, right-click and select **Properties**. Go to the *Log on* tab, select *This account:* and restore the required service account.



## 7. Restart PamManagement / pammanager service.

The logging level within PAM using Log4j version 2, can be configured using the file **log4j2.pam.xml**.

# Roll back to Log4j version 1

1. **Download** and **uncompress** log4j2 archive: <https://bin.xtontech.com/product/xtam-log4j2-2.23.1.zip>
2. **Stop** PamManagement / pammanager service.
3. **Copy** the following files to two folders from `lib1` folder of the uncompressed archive:

`$PAM_HOME/web/webapps/xtam/WEB-INF/lib/`

`$PAM_HOME/web/webapps/xtamWorker/WEB-INF/lib/`

`lib1/slf4j-api-1.7.5.jar`

`lib1/slf4j-log4j12-1.7.22.jar`

`lib1/log4j-1.2.17.jar`

4. **Delete** the following files from `$PAM_HOME/web/lib` folder:

`disruptor-3.4.4.jar`

`log4j-api-2.23.1.jar`

`log4j-core-2.23.1.jar`

`log4j-slf4j-impl-2.23.1.jar`

`slf4j-api-1.7.36.jar`

5. **Edit:**

- a. For Linux: edit file `$PAM_HOME/bin/pammanager`

replace

```
1 export JAVA_OPTS="$DERBY_OPTS -Dlog4j.configuration=file://$CATALINA_
  BASE/conf/log4j2.pam.xml -
  Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
```

with

```
1 export JAVA_OPTS="$DERBY_OPTS -Dlog4j.configuration=file://$CATALINA_
  BASE/conf/log4j.pam.properties -
  Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
```

- b. After making the modifications above, this section will look similar to this example:

```
export JAVA_OPTS="$DERBY_OPTS -Dlog4j.configuration=file://$CATALINA_
  BASE/conf/log4j.pam.properties -
  Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true -
  Dlog4j2.formatMsgNoLookups=true -Dlog4j2.formatMsgNoLookups=true --add-opens
  java.base/java.lang=ALL-UNNAMED --add-opens
  java.xml/com.sun.org.apache.xerces.internal.util=ALL-UNNAMED --add-opens
  java.base/sun.security.provider=ALL-UNNAMED"
```

**Refresh** the service configuration if needed.

- c. For Windows: edit file `$PAM_HOME/bin/ServiceManagement.cmd`

replace

```
1 | @set JAVA_OPTS=%DERBY_OPTS% -Dlog4j.configurationFile=file:///C:\CATALINA_
  | BASE%\conf\log4j2.pam.xml -
  | Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
```

with

```
1 | @set JAVA_OPTS=%DERBY_OPTS% -Dlog4j.configuration=file:///C:\CATALINA_
  | BASE%\conf\log4j.pam.properties -
  | Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
```

d. After making the modifications above, this section will look similar to this example:

```
@set JAVA_OPTS=%DERBY_OPTS% -Dlog4j.configuration=file:///C:\CATALINA_
BASE%\conf\log4j.pam.properties -
Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true -
Dlog4j2.formatMsgNoLookups=true --add-opens java.base/java.lang=ALL-UNNAMED --add-
opens java.xml/com.sun.org.apache.xerces.internal.util=ALL-UNNAMED --add-opens
java.base/sun.security.provider=ALL-UNNAMED
```

From an administrative command prompt, navigate to \$PAM\_HOME and run the command:

```
1 | bin\ServiceManagement.cmd remove
```

When the above command completes successfully, run the command:

```
1 | bin\ServiceManagement.cmd install
```

6. **Start** PamManagement / pammanager service.

The logging level within PAM using Log4j version 1, can be configured using the file  
**log4j.pam.properties**

## Adding Syslog configuration to log4j2

To add Syslog appender **add the following line** before <Async name="all"> tag (replace HOST with the real Syslog host, edit port 514 and use UDP or TCP as a protocol). The following lines should be added to the log4j2.pam.xml file:

```
1 | <Syslog name="syslog" host="HOST" port="514" protocol="UDP" appName="xtam"
  | id="xtam" newLine="true"/>
```

and **add Async appender reference** so it will look like this one below:

```
1 | <Async name="all">
2 |   <AppenderRef ref="console"/>
3 |   <AppenderRef ref="file"/>
4 |   <AppenderRef ref="syslog"/>
5 | </Async>
```

Restart the **PamManagement** service to reflect the added configuration.

## Alert and Report Subscriptions

### Alert and Report Subscriptions

Alert and Report subscriptions can be configured on Records, Containers or System Events (*System Administrators only*).

These notifications will alert the user to activity that has taken place with that object within a short period of time.

This is useful if a record contains a sensitive file or can be used to establish a session to a privileged endpoint and you need to be aware of its activities.

There are **three forms of notifications** available: *In-application Alerts*, *Email Notifications* and *Email Reports*.

When you subscribe to an alert anywhere in the system, when this alert is triggered it will send both an in-application alert as well as an email notification.

When you subscribe to an emailed report, the system will send an automated email either once a day, once a week or once a month, depending on your configuration.

NOTE: Email notifications and reports require that your [Mail Server](#) be configured properly in the Settings and the user must have an email address associated to their account.

### In-application and Email Alerts

In-application alerts are displayed in PAM's Top Menu, represented by a bell icon. A number badge will display the total number of unread alerts that are currently in your queue.

The same in-application alert that is displayed in PAM will also be delivered via email to the address associated to your account.


To view your in-application alerts either click the *bell* icon in the Top Menu to see a few of your latest alerts or click the **See All Alerts** link at the bottom to see all your alerts.

Alternatively, you can navigate to Management > My Alerts to see the full listing of your alerts.

### *Subscribe/Unsubscribe from Alerts*

To subscribe to an alert:



1. Click the **Bell** button located on the object that you wish to be notified about ().
2. Configure the alert subscription as desired. Note the object name will appear in the title area of the configuration dialog.
3. Click the **Select** button to complete your alert subscription.

To unsubscribe from an alert:


1. Navigate to the Management > My Profile > Subscriptions tab.
2. Select the **Alerts** filter option from the *Subscriptions* dropdown menu.
3. Select the alert(s) that you wish to unsubscribe from and then click the **Unsubscribe** button.

## Emailed Reports

Subscribed reports are automatically send to your account's email address based on your configured subscription to that report. Configuration includes the periodic delivery time and report format.

### *Subscribe / Unsubscribe from Reports*

To subscribe to a report:

1. Navigate to the report and configure its display options as required.
2. Once the report is formatted as you like, click the **Email** icon button (.
3. Configure your preferences and click **Select** to complete the subscription.

Period	Select a Daily, Weekly (Sunday) or Monthly (first day of the Month) delivery schedule.
Format	Select either CSV or PDF format. The report will be an attachment to the email.

To send an on-demand report:

1. Navigate to the Management > My Profile > Subscriptions tab.
2. Select the **Reports** filter option from the *Subscriptions* dropdown menu.
3. Select the report(s) that you wish to send now and then click the **Send** button.

To unsubscribe from a report:

1. Navigate to the Management > My Profile > Subscriptions tab.
2. Select the **Reports** filter option from the *Subscriptions* dropdown menu.
3. Select the report(s) that you wish to unsubscribe from and then click the **Unsubscribe** button.

## Subscribe and Unsubscribe to Alerts and Notifications

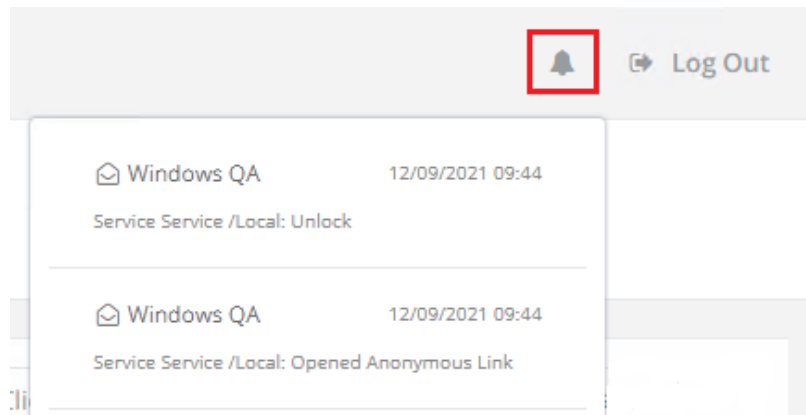
Alerts, Notifications and Reports within Access Manager can be configured on either Records, Folders or System Events (*System Administrators only*).

These notifications will alert the user to activity that has taken place against that object within a short period of time.

This is useful if a record contains a sensitive file or can establish a session to a privileged computer and you need to be aware of its activities.

Alerts will appear in the Alerts box located along the top of PAM as well as the Alerts section located in Management > My Alerts.

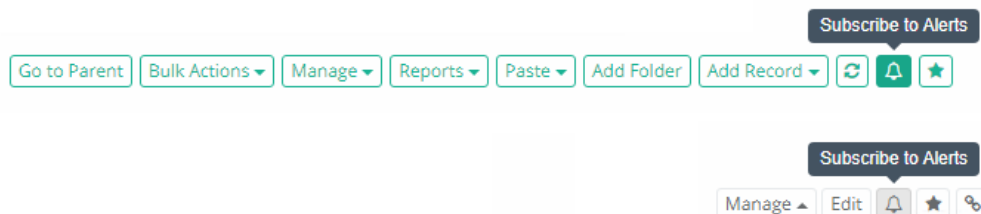
If a Mail Server has been properly configured, then these alerts will also be delivered via email to the user.



Reports will be delivered via email (to the address associated to the user's account) in the format and time period requested.

## To subscribe to an alert for a Record or Folder:

1. Login to PAM as a user with permissions to the *Record* or *Folder* that you would like to subscribe to alerts.
2. Open the Record or Folder and click the **Alert** button located in the toolbar. For Folders, this button is located along the top toolbar and for Records it is located along the bottom.



3. Choose your Category, Level and optionally an Event Filter. Click **Select** to complete the subscription.
4. Click **OK** to confirm the subscription has been created.

## Subscribe alert

To *subscribe* to an alert for System Events:

1. Login to PAM as a System Administrator.
2. Navigate to Management > My Profile > Subscriptions.
3. Click the **Subscribe** button.
4. Choose your *Category*, *Level* and optionally an *Event Filter*. Click **Select** to complete the subscription.

Category

Application ▼

Level

Error ▼

Event Filter

Cancel

Select

- Click **OK** to confirm the subscription has been created.

## Subscribe report

To *subscribe* to an email delivered report for a Record, Folder or PAM:

- Login to PAM as a user with permissions to the Record or Folder log that you would like to subscribe. Users with the role *System Administrator* or *Auditor* can only subscribe to Global Reports.
- Open the Object's log or the Global report that you would like to subscribe to and click the **Email** button located in the toolbar. This button is located along the top toolbar near the Refresh button.

Time: Last Month ▼

Category: Any ▼

Level: Any ▼

↺

✉

Search:

CSV

PDF

- Select your **Period**, **Format** and **Save to Folder** option, and then click the **Select** button to complete the subscription:
  - Period:** Choose between Daily, Weekly or Monthly.
    - Daily* will be queued for generation once a day (*12am the System server time*) and the report will be filtered to the last day of events (based on the time the report is created)
    - Weekly* will be queued for generation once a week (*Sunday 12am the System server time*) and the report will be filtered to the last week of events (based on the time the report is created)
    - Monthly* will be queued for generation once a month (*first of the month, 12am the System server time*) and the report will be filtered to the last month of events (based on the time the report is created)
  - Format:** Choose the format of the delivered report, either CSV, PDF or Zip Protected. *Zip protected* will save the selected report format to a password protected zip file. Enter the password for this Zip file when prompted.

## Subscribe

Period

Monthly ▼

Format

CSV ▼

Cancel

Select

- **Save to Folder:** Choose this option to save the generated report into the shared folder specified by the global parameter Report Folder instead of emailing the report to the subscriber.

4. Click **OK** to confirm the subscription has been created.

The first report will be queued for immediate delivery and each subsequent report will be delivered based on your selected Period.

## View and unsubscribe

To view all or unsubscribe any subscriptions:

1. Login to PAM as any user with subscribed alerts.
2. Navigate to Management > My Profile > Subscriptions to see a complete list of all current subscriptions for the logged in user account.
3. Choose either *Alerts* or *Reports* from the Subscriptions dropdown menu.
4. Select one or more subscriptions by clicking the box next to their entry.
5. Click **Unsubscribe** to remove the selected subscriptions.

Profile

Subscriptions

Found 4 subscriptions.

Subscriptions: Alerts ▼

Subscribe

Unsubscribe

↺

	Object	Object Type	Category	Level	Event
<input type="checkbox"/>	Unix Host with Key + Pass Session	Unix Host with Protected Key	Permissions	Information	
<input checked="" type="checkbox"/>	Unix Host with Key + Pass Session	Unix Host with Protected Key	Policy	All	
<input type="checkbox"/>	Unix Host with SU Session	Unix Host with SU	Permissions	All	
<input checked="" type="checkbox"/>		System	Application	Error	

## Software Updates

How to check for and update Privileged Access Management to the Latest Version.

The development of Privileged Access Management (PAM) follows an Agile development process which means a fast paced and frequent software release cycle. Due to this, the software provides an easy method to check for and ultimately deploy the latest version.

Before you update, review the latest [Privileged Access Management Release Notes](#).

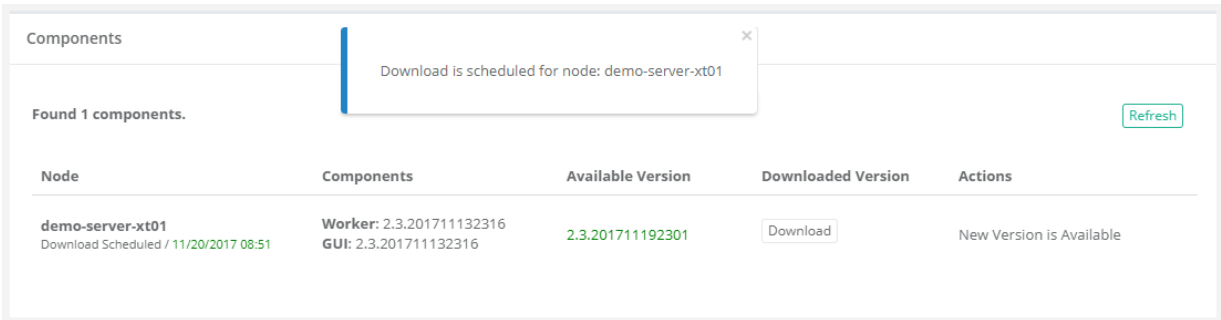
PAM updates may contain changes that require modifications to the PAM database. For this reason, please ensure that the PAM schema owner has DDL permissions on the database before starting the software update process.

## Check and Update PAM Online

To Check and Update PAM Online (for offline update scroll down to the next section).

To perform an Online Update, your PAM node(s) must be able to communicate with the PAM distribution server to complete a version check and to download the software package. If required, *whitelist* the domain "bin.xtontech.com" using port 443 in your firewall.

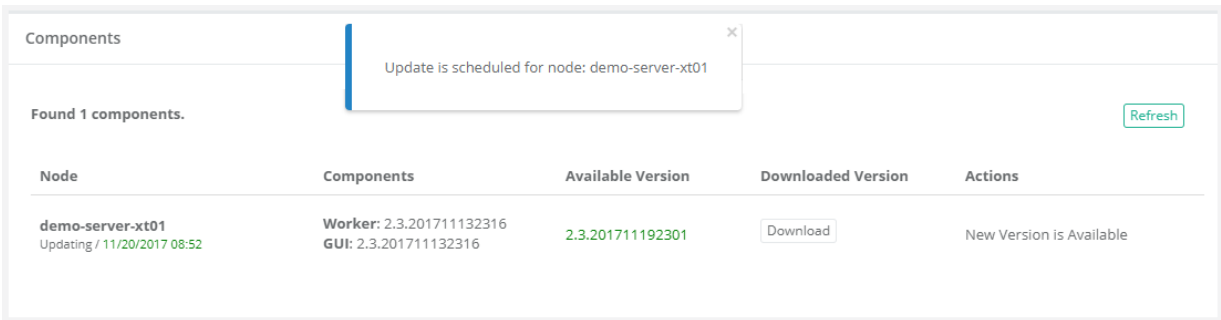
1. Login to PAM as a System Administrator.
2. Navigate to Administration > Updates. The Application Update page will display all the components configured, their Current Version and the latest Available Version. If the available version is more recent than your current version, a **Download** button will be visible.
3. Click **Download** to queue the download process. The download will be processed when possible and may take a few minutes to complete.



The screenshot shows the 'Components' page with a notification that a download is scheduled for node 'demo-server-xt01'. Below the notification is a table with columns: Node, Components, Available Version, Downloaded Version, and Actions. The table lists one component, 'demo-server-xt01', with its current version (2.3.201711132316) and available version (2.3.201711192301). A 'Download' button is visible in the Actions column, and the text 'New Version is Available' is displayed.

Node	Components	Available Version	Downloaded Version	Actions
demo-server-xt01 Download Scheduled / 11/20/2017 08:51	Worker: 2.3.201711132316 GUI: 2.3.201711132316	2.3.201711192301	Download	New Version is Available

4. When the download is finished, an Install button will become visible under the **Actions** column. Click **Install** to queue the installation process. The installation will be processed when possible and may take a few minutes to complete and during this time, connectivity to the system will be intermittent. We recommend performing the installation during “off peak” hours if possible.



The screenshot shows the 'Components' page with a notification that an update is scheduled for node 'demo-server-xt01'. Below the notification is a table with columns: Node, Components, Available Version, Downloaded Version, and Actions. The table lists one component, 'demo-server-xt01', with its current version (2.3.201711132316) and available version (2.3.201711192301). A 'Download' button is visible in the Actions column, and the text 'New Version is Available' is displayed.

Node	Components	Available Version	Downloaded Version	Actions
demo-server-xt01 Updating / 11/20/2017 08:52	Worker: 2.3.201711132316 GUI: 2.3.201711132316	2.3.201711192301	Download	New Version is Available

- After the update is installed, the current **Components** and **Available Version** numbers will be identical and the **Action** message will state that the current version is up to date.

Components				
Found 1 components.				<button>Refresh</button>
Node	Components	Available Version	Downloaded Version	Actions
demo-server-xt01 <small>Working / 11/20/2017 09:10</small>	Worker: 2.3.201711192301 GUI: 2.3.201711192301	2.3.201711192301		Current version is up to date

## Check and Update PAM Offline

### To Check and Update PAM Offline:

- Download the offline update from here: <https://bin.xtontech.com/product/pam-pkg.zip>
- Copy the downloaded zip file to the PAM server.
- Extract the zip file to a temporary location on the PAM server.
- In this temporary location, navigate to `/pkg/pam` and copy the files `xtam.war` and `xtamWorker.war`.
- Paste these files to `$PAM_HOME/content`, or the directory specified by the `Administration / Settings / Properties / Content Location` parameter.
- Once copied, PAM will begin the update process automatically.
- The update process takes about 5 minutes to complete and you should open PAM and navigate to Administration > Updates to confirm when the process is complete.

If your deployment includes the [Federated Sign-In Module](#), then you will need to complete the following additional steps when performing an offline update.

- Download and then unpack the web archive <https://www.xtontech.com/wp-content/uploads/2017/12/web.zip>
- Copy the `web.xml` file to `$PAM_HOME/web/webapps/xtam/WEB-INF` replacing the file which already exists. (Consider making a copy of the existing `web.xml` file in case of issues.)
- Restart the **PamManagement** (Windows) or **pammanager** (Linux) service.

## Performing PAM software update manually

- Login to PAM host server. Administrative privileges may be required.
- Download the offline update (<https://bin.xtontech.com/product/pam-pkg.zip>) and extract to a temporary location.
- Stop the **PamManagement/pammanager** service.  
Note that this PAM node will now be offline until the update is complete.
- Navigate to `$PAM_HOME/web/webapps` and delete both files `xtam.war` and `xtamWorker.war`
- Also in this same location, delete both directories `xtam` and `xtamWorker`.
  - Optionally, rather than deleting these files and directories, you can move them to a temp location outside of `$PAM_HOME`. If the update process fails, you can move these back and restart the service.

6. From within the extracted .zip in [step 2](#), navigate to `$PAM_HOME/pkg/pam` and copy the files `xtam.war` and `xtamWorker.war`.
7. Paste both copied files to `$PAM_HOME/web/webapps`.
8. Start the **PamManagement/pammanager** service. This will begin the update process which should complete in a few minutes.

If you are not using the Federated Sign-in Module, then the update process should be complete for this node.

If you are using the Federated Sign-in Module, then you will also need to complete these steps:

1. Stop the **PamManagement/pammanager** service again. This is a second operation which can not be combined with the first procedure.
2. Download the Federated Sign-in Module configuration file (<https://www.xtontech.com/wp-content/uploads/2017/12/web.zip>) and extract to a temporary location.
3. In this extracted archive, there will be a single `web.xml` file.
4. Copy `web.xml` and paste to `$PAM_HOME/web/webapps/xtam/WEB-INF`, overwriting the current file of the same name that already exists in this directory.
5. Start the **PamManagement/pammanager** service.
6. Once the update process is complete for this node, you can repeat these steps for the next PAM node.

## PAM and OS upgrade

PAM runs as an independent product that has operating system (OS) services added. Performing an in-place upgrade of the OS should complete without any PAM issues.

It is always good practice to perform these types of operations in a test/dev environment before doing so in a Production environment, as there are always things that can be learned through this process.

Before initiating the OS upgrade, it is beneficial to first stop all PAM services (PamManagement, PamDirectory, PamSession), and also take a backup of the PAM directory and store this in another location/folder.

## Roll Back Update

Please follow the below steps to update and restore the previously backed up version of PAM:

1. Stop the *PamManagement (pammanager for Linux)* service.
2. Copy `xtam.war` and `xtamWorker.war` from `$PAM/web/webapps` folder to outside of `$PAM` folder to back up the current version.
3. Start the *PamManagement (pammanager for Linux)* service.
4. In PAM Web GUI go to Administration > Updates and **update** the Application as usual.
5. Wait until the application updates (3-5 minutes).

## To restore the previously backed up version of PAM:

1. Stop the *PamManagement (pammanager for Linux)* service.
2. Delete the `xtam` and `xtamWorker` folders from `$PAM/web/webapps`.

3. Copy backed up files to `$PAM/content` or the directory specified by the `Administration / Settings / Properties / Content Location` parameter.
4. Start the *PamManagement* (*pammanager* for Linux) service.

## Recovering From Post Update Errors

Please follow the below steps if the server does not start up after the automatic update procedure:

1. **Stop** the PamManagement (*pammanager* for Linux) service.
2. **Delete** the "`xtam`" and "`xtamWorker`" folders from `$PAM_HOME/web/webapps` (do not rename this folder in place).
3. **Start** the *PamManagement* (*pammanager* for Linux) service.

## Updating the Framework

Updating Existing PAM Deployment to the Currently Supported OpenJDK Release.

While all new installations use the latest, PAM officially supported OpenJDK components (<https://jdk.java.net/>) as the default configuration, existing deployments should be updated manually if needed.

PAM officially supports OpenJDK 21.0.7 and this framework will be used for all new installations.

For existing deployments that are currently using OpenJDK 11, 12, 13, 14, 15 or 17 this guide will update you to the latest supported version.

For existing deployments that are currently using JRE 1.8\_x, please see [this guide](#) for the update procedure.

## Prerequisites

- An operational PAM deployment with the latest software version. Please update to the latest available version before proceeding.
- Updated application Framework to version 21.0.7 for new deployments. Existing deployments require update of the Framework.
- An operational PAM deployment with framework version 11, 12,13, 14, 15 or 17. If you are using 1.8\_x, please use [this guide](#) to update.

To check your Framework version, login to PAM with a System Administrator account, navigate to Management > About and locate the **Framework** parameter. If you see a version like **Framework: 11.x.x** or higher, please continue with this guide.

Please read the entire procedure outlined in the article before beginning. If you have any questions, please contact the Support team: <https://support.imprivata.com/communitylogin>.

## Considerations

- Each PAM node that is updated will be offline and inaccessible for the entirety of the migration.
- The user performing the migration will be required to update files and configurations on the PAM host server. Appropriate privileges are required.



- We highly recommend deploying a test instance of PAM that mirrors your production instance as closely as possible to test the migration (DB type, [Federated Sign-In](#), certificates, MFA/SSO, AD Integration, etc). Once the migration is successful with the test instance you can reproduce the procedure on your production instance.

Please read the entire procedure outlined in the article before beginning. If you have any questions, please contact our Support Team <https://support.imprivata.com/communitylogin>.

## Step 1. Download and Extract Framework Components

1. Download the latest supported framework packaged for PAM Server to your PAM host server and extract this archive outside the \$PAM\_HOME directory. If you have multiple nodes, you will need to perform this procedure on all node servers.
  - Windows: <https://bin.xtontech.com/product/pam-framework.zip>
  - Linux: <https://bin.xtontech.com/product/pam-framework.tgz>
  - Linux ARM: <https://bin.xtontech.com/product/pam-framework.aarch64.tgz>
2. Download the PAM JDK Update Pack to your PAM host server (Windows and Linux) and extract the archive to your \$PAM\_HOME directory. The extracted archive will create a new directory with the name \$PAM\_HOME/pam-jdk17-pack.
  - <https://bin.xtontech.com/product/pam-jdk17-pack.zip>

## Step 2. Stop the PAM Services

Once the services are stopped, PAM will become inaccessible until the update is completed.

1. For Windows deployments, stop the **PamManagement** and **PamDirectory** services:

```
1 | net stop PamManagement
```

```
1 | net stop PamDirectory
```

2. For Linux deployments, stop the **pammanager** and **pamdirectory** services:

```
1 | service pammanager stop
```

```
1 | service pamdirectory stop
```

## Step 3. Updating the OpenJDK Framework

1. Navigate to \$PAM\_HOME/jre, rename and move the existing file to \$PAM\_HOME/jre.old to a location outside of \$PAM\_HOME (don't just rename and leave in place, make a copy outside of \$PAM\_HOME). In case of any issues, you can use these backup copies to roll back the update process.

2. Replace the existing PAMjre directory with a new one. Once the old file been moved to a location outside of \$PAM\_HOME, move the jre directory downloaded in Step 1 to \$PAM\_HOME/jre.
3. Copy existing PAM Certificates and Configurations. Copy the file \$PAM\_HOME/jre.old/lib/security/cacerts to \$PAM\_HOME/jre/lib/security overwriting the current file.

Note: This step will migrate the existing certificates loaded into the previous PAM deployment including ADS, AD connection certificates as well as SSL certificate for CAS integration.

4. Update PAM container files.

Copy all files from \$PAM\_HOME/pam-jdk17-pack/ to \$PAM\_HOME/bin overwriting the current files.

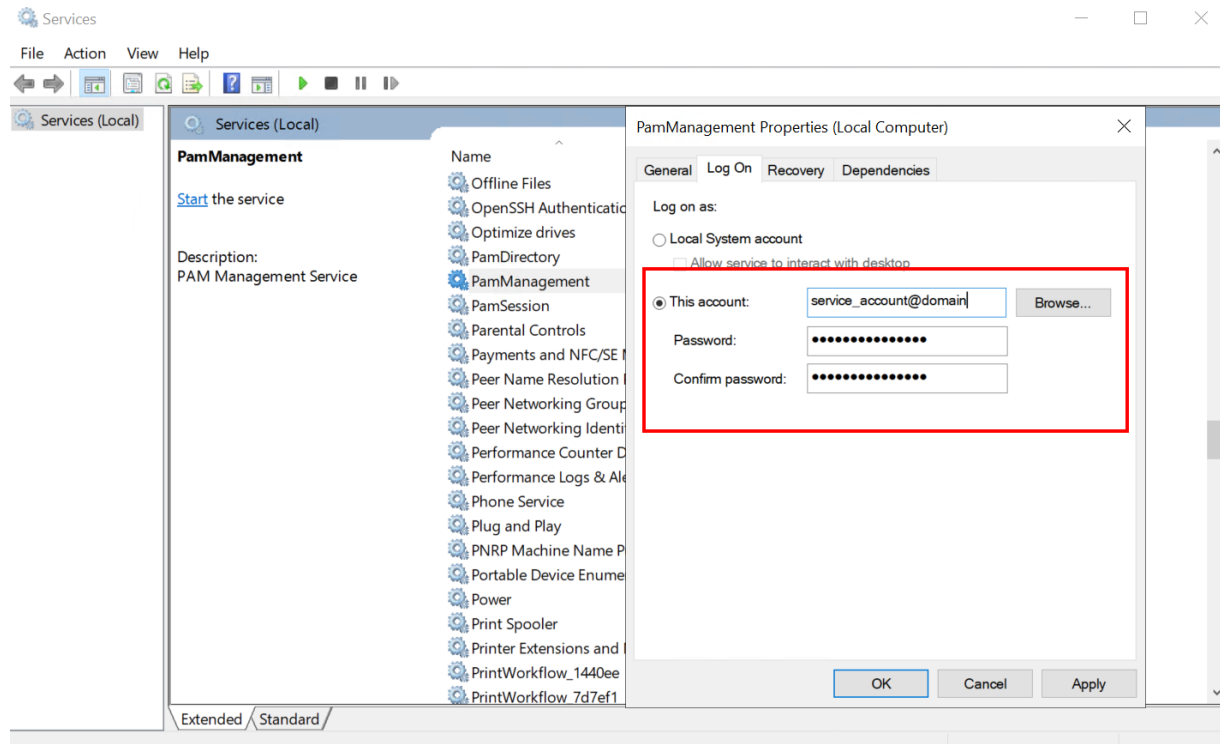
5. Redeploy Services:

- Windows

From an administrative command prompt, navigate to \$PAM\_HOME and run the commands:

```
1 bin\ServiceManagement.cmd remove
2 bin\ServiceManagement.cmd install
```

Note: The **PamManagement** service resets to the default *Local System account* Log on property once this service for PAM is reinstalled. If you are using a Log account other than an Local System account for this service then you must restore it prior to restarting the **PamManagement** service. Navigate to *Services* on Windows and find *PamManagement*, right-click and select **Properties**. Go to the *Log on* tab, select *This account:* and restore the required service account.



- Linux

From the command prompt navigate to `$PAM_HOME` and run the command:

```
1 | sh bin/update-jdk-17.sh
```

## Step 4. Start the PAM Services

1. For Windows deployments, start the **PamManagement** and **PamDirectory** services:

```
1 | net start PamDirectory
```

```
1 | net start PamManagement
```

2. For Linux deployments, start the **pammanager** and **pamdirectory** services:

```
1 | service pamdirectory start
```

```
1 | service pammanager start
```

These services may take a few minutes to fully start.

## Step 5. Test and Verify

Once the services come back online, you should now login and thoroughly test the system. This should include, but not be limited to:

1. Login with all applicable types of user accounts; Local, AD/LDAP, MFA and SSO.
2. Accessing existing records (and creating new records) in both the Record List and Personal Vault, including the unlock action.
3. Creating remote sessions.
4. Executing jobs and tasks (on demand and scheduled).
5. Viewing and exporting reports.

To confirm the update, check the Framework version on the Management > **About** screen. The displayed version should match the version that was downloaded.

## Rollback

If the migration or testing fails and you need to rollback to the previous Framework, then follow this procedure. If you do not need to rollback, proceed to the next section.

1. Stop the PAM services as described earlier.
2. Rename the new `$PAM_HOME/jre` to `$PAM_HOME/jre.new`
3. Rename the previous `$PAM_HOME/jre.old` back to `$PAM_HOME/jre`
4. Start the PAM services as described earlier.

When the services come back online, PAM should be using the previous framework. You should now perform the testing and validation again.

## Step 6. Cleanup

After all the testing is complete and the system is fully operational, you may choose to remove the following directories:

- `$PAM_HOME/jre.old`
- Files downloaded in *Step 1* and extracted archives.

## Updating the Session Manager Component

How to update the PAM Session Manager module.

At times, PAM updates its core Session Manager module to implement new functionality or to address new security protocols.

As these updates are infrequent, they are not included as part of the weekly PAM software updates.

The procedure outlined in this article should be used to update the Session Manager module when updates are released.

The latest Web Session Manager component is version 1.5.5-20240502.

## Windows Server

1. Update your [PAM software to the latest available version](#) before updating your Session Manager component.
2. Login to the Windows host server where the Session Manager module is deployed.
3. Download the latest version of the Session Manager component from here:  
<https://bin.xtontech.com/product/pam-session.zip>
4. Extract the `.zip` file to a temporary location on this host server. For example, extract to `c:\tmp` resulting in the folder `c:\tmp\guacd`.
5. Stop the **PamSession** service.
6. Rename the folders:  
`$PAM_HOME\guacd\bin` to `$PAM_HOME\guacd\bin0`  
`$PAM_HOME\guacd\lib` to `$PAM_HOME\guacd\lib0`  
`$PAM_HOME\guacd\usr` to `$PAM_HOME\guacd\usr0`
7. From within the extracted archive,
  - move the folder `c:\tmp\guacd\bin` to `$PAM_HOME\guacd`. This will create the new folder `$PAM_HOME\guacd\bin`
  - move the folder `c:\tmp\guacd\lib` to `$PAM_HOME\guacd`. This will create the new folder `$PAM_HOME\guacd\lib`
  - move the folder `c:\tmp\guacd\usr` to `$PAM_HOME\guacd`. This will create the new folder `$PAM_HOME\guacd\usr`
8. Start the **PamSession** service.
9. Test the new update by starting a new in-browser PAM session.

- If the test is successful, you can then delete the temporary folder `c:\tmp\guacd` and the old binaries at `$PAM_HOME\guacd\bin0`, `$PAM_HOME\guacd\lib0`, `$PAM_HOME\guacd\usr0`
- If the test is unsuccessful, you can rollback the update to the previous version by stopping the **PamSession** service, delete the new `$PAM_HOME\guacd\bin`, `$PAM_HOME\guacd\lib`, `$PAM_HOME\guacd\usr` directories, rename the backup from:
  - `$PAM_HOME\guacd\bin0` to `$PAM_HOME\guacd\bin`,
  - `$PAM_HOME\guacd\lib0` to `$PAM_HOME\guacd\lib`,
  - `$PAM_HOME\guacd\usr0` to `$PAM_HOME\guacd\usr` and finally starting the **PamSession** service.

## Linux Server (x86 or ARM)

1. Update your [PAM software to the latest available version](#) before updating your Session Manager component.
2. Login to the Linux host server where the Session Manager module is deployed.
3. Download the latest version of the Session Manager component using the appropriate link below:
  - Linux x86: <https://bin.xtontech.com/product/pam-session.tgz>
  - Linux ARM: <https://bin.xtontech.com/product/pam-session.aarch64.tgz>
4. Extract the archive file to a temporary location on this host server. For example, extract to `/tmp` resulting in the folder `/tmp/guac`.
5. Stop the **pamsession** service.
6. Rename the folder `$PAM_HOME/guac` to `$PAM_HOME/guac0`.
7. Move the folder `/tmp/guac` to `$PAM_HOME`.
8. Copy the folder with two security keys inside from `$PAM_HOME/guac0/etc/ssl` to `$PAM_HOME/guac/etc` so that newly copied folder `$PAM_HOME/guac/etc/ssl` will contain both public and private keys.
9. Run shell command `$PAM_HOME/guac/setup/setup.sh`.
10. Start the **pamsession** service.
11. Test the new update by starting a new in-browser PAM session.
  - If the test is successful, you can then delete the temporary folder `c:\tmp\guac` and the old binaries at `$PAM_HOME/guac/bin0`, `$PAM_HOME/guac/lib0`, `$PAM_HOME/guac/usr0`.
  - If the test is unsuccessful, you can rollback the update to the previous version by stopping the **pamsession**, delete the new `$PAM_HOME/guac` directory, rename the backup from `$PAM_HOME/guac0` to `$PAM_HOME/guac` and finally starting the **pamsession** service.

To print the version of WEB Session Manager execute the following command from the deployment folder where the application is installed:

- **Windows:** `.\guacd\bin\guacd -v`
- **Linux:** `./guac/sbin/guacd -v`

## Updating the WEB Container

Updating your existing PAM deployment to the currently supported Apache Tomcat release.

While all new installations use the latest, PAM officially supported Tomcat version as the WEB container, existing deployments should be updated manually if needed.

PAM officially supports Tomcat version 9.0.104 as its WEB container.

## Prerequisites

An operational PAM deployment with the latest software version.

Please update to the latest available version before proceeding.

## Considerations

- Each PAM node that is updated will be offline and inaccessible for the entirety of the upgrade.
- The user performing the upgrade will be required to update files on the PAM host server. Appropriate privileges are required.
- We recommend deploying a test instance of PAM that mirrors your production instance as closely as possible to test the migration (DB type, Federated Sign-In, certificates, MFA/SSO, AD Integration, etc). Once the upgrade is successful with the test instance you can reproduce the procedure on your production instance.
- Updated WEB Container to version 9.0.104 for new deployments. Existing deployments require update of the Web Container.
- An updated version of the [software's framework](#). Please update to the latest available version of the framework before continuing.

Please note that it is possible to operate the latest WEB Container on a version of the framework prior to 17. The additional steps for this configuration are detailed in [Step 3](#).

Please read the entire procedure outlined in the article before beginning. If you have any questions, please contact the Support team: <https://support.imprivata.com/communitylogin>.

## Step 1. Download and Extract WEB container Components

[Download](#) the latest supported WEB container for PAM Server to your PAM host server and extract this archive outside the \$PAM\_HOME directory. If you have multiple nodes, you will need to perform this procedure on all node servers:

<https://bin.xtontech.com/product/pam-web.zip>

## Step 2. Stop the PAM Services

Once the service is stopped, this PAM node will become inaccessible until the upgrade is completed.

For Windows deployments, stop the **PamManagement** service:

```
1 | net stop PamManagement
```

For Linux deployments, stop the **pammanager** service:

```
1 | service pammanager stop
```

## Step 3. Updating the WEB Container

1. Make a backup copy of the current folders `$PAM_HOME/web/bin` and `$PAM_HOME/web/lib` to a location outside of `$PAM_HOME` (don't rename and leave in place, make a copy outside of `$PAM_HOME`). In case of any issues, you can use these backup copies to roll back the update process.
2. **Copy** all files from the `web/bin` folder of the extracted archive in [Step 1](#) to the directory `$PAM_HOME/web/bin`. **Replace** all files including those that exist of the same names.
3. **Copy** all files from the `web/lib` folder of the extracted archive in [Step 1](#) to the directory `$PAM_HOME/web/lib`. **Replace** all including those that exist of the same names.

## Step 4. Start the PAM Services

For Windows deployments, start the **PamManagement** service:

```
1 | net start PamManagement
```

For Linux deployments, start the **pammanager** service:

```
1 | service pammanager start
```

## Step 5. Test and Verify

Once the service comes back online, you should now login and thoroughly test the system. This should include, but not be limited to:

1. Login to PAM with all applicable types of user accounts: Local, [AD/LDAP](#), [MFA](#) and [SSO](#).
2. Accessing existing records (and creating new records) in both the Record List and Personal Vault, including the unlock action.
3. Creating remote sessions.
4. Executing jobs and tasks (on demand and scheduled).
5. Viewing and exporting reports.
6. To confirm the update, check the **WEB Container** version on the Management > *About* screen. The displayed version should match the officially supported version mentioned in the beginning of this article.

## Rollback

If the upgrade or testing fails and you need to roll back to the previous WEB Container, then follow this procedure. If you do not need to rollback, proceed to the next section.

1. Stop the PAM service as described earlier.
2. Delete `$PAM_HOME\web\bin` and restore the backup copy to this location.
3. Delete `$PAM_HOME\web\lib` and restore the backup copy to this location.
4. Start the PAM service as described earlier.

When the services come back online, PAM should be using the previous WEB Container.

You should now perform the testing and validation again.

## Step 6. Cleanup

After all the testing is complete and the system is fully operational, you may choose to remove the following:

- The backup copies of the original WEB Container folders that was made outside of `$PAM_HOME`
- File downloaded in [Step 1](#) and its extracted archive.

## Disable WEB GUI check for the update

You can disable WEB GUI check for the latest version by providing system property

**xtam.web.version.disable=true** (default values is false) in `$PAM_HOME/web/conf/catalina.properties` file.

The option disables periodic connection to check for the latest version for the update repository for deployments operating in air-gaped or regulated environments.

## Updating the Federated Sign-in Module

Periodically, PAM updates its Federated Sign-in Module to support new authentication providers or to address new security protocols.

As these updates are infrequent, they are not included as part of the weekly PAM software updates.

The procedure outlined in this article should be used to update the Federated Sign-in Module when new versions are released.

The latest version of the Federated Sign-in Module version 6.5 component is 6.5.5.3 202506124.

If you want to migrate from the version 5 to the version 6.5 component, please review our [Migration to Federated Sign-in v6.5](#) guide.

## Considerations

- If possible, we would recommend you update a test environment first to become comfortable with the procedure and to test the results before updating production.
- Any customizations that you may have made to [Federated Sign-in](#) Module will be lost during the upgrade process and will need to be manually remade after the update is complete.
- Each PAM node where the Federated Sign-in Module is deployed will need to be updated using this procedure.

Please read the entire procedure outlined in the article before beginning. If you have any questions, please contact the Support team: <https://support.imprivata.com/communitylogin>.

## Step 1. Download and Extract Federated Sign-in Module

Download the latest supported Federated Sign-in Module for PAM to your PAM host server and extract the archive <https://bin.xtontech.com/product/pam-cas.zip> for legacy version 5.2 (or <https://bin.xtontech.com/product/pam-cas.65.zip> for product version 6.5) outside the `$PAM_HOME` directory.

If you have multiple nodes, you will need to perform this procedure on all node servers.



## Step 2. Stop the Pam Services

Once the service is stopped, this PAM node will become inaccessible until the update is completed.

- For Windows deployments, stop the **PamManagement** service:

```
1 | net stop PamManagement
```

- For Linux deployments, stop the **pammanager** service:

```
1 | service pammanager stop
```

## Step 3. Updating the Federated Sign-in Module

Navigate to `$PAM_HOME/web/webapps` and move both the existing `cas.war` file and the `/cas` directory to a location outside of `$PAM_HOME` (do not simply rename them in place).

Once both have been moved to a location outside of `$PAM_HOME`, copy the new `cas.war` file downloaded and extracted from step 1 to this same location (`$PAM_HOME/web/webapps`).

## Step 4. Start the Pam Services

- For Windows deployments, start the **PamManagement** service:

```
1 | net start PamManagement
```

- For Linux deployments, start the **pammanager** service:

```
1 | service pammanager start
```

During startup, PAM will automatically deploy the new [Federated Sign-in](#) Module.

This process may take several minutes to complete.

## Step 5. Test and Verify

Once the service comes back online, you can now open the PAM login page and test authentication.

This should include all authentication methods configured in PAM, for example, local user authentication, AD authentication, SSO or MFA.

If no issues are found during testing, then the update process is complete. You may now remake any customizations that you had made previously.

You can check your [Federated Sign-in](#) Module version by logging into the PAM web console with a PAM Administrator account and navigating to the Management > About page.

Verify your version number using the value shown on the Authentication parameter.

## Rollback

During testing, if you found issues with the new [Federated Sign-in](#) Module, you can rollback to your previously working version using this procedure.

If you do not need to rollback, please proceed to the next steps:

1. Stop the PAM service as described earlier.
2. Delete the new `cas.war` and `/cas` directory that were deployed to `$PAM_HOME\web\webapps`.
3. Copy back your original `cas.war` and `/cas` directory to this location (`$PAM_HOME\web\webapps`).
4. Start the PAM service as described earlier.

## Step 6. Cleanup

After your testing is complete and the new [Federated Sign-in](#) Module is working as expected, you may choose to remove the following as part of the cleanup process:

- Files downloaded in [Step 1](#) and the extracted archive.
- The backup copy of `cas.war` and the `/cas` directory.

## Reports

### Reports

PAM provides a series of built-in reports that help to locate objects, find user activity, understand permissions and view audit events throughout the system.

The following reports are available to PAM appropriately permissioned users to view, search and export.

- [Access report](#) provides a list of all users (unwound from groups) that have access to the selected object, their level of access and how they have been granted access (Group Membership, Individual ACL, Global Role or Global Permission).
- [Audit Log report](#) that provides a report of audit events captured throughout the System solution by all users and activities.
  - Use this report to investigate Audit Events in PAM.
- [Bindings report](#) provides a list of all users (unwound from groups) that have workflow bindings to the selected object, a summary of their binding configuration and how they are bound (group membership or by direct assignment).
- [Change History Report](#) provides a listing of all changes that have been made to a record's field values (i.e. Host, Port, User or Password).
- [Custom Queries](#) provides a location to create and view any custom query that have been generated.
  - These custom queries, written in the HQL querying language, are written and maintained by PAM System Administrators.
- [Dashboard](#) provides a graphical understanding of various categories of objects throughout the System as well as trending data over a 7 day period.
- [Inventory report](#) provides a list of all objects (records and folders) along with their metadata and permissions.
  - Use this report to find objects based on metadata, activity or permissions.

- [Job History report](#) provides a list of all Jobs or Tasks that have already been executed, along with their details.
  - Use this report to find details about scheduled or previously executed tasks.
- [Job Summary report](#) provides a list of all Jobs or Tasks that have already been executed, aggregated to illustrate a summary of their results including a number of executions per task per day.
  - The summary can be displayed in a data-table or presented in a line chart.
- [Local Group Membership Report](#) displays all local groups and members of the groups, members of the groups could be local users or AD users.
- [Requests report](#) provides a list of all Workflow Instances, including those that are active, approved and rejected.
  - Use this report to find any information about Workflow instances and states.
- [Sessions report](#) provides a list of all Active and Completed remote sessions in the System.
  - Use this report to investigate session activity and to access video and keystroke recordings.
- [Session Events report](#) provides a list of all keystrokes, clipboard text and command sequences users entered during any remote session.
  - Use this report to investigate session activity and search for keystroke or command entries throughout all sessions.
- [Statistics report](#) provide a graphical understanding of various categories of objects throughout the System.
  - Use these reports to understand system usage and various trends over time.
- [Subscriptions \(Alerts\) report](#) provides a list of alerts that the users' of the System are subscribed to, along with their alert configuration and an option to Unsubscribe them from their selected alert(s).
- [Subscriptions \(Reports\) report](#) provides a list of reports that the users' of the System are subscribed to, along with their report configuration and an option to Unsubscribe them from their selected report(s).
- [Tasks report](#) provides a list of all records that have at least one task associated to them, along with each task's details.
- [Users report](#) provides a list of all users and groups that have accessed the System.
  - Use this report to understand user behavior, activity, permissions and IP based locations.
- [Workflows report](#) provides a list of all System workflows along with their templates, bindings and configuration.
  - Use this report to understand where Workflows are deployed and how they are configured.

[Report Center](#) is a central location for PAM reports, both built-in and user saved. The user saved reports are versions of the built-in reports that have been customized through the use of unique filters and columns to better locate specific information in PAM.

If you would like to send PAM events to your SIEM or Syslog server, then please refer to this [page](#) for more information.

## Working with reports

The reports are available to any System Administrator or Auditor that logs into PAM.

All reports are accessible from the Reports section of the left navigation section and provide the following functionality.

- **Filters** that allow for report events to be specified based on parameters like time and category.
- **Search** box to query and locate specific events based on parameters like name, events and ID.
- **Export** commands to make the reports available to users outside of the PAM system. CSV, XLSX and PDF formats are available for export.

To learn about the specific information and functionality contained in each report, please click on the **Report Name** in the [Show Available Reports](#) article.

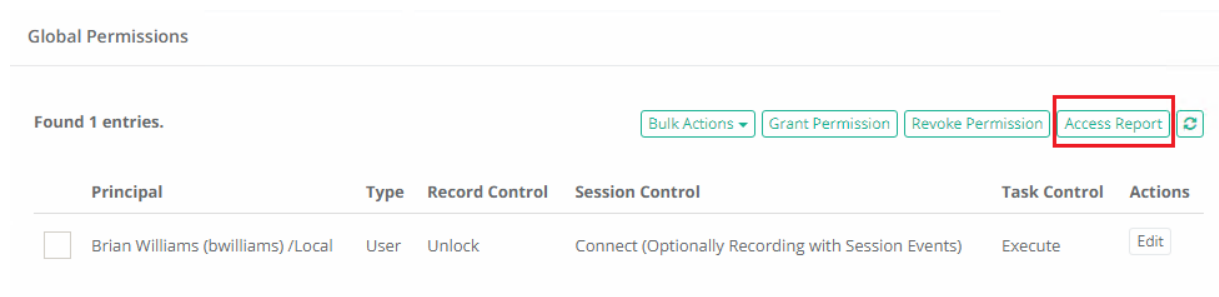
## Access Report

The Access report provides a list of all users (unwound from groups) that have access to the selected object, their level of access and how they have been granted access (*Group Membership, Individual ACL, Global Role or Global Permission*).

Each listed permission associated to the user represents a unique permission ensuring the reader can understand the entire scope of permission granted to each individual user.

The Access report is available from the following locations by accounts with the appropriate permissions:

- **Object's Permissions page:** Any user with permission to modify an object's permission can view this report by clicking the **Access Report** button from the object's permission page (Manage > Permissions).
- **Inventory Report:** Any user with permission to access the system or vault [Inventory report](#), can view this report by selecting the **View Access Report** option located in each object's Action menu.
- **Global Permissions:** Any user with permission to access the [Global Permissions](#) page can view this report by clicking the **Access Report** button.



The screenshot shows the 'Global Permissions' page. At the top, it says 'Found 1 entries.' Below this, there are four buttons: 'Bulk Actions', 'Grant Permission', 'Revoke Permission', and 'Access Report'. The 'Access Report' button is highlighted with a red rectangle. Below the buttons is a table with columns: Principal, Type, Record Control, Session Control, Task Control, and Actions. The table contains one entry for 'Brian Williams (bwilliams) /Local' with a checkbox in the Principal column and an 'Edit' button in the Actions column.

Principal	Type	Record Control	Session Control	Task Control	Actions
<input type="checkbox"/> Brian Williams (bwilliams) /Local	User	Unlock	Connect (Optionally Recording with Session Events)	Execute	Edit

## Access report options

The following options are provided with the Access report:

- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.

## Provided Information

The following information is provided as columns in the Access report:

- **User:** Displays the user's name and (login).
- **Permissions:** Displays the user's specific Permission to this object. Permissions include:
  - *Global Role:* If the user has access via a Global Role, the role name will be displayed.
  - *Global Permission:* If the user has access via a Global Permission, the specific level of access for each role (*Record Control/Session Control/Task Control*) will be displayed.
  - *ACL:* If the user has access via a specific ACL (either individual or by Group membership), the specific level of access for each role (*Record Control/Session Control/Task Control*) will be displayed.

When access is granted due to Group membership, the name of this group will be shown at the end of the line in parenthesis. For example, (Developers) meaning this specific permission was granted to this user because they are a member of the Developers group.

#### Access Report

Found 10 users.



Show 50 entries

Search:

CSV

PDF

XLSX

PDF Protected

CSV Protected

XLSX Protected

Showing 1 to 10 of 10 entries

User	Permissions
admin user (admin)	Global Role: Admin
auditor 01 (auditor)	Global Role: Auditor Global Permission: Viewer/None/None
Bob Barker (bob)	Global Role: Admin ACL: Viewer/None/None
Chris Kolodziejewski (chrisk)	Global Role: Admin (Developers) ACL: Viewer/None/None
editor editor (editor)	Global Permission: Editor/None/None
permission testaccount (permissiontest)	ACL: Viewer/None/Manage
personal Viewer (personalViewer)	ACL: Viewer/None/None
user 01 (user01)	ACL: Viewer/None/None ACL: Unlock/Connect (No Recording without Session Events)/Review
user 04 (user04)	Global Permission: Viewer/None/None
Service Administrator (xtamadmin)	Global Role: Admin Global Role: Auditor Global Permission: Viewer/None/None (ABC) ACL: Owner/Connect (Optionally Recording with Session Events)/Manage

First Previous 1 Next Last

## Audit Log Report

The Audit Log provides a report of audit events captured throughout the solution by all users and activities.

## Options

The following options are provided with the Audit Log report:

- **Filtering** is available for *Time*, *Category* and *Level* options.
- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.
- **Subscribe** is available by clicking on the envelop icon.
- **Save report** is available by clicking on the star icon.
- **Refresh** is available by clicking on the refresh icon.

## Provided Information

The following information is provided as columns in the Audit Log report

- **Time:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of the recorded event.
- **User:** Displays the account that performed the recorded event. The account `pamservice` is used by the system for performing background or scheduled tasks. This is not a user account.
- **IP:** Displays the detected IP address of the user that performed the recorded event.
- **Object:** Displays the name and provides a link to the object (record or folder) that is associated to the recorded event.
- **Category:** Displays the category (used to organize events based on relationship) of the recorded event.
- **Level:** Displays the level of the recorded event. Level includes *INFO*, *WARNING* and *ERROR*.
- **Event:** Displays the type of the recorded event. Type includes examples like *Edit*, *Create*, *Connection*, *Update Queue Records* and more.
- **Message:** Displays any system messages associated to the recorded event.

## Saved Filters

Various filters in the Audit Log report are useful to customize the view to the system assets for different purposes by the *Auditors*, *System Administrators*, *System Owners*.

1. **Select** *Columns* or *Filters* to display in your Audit Log report.
2. **Save** various Audit Log report configurations (report columns and filters) for further.
3. Reuse and receive quick access to the saved filters.

Save Report  
Name




### System Audit Log

Found 64 audit log records.

Time: Last Day ▾ Category: Any ▾ Level: Any ▾ Columns ▾   

Show 50 ▾ entries

Search:

Showing 1 to 50 of 64 entries

Time	User	IP	Object	Category	Level	Event
12/10/2021 11:26:26	Service Service (pamservice) /Local	10.153.182.38	pam02-01	Application	INFO	Health Check
12/10/2021 11:14:32	Service Administrator (pamadmin) /Local	10.153.182.38	<a href="#">Unix QA team</a>	Operation	INFO	Session Rated
12/10/2021 11:10:33	Service Administrator (pamadmin) /Local	10.153.182.38	pam02-01	Operation	INFO	Logout
12/10/2021 11:10:33	Service Administrator (pamadmin) /Local	10.153.182.38	pam02-01	Operation	INFO	Login

## Bindings Report

The Bindings report provides a list of all users (unwound from groups) that have workflow bindings to the selected object, a summary of their binding configuration and how they are bound (group membership or by direct assignment).

The Bindings report is accessible from the:

- Object's Workflows page: Any user with permission to modify an object's workflows can view this report by clicking the **Bindings Report** button from the object's Workflow page (Manage > Workflows).

# Options

The following options are provided with the Bindings report:

- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.

## Provided Information

The following information is provided as columns in the Bindings report

**User:** Displays the user’s name and (login).

**Bindings:** Displays the user’s specific Binding to this object. Use the following example to understand how Binding configurations are displayed:

**IT Dept Connect Approval (business hours) /10 [Record,Connect,Task], [Work Hours], [Checkout], [10.0.0.1], [MFA] (Developers)**

- **IT Dept Connect Approval (business hours)** — Indicates the name of the Workflow Template
- **/10** — Indicates the value of the Duration parameter. If Duration is empty, this parameter will not be included.
- **[Record, Connect, Task]** — Indicates the configured Actions.
- **[Work Hours]** — Indicates the configured Time Selectors.
- **[Checkout]** — Indicates the configured Checkout status of either Optional or Required. If Checkout is Disabled, this value will not appear.
- **[10.0.0.1]** — Indicates the configured IP Filter. If IP Filter is empty, this parameter will not be included.
- **[MFA]** — Indicates that MFA is required. If MFA is disabled, this parameter will not be included.
- **(IT)** — Indicates that this user is configured as part of this binding due to them being a member of the group named Developers.

When a binding is present due to Group membership, the name of this group will be shown at the end of the line in parenthesis. For example, (Developers) meaning this specific binding was associated to this user because they are a member of the Developers group.

Bindings Report

Found 6 users.

Showing 1 to 6 of 6 entries

User	Bindings
Dave Jacobs (dave) /Local	Restrict Access [Admin,Record,Connect,Task], [Always]
MSP Admin (mspadmin) /AD	IT Dept Connect Approval (business hours) [Admin], [Always]
John Williams (john) /Local	Auto Approved [Record,Connect], [Holidays,Weekends], [Checkout] (IT)
User A (usera) /Local	Auto Approved [Record,Connect], [Holidays,Weekends], [Checkout] (IT)
User B (userb) /Local	Auto Approved [Record,Connect], [Holidays,Weekends], [Checkout] (IT)
Jeff Thomas (jeff) /AD	IT Dept Connect Approval (business hours) /10 [Record,Connect,Task], [Work Hours], [Checkout]

# Inventory Report

The Inventory report provides a list of all objects (records and folders) along with their metadata and permissions.

## Options

The following options are provided with the Inventory report:

- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF, XLSX or Matrix file.
- **Sorting** is available by clicking on the desired column header.
- **Subscribe** is available by clicking on the envelop icon.
- **Save report** is available by clicking on the star icon.
- **Refresh** is available by clicking on the refresh icon.

## Provided Information

The following information is provided as columns in the Inventory report:

- **ID:** Displays the object's unique, internal ID for reference.
- **Vault:** Displays the name of the Vault.
- **Object:** Displays the name and provides a link to the object (record or folder).
- **Host:** Displays the host of the object.
- **User:** Displays the name of the user.
- **Type:** Displays the record type of the object.
- **Reference Record:** Displays the record reference of the object.
- **Author:** Displays the name of the user that created the object.
- **Editor:** Displays the name of the user that last modified the object.
- **Created:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the object was created.
- **Modified:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the object was last modified.
- **Accessed:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the object's [heartbeat](#) was last attempted.
- **Rotated:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when last time record password was successfully rotated by the system.
- **Connected:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when last time a user connected to the asset described by this record.
- **ACL:** Displays the permissions that are assigned to this object. It will displays *Inherited from: {parentName}* if this object's permissions are inherited and *Unique* if the object's permissions are not inherited from a parent. The account that performed the act and the time of when the permission was granted is also displayed.
  - **Direct ACL:** Displays permissions directly granted to a user or group.
  - **Expanded ACL:** Displays permissions for all users with specific permissions either directly or through group membership, global permissions or a global role.

Expanded ACL mode is disabled for PDF export when more than 1000 objects are included in the report.



- **Action Menu:** Provides the following options:
  - View Audit Log: Opens the Record Audit Log report to display all events associated to this object. Available for records only.
  - View Access Report: Opens the Access Report of this object display all users that have access to this selected object. The permissions will detail how they gained access (Group or Individual ACL, Global Role or Global Permission) and what level of access each user has.

## Matrix Export

In addition to the regular export options using CSV, PDF and XLSX, the Inventory report provides the option to also export the data into a Matrix format.

This Matrix export produces a unique row for each object in the report representing individual user or group permission that are assigned to the object.

Because objects may contain more than a single assigned permission, it is expected that the Matrix report will include multiple rows for each object.

These duplicated rows are useful for maintaining consistent object metadata while the individual permissions displayed in the report easily allow Auditors and Owners to analyze privileged access using Excel.

## Saved Filters

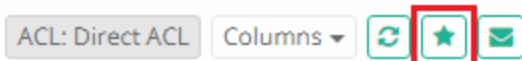
Various filters in the Inventory report are useful to customize the view to the system assets for different purposes by the *Auditors*, *System Administrators*, *System Owners*.

**Select** to display in your the Inventory report:

- Columns
- Filters

**Save** various Inventory report configurations (report columns and filters) for further.

Reuse and receive quick access to the saved filters.



Save Report  
Name

Found 19 objects.

ACL: Direct ACL Columns   

Show 50 entries

Search:

CSV

PDF

XLSX

Matrix

PDF Protected

CSV Protected

XLSX Protected

Matrix Protected

Showing 1 to 19 of 19 entries

Id	Object	Type	Author	Editor	Created	Modified	
i-34xeLjbrG8l	<a href="#">Root Folder</a>	Folder	Service Administrator (pamadmin) /Local	Service Administrator (pamadmin) /Local	11/09/2021 10:33:29	11/09/2021 10:33:29	...
i-IS83wTyVYUT	<a href="#">Remote Ubuntu Desktop</a>	Unix Host	Service Administrator (pamadmin) /Local	Service Administrator (pamadmin) /Local	11/09/2021 10:46:42	11/15/2021 11:20:10	...
i-6ZEy6O52Hrw	<a href="#">Windows Server</a>	Windows Host	Service Administrator (pamadmin) /Local	Service Administrator (pamadmin) /Local	11/10/2021 11:41:04	11/10/2021 11:41:04	...

## Change History Report

The Change History report provides a listing of all changes that have been made to a record's field values (i.e. Host, Port, User or Password).

This includes changes made by a named user of PAM and changes made by PAM itself during operations like automated password rotations.

As part of the Change History Report, the account that made the change (*Modified By*), the time the change was made (*Modified At*) and the updated field values (*Changes*) will be displayed, beginning with the most recent change at the top of the report.

Each listed Change will include a **Restore** option that will restore the field values from this time back to the current record.

The Change History report is accessible from within any Record by accounts with *Record Control: Owner* permissions or *System Administrators*.

Found 5 history records.



Show  entries

Showing 1 to 5 of 5 entries

**Modified At:** 03/03/2020 11:31

**Modified By:** Chris Kolodziejski (chrisk) /Local

**Changes:**

User: localadmin

Port: 10024

Host: 10.0.0.24

Password: \*\*\*\*\*

Restore

**Modified At:** 01/23/2020 08:18

**Modified By:** Chris Kolodziejski (chrisk) /Local

**Changes:**

description: windows host session (xtonprod)

Restore

**Modified At:** 07/29/2019 13:26

**Modified By:** Chris Kolodziejski (chrisk) /Local

**Changes:**

User: localAdmin

Password: uARNe6Q-j^E#g5wg\*an5%Ab

Restore

**Modified At:** 07/29/2019 13:23

**Modified By:** Chris Kolodziejski (chrisk) /Local

**Changes:**

name: Windows Host

description: windows host session

Restore

**Modified At:** 07/29/2019 13:22

**Modified By:** Chris Kolodziejski (chrisk) /Local

**Changes:**

User: local01

Port: 10023

name: Windows Host (internal)

description: windows host session (internal) with non-domain account

Host: 10.0.0.23

type: Windows Host

Password:

Restore

First Previous 1 Next Last

## Custom Queries

The Custom Queries menu provides a location to create and view any custom queries that have been generated.

Custom Queries are written in the HQL language which is similar to SQL, comprehensive reports can be created that join data from different tables/objects (<https://docs.jboss.org/hibernate/orm/3.3/reference/en-US/html/queryhql.html>).

Custom Queries can be created, edited and deleted by PAM System Administrators only.

Users with the global role *Auditor* may only view Custom Queries.

The Custom Query has report **Examples** and also the code needed to return all fields for different **Objects**.

Custom Query Example Custom Query

Save

Examples

Objects

View

Cancel

Name

Example Custom Query

Description

The example of the custom query to define new report.

HQL

1

select

2

r.id as id,

3

r.name as name,

4

r.recordType.name

5

r.author.name as a

6

r.created as creat

7

from

8

Record r

Filter

Example Custom Query

Example Record Types Report

Example Report Records with Record Types and Session Managers


Example Report Windows Hosts with no Password Resets

Example Report Windows Hosts with Password Resets

Example Report with Enabled Search

Example Summary Report Record Count by Record Type

Custom Query Example Custom Query

Save Examples Objects View Cancel 

Name

Example Custom Query

Description

The example of the custom query. Please use this example to define new report.

HQL

```
1 select
2   r.id as id,
3   r.name as name,
4   r.recordType.name as recordType,
5   r.author.name as author,
6   r.created as created
7 from
8   Record r
```

Filter

AdminMessage

AdminMessageViewer

AdsFolder

Alert

AnalyticsProfile

AnalyticsRule

AnonymousLink

AuditLog

AuthenticationToken

DeviceParameter

## Creating a New Custom Query

1. Login to PAM with a System Administrator account.
2. Navigate to Reports > Custom Queries and click the **Create** button.
3. Enter a **Name** and optional **Description** in the appropriate fields.
4. Enter your custom HQL statement into the **HQL** field.

Use the **Example** menu to select a pre-built report example that will load a sample custom report. You may customize these example reports as necessary and use the **Save** button to make it available to your users.

To enable a column to display a link to a record page, select record ID in this column and name the column `record_id`.

5. Click the **Save** button to save your new custom report.

Click the API Documentation link to open the interactive REST API documentation to further help with the construction of your HQL statements.

To View the results of a custom report, simply click on the report's **Name** or its **View** button. When viewed, the results will be queried and displayed as found. From within a custom report, the following options are available:

- **Search** is only available if the functionality was included in your HQL statement. See the example report **Example Report with Enabled Search** to see how Search is enabled.
- **Export** is available to export the available on-screen data to either a CSV or PDF file.

Columns will be displayed as defined in your HQL statement. The Columns selector will allow you to show or hide each column in the report.

PAM includes the option *to delegate custom queries execution to folder owners*.

The option allows involving more users in the system management and audit.

The option allows delegating custom queries execution to vault or folder owners by enabling Custom Queries that reference record IDs using **record\_id** HQL alias on the folder level in the reports menu.

An example of the custom report that could be delegated to the folder level is given by the following HQL producing all record update audit log events from the selected folder with search and export (**PDF, CSV, Encrypted PDF or CSV**) options (note **record\_id** alias returned by the HQL as the last column in a select clause that enables the option to Enable custom report on the folder level):

**select**

- **r.name** as recordName,
- **a.user.name** as User,
- **a.created** as created,
- **a.event** as Event,
- **r.id** as record\_id

**from**

- AuditLog a,
- Record r

**where**

- a.modelId=r.id
- and a.event = 'Update'
- and r.name like :search

## Record View screen

The Record View screen enables system administrators to create action-able custom queries that provide immediate drill-down access to the reported assets to make changes or to further investigate the case using record-based reporting.

To enable a column to display a link to a record page, select record ID in this column and name the column **record\_id**.

Example of report displaying archived records with **record name**, **record type** and a **link to a record**:

```
1 | select
2 |     m.name as name,
3 |     m.description as description,
4 |     m.recordType as recordType,
5 |     m.created as created,
6 |     m.author as author,
7 |     m.id as record_id
8 | from
9 |     Record m
10 | where m.archived is true
```

Example Custom Query

Description is here.

Root Folder / Custom Queries / Example Custom Query

Example Custom Query

Found 512 objects. Columns

Show 25 entries      Search:       CSV PDF XLSX PDF Protected CSV Protected XLSX Protected

Showing 1 to 25 of 512 entries

Record_id	Name	RecordType	Author	Created
<a href="#">i-3GvzsrY6DnR</a>	WINSRV2016RDS	Windows Host	pamservice	2021-03-12 18:21:41 EST
<a href="#">i-bsjfMulj6PF</a>	WINSRV2016RDS: Administrator	Active Directory User	pamservice	2021-03-12 18:21:41 EST
<a href="#">i-wvUHS3esgh</a>	WINSRV2016RDS: DefaultAccount	Active Directory User	pamservice	2021-03-12 18:21:42 EST
<a href="#">i-b3XsNxx028A</a>	WINSRV2016RDS: Guest	Active Directory User	pamservice	2021-03-12 18:21:42 EST
<a href="#">i-7VPYBUyWOih</a>	WINSRV2016RDS: kate	Active Directory User	pamservice	2021-03-12 18:21:43 EST
<a href="#">i-EIHFDHQICL</a>	WINSRV2016RDS: kate	Active Directory User	pamservice	2021-03-12 18:21:43 EST
<a href="#">i-a0S08kWL3IQ</a>	WINSRV2016RDS: katek	Active Directory User	pamservice	2021-03-12 18:21:43 EST

Example of custom query with Id filter

When attempting to filter by [Secure Id's](#) , use the below format:

where r.id = '\$ {i-xxx}'

where r.id in ('\$ {i-xxx}', '\$ {i-yyy})

where r.id = '\$ {:search}'

# Job History Report

The Job History report provides a list of all Jobs or Tasks that have already been executed, along with their details.

## Options

The following options are provided with the Job History report:

- **Filtering** is available for Time and State options.
- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF, XLSX or TXT file. The TXT (text) option is used to combine the task execution results of all displayed tasks into a single text file output.
- **Sorting** is available by clicking on the desired column header.
- **Subscribe** is available by clicking on the envelop icon.
- **Save report** is available by clicking on the star icon.
- **Refresh** is available by clicking on the refresh icon.

## Provided Information

The following information is provided as columns in the Job History report:

- **Time:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the job or task was queued.
- **Type:** Displays the type of execution associated to this job. For example, OnDemand or Policy based execution.
- **User:** Displays the account that executed the job or task. The account pamservice is used by the system for performing background or scheduled tasks. This is not a user account.
- **Object:** Displays the name and provides a link to the object (record or folder) that is associated to the Job or Task.
- **Host:** Displays the host name value from the record which executed this task.
- **Task:** Displays the name of the associated task.
- **Processed:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the job or task was ended.
- **Result:** Displays the current result of the task (Achieved).
- **State:** Displays the state of the executed job or task.
- **Message:** Displays the message during of the task execution.
- **Actions Menu:** Provides the following options:
  - **Details:** Displays the details or results of the executed task.

## Saved Filters

Various filters in the Job History report are useful to customize the view to the system assets for different purposes by the Auditors, System Administrators, System Owners.

1. **Select** Columns or Filters to display in your Job History report.
2. **Save** various Job History report configurations (report columns and filters) for further.
3. Reuse and receive quick access to the saved filters.



### Save Report Name

### Job History

Found 11 job records.

Time: Last Month ▾

State: Any ▾

Columns ▾

Bulk Actions ▾



Show  entries

CSV

PDF

TXT

XLSX

CSV Protected

PDF Protected

TXT Protected

XLSX Protected

Search:

Showing 1 to 11 of 11 entries

	Time	Type	User	Object	Host	Processed	Result	State	
<input type="checkbox"/>	12/15/2021 12:11:30	On Demand	Service Administrator (pamadmin) /Local	Windows 10 Enterprise	10.153.182.41	12/15/2021 12:12:11		Error	<a href="#">Details</a>
<input type="checkbox"/>	12/15/2021 12:10:17	On Demand	Service Administrator (pamadmin) /Local	Windows 10 Enterprise	10.153.182.41	12/15/2021 12:10:26		Error	<a href="#">Details</a>

## Job Summary Report

The Job Summary report provides a list of all Jobs or Tasks that have already been executed, aggregated to illustrate a summary of their results including a number of executions per task per day.

The summary can be displayed in a data-table or presented in a line chart.

## Options

The following options are provided with the Job Summary report:

- **Filtering** is available for Time and State options.
- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.

## Information Provided

The following information is provided as columns in the Job Summary report:

- **Date:** Displays the date (MM/DD/YYYY) of when the job or task was executed against any record.
- **Task:** Displays the name of the associated task.
- **State:** Displays the state of the task.
- **Result:** Displays the result of the executed task. If the script does not include a Result response, then this column will be empty.
- **Count:** Displays the total of number of times this task was executed on this date across all records.
- **Actions Menu:** Provides the following options:
  - *Details:* Displays the details or results of all the executed tasks included in the count.
  - *Chart:* Generates a chart displaying this task across all its date ranges, states and included results.


Jobs Summary


Found 8 jobs summary records.

Time: All Jobs

State:

Columns





Show 50 entries

Search:

CSV

PDF

XLSX

PDF Protected

CSV Protected

XLSX Protected

Showing 1 to 8 of 8 entries

Date	Task	State	Result	Count
04/20/2021	Check Status Remote Windows	Completed		2
04/20/2021	Check Status Remote Windows	Error		1
04/20/2021	Check Status Remote SSH	Completed		1
04/19/2021	Check Status Remote SSH	Completed		1

## Local Group Membership Report

Local Group Membership report displays all local groups and members of the groups, members of the groups could be local users or AD users.

Local Group Membership report is located in Administration > Local Groups > Local Group Membership report.

Local Group Membership report is available for users with global role service administrator and for owners on Folder Level Manage > Local Groups > Local Group Membership report.

## Options

The following options are provided with the Local Group Membership report:

- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.



## Provided Information

The following information is provided as columns in the Local Group Membership report:

- **Member Name:** Displays the name's of the members in group.
- **Directory:**Displays the type of user's directory - ActiveDirectory/Local.
- **Group Name:** Displays the name of the group.
- **Group Folder:** Displays the name of the folder which the group is belong.
- **Member Type:** Displays the type of the user.

Local Group Membership Report

Found groups.

Columns  

Show 

All

 entries

Search:

CSV

PDF



XLSX

PDF Protected

CSV Protected

XLSX Protected

Showing 1 to 2 of 2 entries

Member Name 	Directory	Group Name 	Group Folder	Member Type
Service Administrator (xtamadmin)	Local	Local Work Group		User
Victoria Fomenko (vfomenko)	Local	Local Work Group		User

First

Previous

1

Next

Last

## Requests Report

The Requests report provides a list of all Workflow Instances, including those that are active, approved and rejected.

## Options

The following options are provided with the Requests report:

- **Filtering** is available for a Time option.
- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Subscribe** is available by clicking on the envelop icon.
- **Save report** is available by clicking on the star icon.
- **Sorting** is available by clicking on the desired column header.

## Provided Information

The following information is provided as columns in the Requests report:

- **Request ID:** Displays the unique ID of the request.
- **Approved:** Displays the name of the user that approved the request.
- **Request Time:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the request was submitted.
- **Requester:** Displays the name of the user that made the request or for which the request was made on-behalf of.
- **Workflow Design:** Displays the name of the workflow template that was used for this request.
- **Action:** Displays the action (i.e. Unlock or Connect) and time (minutes or range) of the request.
- **Enabled From:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of from the request was enabled.
- **Enabled To:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of the request was enabled to.
- **Requested Time:** Displays the asked time of the request.
- **Object:** Displays the name and provides a link to the object that the request was made for.
- **Reason:** Displays the reason the user entered for submitting the request.

- **Ticket Type:** Displays the ticket type of the request.
- **Ticket:** Displays the ticket of the request.
- **Status:** Displays the current status (Active, Approved or Rejected) of this request.
- **Approvers:** Displays the names of the users that approve the request.
- **Actions:** Displays the actions of the users.
- **Actions Menu:** Provides the following options:
  - Details: Displays the additional details of the request.
  - Sessions: Displays any active or completed sessions associated with this request.

## Saved Filters

Various filters in the Requests report are useful to customize the view to the system assets for different purposes by the *Auditors*, *System Administrators*, *System Owners*.

1. **Select** Columns or Filters to display in your Requests report.
2. **Save** various Requests report configurations (report columns and filters) for further.
3. Reuse and receive quick access to the saved filters.

### Requests Report

Home / Requests Report

Requests Report

Found 10 requests.

Time: Last Month Columns

Show 50 entries

Search:

CSVPDFXLSXPDF ProtectedCSV ProtectedXLSX Protected

Showing 1 to 10 of 10 entries

Time	Requester	Workflow	Action	Object	Reason	Status	Actions
06/09/2021 21:46:57	John Williams /Local	Auto Approved	Connect:60	Production Windows Server	request again	Completed	
06/09/2021 21:38:25	John Williams /Local	Auto Approved	Connect:15	Production Windows Server	patch server	Completed	
06/09/2021 18:41:15	John Williams /Local	Auto Approved	Connect:15	Production Windows Server	#123	Completed	
06/07/2021 18:25:54	John Williams /Local	Auto Approved	Connect:15	Production Windows Server	#123	Completed	
06/03/2021 17:25:52	John Williams /Local	Auto Approved	Connect:15	Production Windows Server	patch server	Completed	

## Sessions Report

The Sessions report (Reports > Sessions) provides a list of all *Active* and *Completed* remote sessions in PAM as well as provides access to any video or keystrokes recordings.

The My Sessions report (Management > My Sessions) provides a list of all *Active* and *Completed* remote sessions that your account has permissions to connect.

This may include all currently active or previously completed sessions that you personally established as well as sessions that other users have established.

Sessions that you have not created are displayed as a quick method to identify sessions that you may join or have relevance.

Some of the described options below may not be available due to your account lacking the required permissions to access them.

## Options

The following options are provided with the Sessions report:

- **Filtering** is available for Time and State options.
- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.
- **Subscribe** is available by clicking on the envelop icon.
- **Save report** is available by clicking on the star icon.
- **Refresh** is available by clicking on the refresh icon.

## Provided Information

The following information is provided as columns in the Sessions report:

- **Record:** Displays the name and provides a link to the record that was used to connect to a remote session.
- **User:** Displays the user that established the remote session.
- **Start Time:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the session started.
- **Completion Time:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the session completed. This column will be empty for Active sessions.
- **Heartbeat Time:** Displays the heartbeat or status job of the record.
- **Type:** Displays the remote protocol used to establish this connection.
- **Status:** Displays the current status of the session, either Active or Completed.
- **ID:** Displays the user's record ID.
- **IP:** Displays the detected IP address of the user that performed the recorded event.
- **Host:** Displays the user's record host.
- **Account:** Displays the user's account.
- **Session Manager:** Displays the session manager for the connection.
- **Rating:** Displays the rating of the record (changeable by System Administrator).
- **Rating Comment:** Displays the comment to the rating of the record (changeable by System Administrator).
- **Reviewer:** Displays the user name who reviewed the session and added ratings and comments.
- **Reviewed:** Displays the date of review and the session rate.
- **Risk:** Displays the risk score provides a quick indication of unwanted or suspicious activity on the servers with the trending of operators executing watched commands.
- **Request:** Displays the request for the session connection.
- **Connection:** Displays the original letters and digits id of the connection done by this record.
- **Recording:** Displays the status of the session recording.
  - In Progress: The current, active session is being recorded.
  - Not Recording: The current, active session is not being recorded.
  - Available: The session is complete and a video recording is available.
  - Not Recorded: The session is complete and a video recording is not available.
- **Action Menu:** Provides the following options:
  - Instant Video Playback: The session recording is available to be viewed directly in your browser. *This option is only available if the session was recorded.*
  - Events: Opens the keystroke recording log for the session.
  - Clear Rating: Removes the rating and comments to the session record with a warning window.

- Convert to AVI: Begins the conversion process so the session recording is converted and saved to a `.avi` file. *This option is only available if the session was recorded.*
- Convert to MOV: Begins the conversion process so the session recording is converted and saved to a `.mov` file. *This option is only available if the session was recorded.*
- Convert to MP4: Begins the conversion process so the session recording is converted and saved to `.mp4` file. *This option is only available if the session was recorded.*
- Download: possibility to download session record if it was recorded and available as converted to `.avi`, `.mov` or `.mp4` file. *This option is only available if the session was recorded.*

## Saved Filters

Various filters in the Sessions report are useful to customize the view to the system assets for different purposes by the *Auditors*, *System Administrators*, *System Owners*.

1. **Select** Columns or Filters to display in your Sessions report.
2. **Save** various Sessions report configurations (report columns and filters) for further.
3. Reuse and receive quick access to the saved filters.



### Save Report

Name




### System Sessions



Found sessions.

Time: Last Month ▾ State: Any ▾ Columns ▾   

Show  entries

Search:

Showing 1 to 17 of 17 entries

Record	Start Time	Completion Time	Status	Session Manager	Rating	Recording
Unix QA team	12/09/2021 09:44:48	12/09/2021 09:44:58	Completed	ssl:pam02-01:4822	★★★★★	Available 
Windows QA	12/09/2021 09:27:04	12/09/2021 09:29:25	Completed	ssl:pam02-01:4822	★★★★★	Available 

## Session Events Report

The Session Events report provides a list of all keystrokes including SQL traffic over tunnels, clipboard text, command sequences and file transfers users entered or performed during any remote session.

Use this report to investigate session activity and search for keystroke or command entries throughout all sessions.

## Options

The following options are provided with the Session Events report:

- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.
- **Refresh** is available by clicking on the refresh icon.

- **Save** is available by clicking on the star icon.
- **Subscribe** is available by clicking on the envelop icon.

## Provided Information

The following information is provided as columns in the Session Events report:

- **Session:** Displays the name of the record that was used to connect to this session.
- **User:** Displays the user that entered these session events during the remote session.
- **Start Time:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the session event started. The value in the parenthesis displays the time from the beginning of the session that this event was captured. Use this value to quickly locate the event if viewing the session recording.
- **End Time:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the session event completed. This column will be empty for Clipboard and Command Sequence events.
- **Type:** Displays the type of the session event.
- **Preview:** Displays the session event that was entered or executed during the session, up to the first 1024 characters. Use the Details option in the Action menu to see all the characters.
- **IP** Displays the users IP that entered these session events during the remote session.
- **Account** Displays the users role that entered these session events during the remote session.
- **Request** Displays the users Request for entered these session events during the remote session.
- **Actions Menu:** Provides the following options:
  - **Details:** Displays the full list of characters entered during this session event.
  - **Jump to Recording:** Opens the in-browser video player and jumps to the session time when this event started. *This option is only available when the session was recorded.*

## Saved Filters

Various filters in the Session Events report are useful to customize the view to the system assets for different purposes by the Auditors, System Administrators, System Owners.

1. **Select** Columns or Filters to display in your Session Events report.
2. **Save** various Session Events report configurations (report columns and filters) for further.
3. **Reuse** and receive quick access to the saved filters.

Save Report

Name

Found 9 Session Events.

Time: Last Month

Columns



Show 50 entries

Search: Remote

CSV

PDF

XLSX

PDF Protected

CSV Protected

XLSX Protected

Showing 1 to 9 of 9 entries

Session	User	Start Time	End Time	Preview	Request	Action
Remote Ubuntu Desktop	Service Administrator (pamadmin) /Local	12/09/2021 09:18:53 ( +5m 45s )	12/09/2021 09:19:03 ( +5m 54s )	<div>c h s Backspace d Backspace Backspace Backspace c h Space Backspace Backspace Backspace</div>		...
Remote Ubuntu Desktop	Service Administrator (pamadmin) /Local	12/09/2021 09:13:59 ( +51s )	12/09/2021 09:14:03 ( +54s )	<div>p a n f Backspace Backspace Backspace Backspace l s Enter</div>		...

## Statistics Report

The Statistics report provides a graphical understanding of various categories of objects throughout the PAM system as well as trending data over a 7 day period.

Statistics are gathered once per day using an automated system task.

## Available graphs

The following graphs are available in the Statistics report:

**Total Records Trend:** Displays a line chart of the total number of records in PAM over the past 7 days.

**Total Records Count:** Displays a pie chart of the total number of records currently in PAM by Record Types.

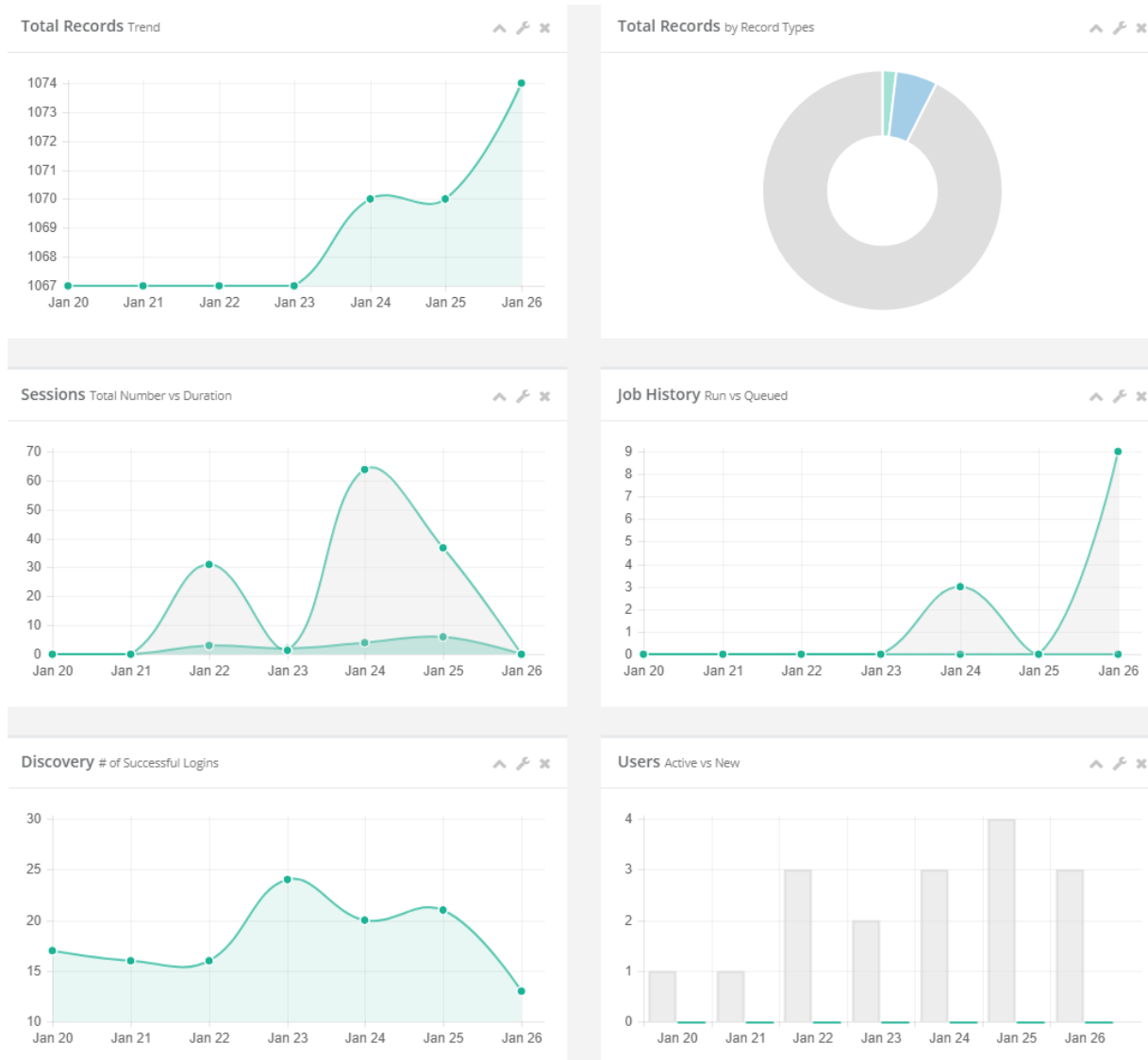
**Sessions:** Displays a comparative line chart of the total number of sessions vs duration (in minutes) per day over the past 7 days.

**Job History:** Displays a comparative line chart of the total number of run vs queued tasks per day over the past 7 days.

**Discovery:** Displays the total number of successful objects found during discovery per day over the past 7 days.

**Users:** Displays a comparative bar graph of the number of new vs active PAM users per day over the past 7 days. Active indicates at least one login to PAM during a day.





## Subscriptions (Reports)

The Subscriptions (Reports) report provides a list of reports that the users' of PAM are subscribed to, along with their report configuration and an option to Unsubscribe them from their selected report(s).

## Options

The following options are provided with the Subscriptions (Reports) report:

- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.

## Provided Information

The following information is provided as columns in the Subscriptions (Reports) report:

- **User:** Displays the User name (login name) of the user subscribed to this report.
- **Object:** Displays the name of the object associated to the report. If it is associated to PAM as a whole rather than an individual named object (i.e. the System), then this value will be blank.
- **Object Type:** Displays the type of object. For example, Folder or *Record Type* name.
- **Report Type:** Displays the type of report. For example Audit Log or Inventory report.
- **Format:** Displays the format of the generated report; PDF, CSV or XLSX.
- **Period:** Displays the delivery period of the report; Daily, Weekly or Monthly.
- **Last Sent:** Displays the date this report was last sent to the user. If the user has not yet received a report, then this will be blank.
- **Next Run:** Displays the date the next time this report is scheduled to be sent to this user.
- **Filter:** Displays the configuration (filter) of their report.
- **Subscription Type:** Displays the subscription type.
- **Column Visibility:** Displays the column visibility.
- **Actions:** Click the **Unsubscribe** button to unsubscribe this user from their scheduled report.

#### Subscriptions (Reports)

Found 5 objects.

Columns 

Show  entries

Search:

CSV PDF XLSX PDF Protected CSV Protected XLSX Protected

Showing 1 to 5 of 5 entries

User	Report Type	Format	Period	Last Sent	Next Run	Action
w w (kate user) /Local	WorkflowRequests	text/csv	Monthly	06/01/2021 15:28:41	07/01/2021 07:00:00	<button>Unsubscribe</button>
w w (kate user) /Local	JobHistory	text/csv	Monthly	06/01/2021 15:28:40	07/01/2021 07:00:00	<button>Unsubscribe</button>
Chris K (chrisk) /Local	WorkflowRequests	text/csv	Monthly	06/01/2021 15:28:43	07/01/2021 07:00:00	<button>Unsubscribe</button>
Chris K (chrisk) /Local	Inventory	text/csv	Monthly	06/01/2021 15:28:38	07/01/2021 07:00:00	<button>Unsubscribe</button>
Peter Senescu (psenescu) /AD	Inventory	text/csv	Monthly	06/01/2021 15:28:37	07/01/2021 07:00:00	<button>Unsubscribe</button>

First Previous 1 Next Last

## Subscriptions (Alerts)

The Subscriptions (Alerts) report provides a list of alerts that the users' of PAM are subscribed to, along with their alert configuration and an option to Unsubscribe them from their selected alert(s).

## Options

The following options are provided with the Subscriptions (Alerts) report:

- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.

## Information

The following information is provided as columns in the Subscriptions (Alerts) report:

- **User:** Displays the User name (login name) of the user subscribed to this alert.
- **Object:** Displays the name of the object associated to the alert. If it is associated to PAM as a whole rather than an individual named object (i.e. the System), then this value will be blank.
- **Object Type:** Displays the type of object. For example, Folder, System or *Record Type* name.
- **Category:** Displays the category of the alert.
- **Level:** Displays the level of the alert.
- **Event:** Displays the Event Filter value of the alert. If the user did not include a Filter value, then this will be blank.
- **Actions:** Click the **Unsubscribe** button to unsubscribe this user from their alert.

#### Subscriptions (Alerts)

Found 21 objects.






Columns 

Show  entries

Search:

CSV PDF XLSX PDF Protected CSV Protected XLSX Protected

Showing 1 to 21 of 21 entries

User 	Object 	Object Type	Category 	Level 	Event 	Action
Zulin Kalathiya (zkalathiya) /AD	<a href="#">Windows Host</a>	Windows Host	Operation	Information	Update Queue Record	<button>Unsubscribe</button>
Zulin Kalathiya (zkalathiya) /AD	<a href="#">Windows Temporary Permission Elevation - Admin</a>	Windows Host	Operation	Information	Update Queue Record	<button>Unsubscribe</button>
Slack Email (XTAMSlack) /Local	<a href="#">Default Root</a>	Folder	Operation	Information	connect	<button>Unsubscribe</button>
Chris K (chrisk) /Local		System	Event	All	Invalid command forbidden	<button>Unsubscribe</button>

## Tasks Report

The Tasks report provides a list of all records that have at least one task associated to them, along with each task's details.

Please note that records that have no tasks will be excluded from this report.

## Options

The following options are provided with the Tasks report:

- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.

## Provided Information

The following information is provided as columns in the Tasks report:

**Record:** Displays the name of the record and its record type.



**Tasks:** Displays the list of all Tasks associated to this record in the format: Script Name (Policy Event).

**Shadow Account:** Displays the associated Shadow Account that is configured to execute the record’s Task. If no [Shadow Account](#) is assigned, then the column value will be empty.

**Inheritance:** Displays whether the record’s task list is unique to this record (Unique) or if it is inherited from a parent (Inherited).

Tasks Report

Found 615 entries.

Columns  

Show 

50

 entries

Search:

CSV

PDF

XLSX

PDF Protected

CSV Protected

XLSX Protected

Showing 1 to 50 of 615 entries

Record	Tasks	Shadow Account	Inheritance
<a href="#">ACME Domain Shadow Account</a> Record Type: Active Directory Account	<ul style="list-style-type: none"><li>Password Reset LDAP (On demand)</li><li>Check Status LDAP (On demand, After Update)</li></ul>		Inherited
<a href="#">After Create or Update</a> Record Type: Windows Host	<ul style="list-style-type: none"><li>Password Reset Remote Windows (On demand)</li><li>Check Status Remote Windows (On demand)</li><li>Windows Local Admin Group Cleanup (On demand)</li></ul>		Inherited
<a href="#">Days after Unlock</a> Record Type: Windows Host	<ul style="list-style-type: none"><li>Password Reset Remote Windows (On demand)</li><li>Check Status Remote Windows (On demand)</li><li>Windows Local Admin Group Cleanup (On demand)</li></ul>		Inherited
<a href="#">Every 2nd day</a> Record Type: Windows Host	<ul style="list-style-type: none"><li>Password Reset Remote Windows (On demand)</li><li>Check Status Remote Windows (On demand)</li><li>Windows Local Admin Group Cleanup (On demand)</li></ul>		Inherited

## Users Report

The Users report provides a list of all users and groups that have accessed PAM, including metadata, IP, activity and permissions.

## Options

The following options are provided with the Users report:

- Search** is available to quickly locate objects using string based queries.
- Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- Sorting** is available by clicking on the desired column header.
- Subscribe** is available by clicking on the envelop icon.
- Save** is available by clicking on the star icon.
- Refresh** is available by clicking on the refresh icon.

## Provided Information

The Columns in the Users report have such information to choose:

- ID:** Displays the ID of the record of the user or group.
- User:** Displays the name of the user or group.
- Type:** Displays the type, either *User* or *Group*.
- First Activity:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when this was added to PAM.
- Last Activity:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the last action was performed by this user.
- Last IP:** Displays the detected IP address of the user from where they last logged into PAM.
- Groups:** Displays the name of any Groups that this user is a member of.

- **Global Roles:** Displays the Global Role assigned to this user and how it was assigned, either directly or via Group membership. This column will be empty for user who have not been assigned a Global Role.
- **Object:** Displays the total number of objects that this user has at least Viewer permissions to access.
- **Event:** Displays the total number of system audit events associated to this user.
- **MFA Token:** Displays the Google Authenticator MFA token assigned to this user.
- **Directory:** Displays the origin of the user, either AD if using Active Directory integration or Local if created as a Local User or Group in PAM.
- **SSH Key:** Displays the SSH Key associated to this user.
- **Action Menu:** Provides the following options:
  - *AD Sync:* Retrieves current First and Last name from Active Directory for this user. *This option will only appear for Active Directory users.*
  - *Reset Cache:* If a user does not have access to any objects nor generated any events, then this option will remove them from this report.
  - *Remove Duplicate Entries:* When a user appears multiple times in the report, use this option to remove the duplicate entries.
  - *View Audit Log:* Opens the System Audit Log report filtered to display only events for this user.
  - *View Objects:* Opens the Inventory report filtered to display only objects this user has permissions to view.
  - *Block/Unblock User:* Blocks or unblocks the user or group members' access to objects in PAM. The blocked user can still login to PAM, but until they are unblocked, they will have no access to any objects or settings. Only System Administrators may manually Block or Unblock users or groups. Blocked users will appear in this report with their User value crossed out (strike-through font).
  - *Block/Unblock SSH Key:* Blocks or unblocks the user's SSH Key (the column *SSH Key* must first be enabled to use this option). This user may no longer [authenticate using their SSH Key](#) until it is unblocked. Blocked SSH keys will appear in this report with their SSH Key create date value crossed out (strike-through font).
  - *Revoke All:* Permissions revokes global, record and folder permissions, global roles, and local group membership *using one button* on the Reports / Users report. The function simplifies user off-boarding from the system as well as releases the user count on the license enforcement. The option also reports a user as a group member in the integrated LDAP User Directory or Active Directory but does not remove the user from the integrated user directory.

## Saved Filters

Various filters in the Users report are useful to customize the view to the system assets for different purposes by the Auditors, System Administrators, System Owners.

1. **Select** Columns or Filters to display in your the Users report.
2. **Save** various Users report configurations (report columns and filters) for further.
3. Reuse and receive quick access to the saved filters.

### Save Report

Name

Found 8 users.

Columns   

Show 10 entries

Search:

CSV

PDF

XLSX

PDF Protected

CSV Protected

XLSX Protected

Showing 1 to 8 of 8 entries

User	First Activity	Last Activity	Object	Event	Directory	
Service Administrator (pamadmin) /Local	11/09/2021 10:32:53	11/26/2021 10:28:55	All	390	Local	...
Brian Williams (bwilliams) /Local	11/15/2021 11:27:41	11/26/2021 10:28:42	12	7	Local	...
John Smith (jsmith) /Local	11/15/2021 12:10:15	11/17/2021 09:41:51	All	3	Local	...
Mary Right (mright) /Local	11/15/2021 12:14:37	11/26/2021 09:50:56	1	6	Local	...

## Workflow Report

The Workflows report provides a list of all workflows along with their templates, bindings and configuration.

### Options

The following options are provided with the Workflows report:

- **Search** is available to quickly locate objects using string based queries.
- **Export** is available to export the available on-screen data to either a CSV, PDF or XLSX file.
- **Sorting** is available by clicking on the desired column header.

### Provided Information



The following information is provided as columns in the Workflows report:

- **Template:** Displays the name of the template assigned to this workflow instance.
- **Users:** Displays the name of the user(s) or group(s) bound to the workflow.
- **What:** Displays the action that is associated to this workflow instance that requires approval to access.
- **When:** Displays the enabled time selector(s) that is bound to this workflow instance.
- **IP:** Displays the IP filter that is bound to this workflow instance.
- **Duration:** Displays the duration value that is bound to this workflow instance.
- **Checkout:** Displays the checkout state is bound to this workflow instance. (Disabled/Optional/Required).
- **MFA:** Displays the MFA state that is bound to this workflow instance. (Disabled/Required).
- **Weight:** Displays the order value that is bound to this workflow instance.
- **Object:** Displays the object (and provides a link to open it) that is assigned this workflow instance.
- **Approvers:** Displays the list of approvers in each step that are assigned to either Approve or Reject the access request.

Workflows Report

The Workflow report provides a list of all workflows in the solution along with their configuration.

Found 1 bindings.

Columns  

Show 10 entries

Search:

CSVPDFXLSXPDF ProtectedCSV ProtectedXLSX Protected

Showing 1 to 1 of 1 entries

Template	Users	What	When	IP	Duration	Checkout	MFA	Weight	Object	Approvers
interactive	wfuser 1 (wfuser1) /Local	All	Always			Disabled	Disabled	100	Root Folder	Step: 1: Service Administrator (pamadmin) /Local (1)

FirstPrevious1NextLast

# Report Center

Report Center is a central location for PAM reports, both built-in and user saved. The built-in reports generally help to locate objects, find user activity, understand permissions and view audit events throughout the system. The user saved reports are versions of the built-in reports that have been customized through the use of unique filters and columns to better locate specific information in PAM.

Report Center can only be accessed by the User with the following roles:

- *System Administrator* role;
- *Auditor* role;
- *Owner* of a record. As an owner, you can only view the report center for the object itself but you can't access the whole system report center. The 'report center' button is only available on the object itself and not from *Records* tab.

Conveniently located in the *Records* section of the application menu for global reports and on the Container level for *Owners*, the Report Center houses available reports grouped by their base type. When a user creates a *Saved Report*, it will be accessible from their *Report Center* in a private view, meaning only visible and managed by the user who created the report. To share their private report, the report owner may choose to **Publish** the report which will make it visible to others in their *Report Center*.

Please note that *System Administrators* have a unique [role](#) in the *Report Center* to oversee and manage all published saved reports. *System Administrator* users will have the options to *view*, *rename*, *unpublish* and *delete* any saved and published reports in the *Report Center*. Unpublished saved reports are only available to the report *Owner*.

**Reports** is the first default tab, displays the current saved reports visible in the Report Center.

**Custom Queries** the second tab, when selected, displays the contents and controls available from the existing Reports > **Custom Queries** page.

## Options

The following options are available in the *Report Center*:

- **Filter** is available to quickly search for a report(s) using specific terms.
- **Bulk Actions** is available to perform an action on multiple, selected saved reports.
- **Select/Unselect All** is available to select all or unselect all saved reports. This option does not select built-in reports.
- **Delete** is available to delete, single or bulk, saved reports that are selected. Use with caution as deleted reports cannot be restored. This option is not available for built-in reports.

## Provided Information

The following information is provided as columns in the *Report Center*:

Only saved reports have Actions. Built-in reports may only be Viewed.

- **Report Type:** Represents the first column header label where all reports, built-in and saved, are grouped by the type of base report from which the report was saved.
- **Name/Description:** Displays the Name and (optional) Description of the report. A saved report's selection box is located to the left of this column.
- **Owner:** Displays the name of the user who created the saved and published report. Built-in and unpublished reports will not display an Owner value.
- **Is Public:** Displays a checkmark for saved reports that have been published or made visible to other permissioned users in their Report Center. Non-public or unpublished saved reports are only visible to the report's Owner.
- **Actions Menu:** Provides the following options to the saved report's Owner or System Administrators (for published reports):
  - *View:* Opens the selected report.
  - *Update Name/Description:* Provides a prompt to modify the saved report's Name and Description.
  - *Publish and Unpublish:* Publish makes a private report available for others to view. Unpublish makes a public report private so that only the report Owner may access.
  - *Delete:* Deletes the selected saved report (single and bulk delete options are available). Use with caution as a deleted report cannot be restored.



## Working with the API

PAM provides a full suite of REST based APIs that can be used to interact with all aspects of the software using custom code or through integration with third-party systems.

To view the full, interactive REST API documentation utilizing OpenAPI formatting, navigate to Administration > Settings > Application Nodes and click the **API Documentation** link.

To see additional examples of API scripts, commands and examples in different languages ([PowerShell](#), [Shell](#), [VBScript](#) and [Python](#)), we encourage you to visit our online help site to search the API documentation.

There are several detailed articles that explain advanced topics when working with the PAM APIs.

## Authentication Tokens

Authentication Tokens allow users to work with the API, without having to hardcode usernames and passwords into their code, to create secure communication channels.

In addition to the benefit of using authentication tokens rather than user and password values in your code, tokens also:

- Have an expiration date to provide temporary usage to internal or external resources.
- Are associated to an actual PAM user account to more easily correlate API functions back to the user.
- Can be restricted to a certain IP filter to limit their use from specific locations.
- Include a comment field to describe their intended usage.
- Can be disabled (and eventually enabled again) or permanently deleted.

NOTE: The use of Authentication Tokens in PAM requires certain pre-requisites to be installed and configured on the host server. Please review our online [Authentication Token](#) article regarding these requirements.

## Managing Tokens

1. To work with new or existing authentication tokens, navigate to Administration > Tokens.
2. Only System Administrators can create and manage Tokens.
3. To generate a new token, click the **Generate Token** button and populate the fields as described below.
4. When finished, click the **Generate** button to generate the token.
5. Once generated, the actual token will appear in the *read-only* **Token** field on this form.

Principal	Enter a user to be associated to this token. A token cannot be assigned to multiple users or groups.
Expiration (mins)	Token expiration time in minutes. Leave this field empty to generate a token that will not expire.

IP Filter	Token access location given as a comma-separated list of IPv4 or IPv6 addresses or masks, optionally preceded by dash to indicate valid IP space outside of the specified mask.  Examples of IP Filter: 10.0.0.0/24 -10.0.0.0/24 10.0.0.0/24,10.1.1.0/24,10.2.2.122
Comment	Brief comment about the token's intended purpose or use.
Token	Displays the token value (read only) once the <i>Generate</i> button is clicked.

Tokens with an expiration date will display this time in the token's row. Expired tokens will be shown with this time struck out.

*To enable or disable* an existing token, click the appropriate **Enable** or **Disable** button shown in the token's row.

Disabled tokens will be shown with the token value struck out and the *Copy to Clipboard* option removed.

*To permanently delete* an existing token, click the **Delete** button shown in the token's row.

## Token Authentication

Using Authentication Tokens for PAM REST APIs.

PAM has always exposed APIs for every function it has, but the only way to access the API is with the use of a username and password.

This means that the application that calls PAM should have this hard coded username and password to login to PAM and ultimately call the API function like creating a new record.

This is generally considered an undesirable approach because exposing the username and password like this also exposes other areas of the network that this user can access which may be completely unrelated to the System's operations.

Because of this and other reasons, we implemented the recommended practice of letting other applications login to the System using tokens.

What PAM can do is generate tokens for a specific user where this token could be used to authenticate in PAM on behalf of the user for which this token was generated.

Then the external application that wants to communicate with PAM should have access to PAM by the PAM-generated token that is saved to or hard coded into the application or function.

The advantages of using the authentication token as compared to a username and password is that the token is specific to the PAM as opposed to an actual user's credentials.

This allows the application to communicate with the PAM without hard coding a user’s password anywhere thus protecting any other areas of the network that this user can access (think of using their AD credentials which could expose any number of security issues).

PAM provides the facilities to generate tokens for specified users, to maintain a current list of tokens and to enable (and disable) tokens invalidating them for subsequent use.

PAM also provides an option to create tokens with expiration making them invalid after a defined period of time.

Token	↕
eyJhbGciOiJIUzI1NiJ9.eyJzdWUiOiJid2lsbGhbmjE3O...	
eyJhbGciOiJIUzI1NiJ9.eyJzdWUiOiJjaHJpc2s6MjE3ODU5N...	
eyJhbGciOiJIUzI1NiJ9.eyJzdWUiOiJjaHJpc2s6MjE3ODU4O...	
eyJhbGciOiJIUzI1NiJ9.eyJzdWUiOiJta2xpbmNoaW46MjE3N...	

# Generate API Authentication Tokens

## To Generate API Authentication Tokens:

PAM requires the use of the [Federated Sign-In Module](#) in order to generate tokens. If you do not have this module deployed then the option to Generate Tokens will not be available.

1. Login to PAM as a System Administrator. *Only System Administrator can manage Authentication Tokens.*
2. Navigate to Administration > Tokens.
3. Click the **Generate Token** button.
4. Populate the *Generate Token* dialog as described below:
  - a. In the **Principal** field, enter the username that the token will be generated for.

Note that only a single user (not multiple users or groups) can have a token generated at a time. Simply repeat this process to generate tokens for additional users or to generate another token for this same user.

- b. In the **Expiration (mins)** field, enter an expiration time for the token in minutes. To generate a token that will not expire, leave this field empty.

Note that the expiration countdown begins when the token is generated not when it is first used.

- c. In the **IP Filter** field, enter location given as a comma-separated list of IPv4 or IPv6 addresses or masks optionally preceded by a dash to indicate valid IP space outside of the specified mask.
- d. In the **Comment** field, enter an optional comment related to this token.
- e. The **Token** field is read-only and will display the token after it is generated.

### Generate Token

Principal ?

bwilliams

Expiration (mins) ?

360

IP Filter ?

10.0.0.0/24

Comment ?

Application integration testing

Token ?

Close

Generate

- 5. When the Generate Token dialog is populated as needed, click the **Generate** button to generate the token for this user.
- 6. This token and its corresponding values will be displayed for reference in the **Authentication Tokens** list.

Only part of the Authentication Token is displayed in the Authentication Tokens list, so you will need to click the **Copy to Clipboard** ( PAM API Authentication Tokens Copy to Clipboard ) button to access the full token.

Read further about how to use these tokens to call the PAM [APIs](#) to retrieve secrets, create new records and more.

## Perform the actions

After the token(s) is generated, you may perform the following actions:

- **Sort** the ordering of tokens by clicking on the desired column header.
- Use the **Search** box to locate specific tokens.
- **Export** the displayed list of tokens to a CSV, PDF, XLSX, CSV Protected or XLSX Protected file.
- Click the **Copy to Clipboard** button to easily share the full token with your user(s) or to paste it into external applications or functions.
- Immediately **Enable** or **Disable** use of the tokens by clicking the appropriate option.

## Provided Information

The following information is provided as columns in the Authentication Tokens report:

- **ID:** Displays the internal PAM ID that is associated with this token.
- **Time:** Displays the timestamp (MM/DD/YYYY HH:MM:SS) of when the token was generated.
- **User:** Displays the user that is associated to this token.
- **Folder:** Displays the Folder.
- **Expiration:** Displays the expiration time associated to this token. An empty field means that the token does not have an expiration time and a time with a strike through indicates that the token has expired.
- **IP Filter:** Displays the comma-separated list of IPv4 or IPv6 addresses or masks optionally preceded by a dash to indicate valid IP space outside of the specified mask. Examples of IP Filter: 10.0.0.0/24, - 10.0.0.0/24, 10.0.0.0/24,10.1.1.0/24,10.2.2.122
- **Token:** Displays part of the token. Use the *Copy to Clipboard* button to access the full token. Disabled tokens will be shown with a strikethrough.
- **Comment:** Displays the optional comment that was associated to this token.
- **Actions Menu:** Provides the following options:
  - **Enable/Disable:** Click *Disable* to disable an enabled token or click *Enable* to enable a disabled token.
  - **Delete:** Click *Delete* to delete a token.

Authentication Tokens










Found 2 tokens.

[Generate Token](#) 

Show  entries

Search:  [CSV](#) [PDF](#) [XLSX](#) [PDF Protected](#) [CSV Protected](#) [XLSX Protected](#)

Showing 1 to 2 of 2 entries

 Id	 Time	 User	 Folder	 Expiration	 IP Filter	 Token	 Comment	
i-8olrwd52OMU	11/01/2021 17:14:56	Gali Fax (User Editor) /Local		<del>11/01/2021 17:24:56</del>	10.0.0.0/24	eyJhbGciOiJIUzI1Ni9eyjZldWl0aWZm9GZm96bzo1Nzg1N...	Access to the folder	<a href="#">Enable</a> <a href="#">Delete</a>
i-bay2H5adFWs	11/01/2021 17:12:03	Victoria Fomenko (vfomenko) /Local		11/01/2021 17:42:03	10.0.0.0/24	eyJhbGciOiJIUzI1Ni9eyjZldWl0aWZm9GZm96bzo1Nzg1N...	Enter to the site	<a href="#">Disable</a> <a href="#">Delete</a>

First Previous 1 Next Last

# API Parameters Details

## Connect Permissions

GUI – Session Control	API – Connect Permissions
None	None
Optionally Recording without Session Events	ConnectNoEvents
Always Recording without Session Events	RecordingNoEvents
Optionally Recording with Session Events	Connect
Always Recording with Session Events	Recording
No Recording with Session Events	NoRecording
No Recording without Session Events	NoRecordingNoEvents

## API Examples

### PowerShell

Getting Started Guide using REST APIs in PowerShell with Privileged Access Management.

This page outlines several specific scenarios in which REST APIs in PAM can be called using PowerShell scripts. Please note that security is strictly enforced, so ensure the account executing the scripts has the appropriate permissions to access the objects in PAM.

In addition to this detailed guide you can also view the list of other functions you can call using REST API by navigating to Administration > Settings > Application Nodes > API Documentation.

Looking for REST API examples using other scripts? Click [Shell examples](#), [VBScript examples](#) or [Python examples](#) for additional information.

The following scripts are provided as an example of what is possible, however they can and should be customized to meet your requirements including outside script integration, formatting and proper error handling.

- [Create a Record](#)
- [Create a Folder](#)
- [Retrieve Root Folder](#)
- [List Folder Content](#)
- [Retrieve a Record](#)
- [Retrieve a Record with Password \(Unlock\)](#)
- [Retrieve a Record Field \(Unlock\)](#)

- [Update a Record](#)
- [Download a File](#)
- [Share a Record or Folder](#)
- [Delete a Record](#)
- [Search for Objects \(Record or Folder\)](#)
- [List Record Types](#)
- [Database Export \(Decrypted\)](#)
- [Database Export \(Encrypted\)](#)
- [Database Import](#)
- [API Token](#)
- [Secure Authentication](#)

## Create a Record

Provides the ability to create a new record with the defined parameters.

```

1  $folderId="183320"    # ID of Parent Folder
2  $typeId = "1724"     # ID of Record Type
3  $recordName = "Name"  # Record Name (required)
4  $recordDescription = "Description" # Record Description (optional)
5
6  $rhost = "host.company.com" # Host URL
7  $rport = "22"             # Host Port
8  $ruser = "user"           # Host User
9  $rpassword="myPassw0rd"   # Host Password
10
11 $rest = "$url/rest/record/new/$folderId/$typeId"
12
13 $Custom = '{{"Host":"{0}","Port":{1},"User":"{2}","Password":"{3}"}}' -f $rhost,
14 $rport, $ruser, $rpassword
15
16 $Body = @{
17     name = $recordName
18     description = $recordDescription
19     custom = $Custom
20 }
21 Invoke-RestMethod -Method Post -ContentType 'application/x-www-form-urlencoded'
22 -Headers @{ 'X-XSRF-TOKEN' = $apiToken } -Credential $mycreds -Uri "$($rest)" -Body
23 $body
24 Write-Host Done

```

## Create a Folder

Provides the ability to create a new folder with the defined parameters.

```

1  $folderId="183320"    # ID of Parent Folder
2  $folderName = "Name"  # Folder Name (required)
3  $folderDescription = "Description" # Folder Description (optional)
4
5  $rest = "$url/rest/folder/create/$folderId"
6

```

```

7 | $folder = @{
8 |     name = $folderName
9 |     description = $folderDescription
10 | }
11 |
12 | $body = $folder | ConvertTo-Json
13 |
14 | Invoke-RestMethod -Method Post -ContentType 'application/json' -Headers @{'X-
XSRF-TOKEN' = $apiToken} -Credential $mycreds -Uri "$($rest)" -Body $body
15 |
16 | Write-Host Done

```

## Retrieve Root Folder

Provides the ability to retrieve the Root Folder (All Records) and its parameters including ID.

```

1 | $rest = "$url/rest/folder/root"
2 |
3 | Invoke-RestMethod -Method Get -ContentType 'application/json' -Credential
$mycreds -Uri "$($rest)"
4 |
5 | Write-Host Done

```

## List Folder Content

Provides the ability to list all content of the specified folder.

```

1 | $folderId="183320"    # Folder ID
2 |
3 | $rest = "$url/rest/folder/list/$folderId"
4 |
5 | Invoke-RestMethod -Method Get -ContentType 'application/json' -Credential
$mycreds -Uri "$($rest)"
6 |
7 | Write-Host Done

```

## Retrieve a Record

Provides the ability to retrieve all the parameters of an existing record **excluding** the password.

```

1 | $recordId="168351"    # Record ID
2 |
3 | $rest = "$url/rest/record/get/" + $recordId
4 |
5 | $secret= Invoke-RestMethod -ContentType 'application/json' -Credential $mycreds
-Uri "$($rest)"
6 |
7 | $custom= $secret.custom | ConvertFrom-Json

```



```

8 |
9 | Write-Output "$($secret.name): $($custom.User) / $($custom.Password)"
10 |
11 | Write-Output $secret
12 | Write-Output $custom
13 | Write-Host Done

```

## Retrieve a Record with Password Unlock

Provides the ability to retrieve all the parameters of an existing record **including** the password.

```

1 | $recordId="168351"    # Record ID
2 |
3 | $rest = "$url/rest/record/unlock/" + $recordId
4 |
5 | $secret= Invoke-RestMethod -ContentType 'application/json' -Credential $mycreds
   -Uri "$($rest)"
6 |
7 | $custom= $secret.custom | ConvertFrom-Json
8 |
9 | Write-Output "$($secret.name): $($custom.User) / $($custom.Password)"
10 |
11 | Write-Output $secret
12 | Write-Output $custom
13 | Write-Host Done

```

## Retrieve a Record Field Unlock

Provides the ability to retrieve a single parameter from a record's field **including** the password.

```

1 | $recordId="168351"    # Record ID
2 | $field="Password"     # The (internal) Name of the field
3 |
4 | $rest = "$url/rest/record/unlock/$recordId/" + $field
5 |
6 | $secret= Invoke-RestMethod -ContentType 'application/json' -Credential $mycreds
   -Uri "$($rest)"
7 |
8 | Write-Output "$($field): $($secret)"
9 | Write-Host Done

```

## Update a Record

Provides the ability to update an existing record.

```

1 | $recordId="183323"    # Record ID
2 | $recordTypeId="e9uc9Av36zM" # Record Type ID

```

```

3  $RecordName = "Updated Name"    # Updated Record Name
4  $RecordDescription = "Updated Description"    # Updated Record Description
5
6  $rhost = "host1.company.com"    # Updated Host URL
7  $rport = "3389"    # Updated Host Port
8  $ruser = "user1"    # Updated Host User
9  $rpassword="myPassw0rd1"    # Updated Host Password
10
11 $password = $mycreds.GetNetworkCredential().password
12
13 $base64AuthInfo = [Convert]::ToBase64String([Text.Encoding]::ASCII.GetBytes("{0}:{1}" -f $user,$password))
14
15 $rest = "$url/rest/record/update/$recordId"
16
17 $Custom = '{{"Host":"{0}","Port":{1},"User":"{2}","Password":"{3}"}}' -f $rhost,
18 $rport, $ruser, $rpassword
19 Write-Host $Custom
20
21 $Body = @{
22     name = $RecordName
23     description = $RecordDescription
24     custom = $Custom
25     rtid = $recordTypeId
26 }
27
28 Invoke-RestMethod -Method Put -ContentType 'application/x-www-form-
29 urlencoded' -Credential $mycreds -Headers @{Authorization = "Basic
30 $base64AuthInfo"; 'X-XSRF-TOKEN' = $apiToken} -Uri "$($rest)" -Body $body
31
32 Write-Host Done

```

## Download a File

Provides the ability to download a file (certificate, SSH key, secured file) associated to a record.

```

1  $recordId="183323"    # Record ID
2  $fieldName = "Cert"    # Internal Name of Field that contains the file
3
4  $rest = "$url/rest/record/unlock/" + $recordId
5
6  $secret= Invoke-RestMethod -ContentType 'application/json' -Credential $mycreds
7  -Uri "$($rest)"
8
9  $custom= $secret.custom | ConvertFrom-Json
10 $file= $custom.$fieldName
11 $fileName= $file.name
12
13 $dwnld = "$url/rest/content/record/$recordId/$fieldName"
14 $output = "C:\Folder\" + $fileName    # Save To Location
15
16 Invoke-WebRequest -Credential $mycreds -Uri $dwnld -OutFile $output
17
18 Write-Output Done

```

## Share a Record or Folder

Provides the ability to share a record or folder with other users or groups.

```
1 $shareUser = "user" # Share object with User or Group Login
2
3 $rest = "$url/rest/user/ensure/$shareUser"
4 $shareUserId = Invoke-RestMethod -Method Get -ContentType 'application/x-www-
  form-urlencoded' -Credential $mycreds -Uri "$($rest)"
5
6 $objectId="186460" # Record or Folder ID to Share
7 $userId = $shareUserId.id
8 $recordControl = "View" # Permission Options: View / Unlock / Edit / Admin
9 $sessionControl = "None" # Permission Options: None / Recording / Connect
10 $taskControl = "None" # Permission Options: None / Execute / Review / Manage
11
12 $rest =
  "$url/rest/permissions/share/$objectId/$userId/$recordControl/$sessionControl/$t
  askControl"
13
14 Invoke-RestMethod -Method Post -ContentType 'application/json' -Headers @{ 'X-
  XSRF-TOKEN' = $apiToken } -Credential $mycreds -Uri "$($rest)"
15
16 Write-Host Done
```

## Delete a Record

Provides the ability to delete an existing record.

```
1 $recordId="186008" # Record ID to Delete
2 $folderId="183320" # Parent Folder ID
3
4 $password = $mycreds.GetNetworkCredential().password
5
6 $base64AuthInfo = [Convert]::ToBase64String([Text.Encoding]::ASCII.GetBytes(("
  {0}:{1}" -f $user,$password)))
7
8 $rest = "$url/rest/record/delete/$folderId/$recordId"
9
10 Invoke-RestMethod -Method Delete -ContentType 'application/json' -Headers @
  {Authorization = "Basic $base64AuthInfo"; 'X-XSRF-TOKEN' = $apiToken } -Uri
  "$($rest)"
11
12 Write-Host Done
```

## Look up for Objects

Search for Objects (Record or Folder).

Provides the ability to search for existing objects, like records or folders, using search query types.

A list of query types can be found [here](#) and will allow you to target specific objects like folders, ACLs or shadow accounts. For example, if you use the search term **folder:Production**, it will return all folders found using the term *Production*.

```
1 | $searchTerm = "object name"    # Value to Search
2 |
3 | $rest = "$url/rest/record/find/View/$searchTerm"
4 |
5 | $secret=Invoke-RestMethod -Method Get -ContentType 'application/json' -
   Credential $mycreds -Uri "$($rest)"
6 |
7 | Write-Host Results:
8 | foreach ($results in $secret){
9 |   Write-Host "Object Name:" $results.name "( Object ID:" $results.id)"
10 | }
11 |
12 | Write-Host Search Complete
```

## List Record Types

Provides the ability to output a list of all currently available Record Types.

```
1 | $rest = "$url/rest/recordtype/list"
2 |
3 | Invoke-RestMethod -Method Get -ContentType 'application/json' -Credential
   $mycreds -Uri "$($rest)"
4 |
5 | Write-Host Done
```

## Database Export Decrypted

Provides the ability to export the PAM database to a decrypted file(s).

```
1 | $password = $mycreds.GetNetworkCredential().password
2 | $base64AuthInfo = [Convert]::ToBase64String([Text.Encoding]::ASCII.GetBytes("{0}:
   {1}" -f $user,$password))
3 |
4 | $rest = "$url/rest/application/export/false"
5 |
6 | Invoke-RestMethod -Method Put -ContentType 'application/json' -Credential
   $mycreds -Headers @{Authorization = "Basic $base64AuthInfo"; 'X-XSRF-TOKEN' =
   $apiToken } -Uri "$($rest)"
7 |
8 | Write-Host Done
```

## Database Export Encrypted

Provides the ability to export the PAM database to an encrypted file(s).

```

1 | $password = $mycreds.GetNetworkCredential().password
2 | $base64AuthInfo = [Convert]::ToBase64String([Text.Encoding]::ASCII.GetBytes("{0}:{1}" -f $user,$password))
3 |
4 | $rest = "$url/rest/application/export/true"
5 |
6 | Invoke-RestMethod -Method Put -ContentType 'application/json' -Credential
   $mycreds -Headers @{Authorization = "Basic $base64AuthInfo"; 'X-XSRF-TOKEN' =
   $apiToken } -Uri "$($rest)"
7 |
8 | Write-Host Done

```

## Database Import

Provides the ability to import an exported PAM database file.

```

1 | $exportName="xtamexp-20180313152316-120" # Export file name
2 |
3 | $password = $mycreds.GetNetworkCredential().password
4 | $base64AuthInfo = [Convert]::ToBase64String([Text.Encoding]::ASCII.GetBytes("{0}:{1}" -f $user,$password))
5 |
6 | $rest = "$url/rest/application/import/$exportName"
7 | Invoke-RestMethod -Method Put -ContentType 'application/json' -Credential
   $mycreds -Headers @{Authorization = "Basic $base64AuthInfo"; 'X-XSRF-TOKEN' =
   $apiToken } -Uri "$($rest)"
8 |
9 | Write-Host Done

```

## API Token

To provide protection against Cross-Site Request Forgery (CSRF) attacks each PAM API function that changes something in the system (mostly, POST, PUT and DELETE REST methods) requires an API Token passed using X-XSRF-TOKEN header. To obtain a token, an PAM REST client has to request it from PAM server by calling /rest/user/whoami function that sets XSRF-TOKEN cookie with the value of the token. Below is the example of PowerShell functions that obtain the API token from PAM server by the server base URL and credentials (ApiToken) or a session (ApiTokenCas) objects depending on the style of the authentication. See examples of using this token in the code samples above.

```

1 | Function ApiTokenCas() {
2 |     [CmdletBinding()]
3 |     Param(
4 |         [Parameter(Mandatory=$true)] $session,
5 |         [Parameter(Mandatory=$true)] $url
6 |     )
7 |
8 |     process {
9 |         $rest = "$url/rest/user/whoami"

```

```

10     $resp=Invoke-RestMethod -WebSession $session -Method Get -Uri $rest -
MaximumRedirection 5
11
12     $session.Cookies.getCookies($rest) | % { if ($_.Name -eq 'XSRF-TOKEN') {
$apiToken = $_.Value } }
13     return $apiToken
14 }
15 }
16
17 Function ApiToken() {
18     [CmdletBinding()]
19     Param(
20         [Parameter(Mandatory=$true)] $creds,
21         [Parameter(Mandatory=$true)] $url
22     )
23
24     process {
25         $rest = "$url/rest/user/whoami"
26         $resp=Invoke-RestMethod -Credential $creds -Method Get -Uri $rest -
MaximumRedirection 5
27
28         $session.Cookies.getCookies($rest) | % { if ($_.Name -eq 'XSRF-TOKEN') {
$apiToken = $_.Value } }
29         return $apiToken
30     }
31 }

```

API token enforcement could be disabled by defining parameter **xtam.api.token.verification=false**

## Secure Authentication

PAM provides several methods for authenticating, first is a standard, non-federated username and password login, the second is a form-based login method, the third is a more robust [federated login experience](#) that supports multi-factor authentication and additional options and the fourth is using [Authentication Tokens](#). Depending on how your PAM installation is configured, the following authentication methods will be used.

### Standard Authentication (non-federated)

If your login experience to PAM is a simple prompt like the one shown below, then you will use the following to authenticate using our REST APIs.

Authentication required

http://localhost:8080

Username

Password

```
$url= "http://localhost:8080/xtam" # PAM URL
$user = "admin" # PAM User

$mycreds= Get-Credential $user

# Your code starts here
```

### Form-Based Authentication

If your login experience to PAM is a form-based login page like the one shown below, then you will use the following to authenticate using our REST APIs.

Welcome to XTAM

Username

Password

Copyright Xton Technologies © 2020

```
1 | $base= "https://pam.company.com/xtam" # PAM URL
```

```
2 | $UserName="admin"    # PAM User
3 | $Password="myPassword" # PAM Password
4 | $body=@{j_username=$UserName;j_password=$Password}
5 | $step1=Invoke-RestMethod -Uri "$($base)/rest/user/whoami" -SessionVariable
   | 'session'
6 | $step2=Invoke-RestMethod -Method Post -Uri "$($base)/j_security_check" -Body
   | $body -WebSession $session
7 |
8 | # Your code starts here
```

```
1 | Invoke-RestMethod -WebSession $session ... # Form-Based Authentication Invoke-
   | RestMethod cmdlet requires a web request session
```

## Federated Authentication

If your login experience to PAM is a federated sign-in page like the one shown below, then you will use the following to authenticate using our REST APIs.




# Log in to Imprivata Privileged Access Management



**Username:**

**Password:**

Log in

 [Forgot your password?](#)

For security reasons, please [log out](#) and exit your web browser when you are done accessing services that require authentication!

```
1  Function CasAuth() {
2      [CmdletBinding()]
3      Param(
4          [Parameter(Mandatory=$true)] $Base,
5          [Parameter(Mandatory=$true)] $CasBase,
6          [Parameter(Mandatory=$true)] $UserName,
7          [Parameter(Mandatory=$true)] $Password
8      )
9
10     process {
11         # post credentials
12         $body=@{username=$UserName;password=$Password}
13         $resp=Invoke-WebRequest -Method Post -Uri "$($CasBase)/v1/tickets" -Body
14         $body -SessionVariable 'session'
15
16         # get service ticket
17         If($resp.Headers.Location.GetType() -Eq [string]) {
```

```

17         $st=Invoke-WebRequest -Method Post -Uri $resp.Headers.Location -Body
"service=$( $Base)/"
18     } Else {
19         $st=Invoke-WebRequest -Method Post -Uri $resp.Headers.Location[0] -
Body "service=$( $Base)/"
20     }
21
22     # get authenticated session using service ticket
23     $resp=Invoke-WebRequest -Uri "$Base/?ticket=$st" -SessionVariable
'session'
24
25     return $session
26 }
27 }
28
29 $url="https://pam.company.com/xtam" # PAM URL
30 $cas_url="https://pam.company.com/cas" # PAM Signin Page URL
31
32 $user = "admin" # PAM User
33
34 $mycreds=Get-Credential $user
35 $password=$mycreds.GetNetworkCredential().password
36 $session=CasAuth -Base $url -CasBase $cas_url -UserName $user -Password
$password
37
38 # Your code starts here

```

**Invoke-RestMethod** -WebSession \$session ... # Federated Authentication Invoke-RestMethod cmdlet requires a web request session

## Token Authentication

If you are using Authentication Tokens, then you will use the following to authenticate using our REST APIs.

```

1  Function TokenAuth() {
2      [CmdletBinding()]
3      Param(
4          [Parameter(Mandatory=$true)] $Base,
5          [Parameter(Mandatory=$true)] $CasBase,
6          [Parameter(Mandatory=$true)] $Token
7      )
8
9      process {
10         try {
11             $resp=Invoke-WebRequest -Method Get -Uri
"$($CasBase)/login?service=$Base/" -Headers @{"token"="$Token"} -SessionVariable
'session' -UseBasicParsing -MaximumRedirection 0 -ErrorAction Ignore
12             If($resp.Headers.Location.GetType() -Eq [string]) {
13                 $loc=$resp.Headers.Location
14             } Else {
15                 $loc=$resp.Headers.Location[0]

```

```

16     }
17     } catch {
18         $loc=$_.Exception.Response.Headers.Location
19     }
20     $resp=Invoke-WebRequest -Uri "$loc" -SessionVariable 'session'
21
22     return $session
23 }
24 }
25
26 $url="https://pam.company.com/xtam" # PAM URL
27 $cas_url="https://pam.company.com/cas" # PAM Signin Page URL
28
29 $token = "yourXTAMtoken" # PAM Token
30
31 $session=TokenAuth -Base $url -CasBase $cas_url -Token $token
32
33 # Your code starts here

```

```

1 Invoke-RestMethod -WebSession $session ... # Token Authentication Invoke-
  RestMethod cmdlet requires a web request session

```

## REST API Shell Scripts

Getting Started Guide using REST APIs in Shell with Privileged Access Management.

This page outlines several specific scenarios in which REST APIs in PAM can be called using Shell scripts.

Please note that security is strictly enforced, so ensure the account executing the scripts has the appropriate permissions to access the objects in PAM.

In addition to this detailed guide you can also view the list of other functions you can call using REST API by navigating to Administration > Settings > Application Nodes > API Documentation.

Looking for REST API examples using other scripts? Click [PowerShell examples](#), [VBScript examples](#) or [Python examples](#) for additional information.

The following scripts are provided as an example of what is possible, however they can and should be customized to meet your requirements including outside script integration, formatting and proper error handling.

*Please note that our examples include use of curl for execution and [jq](#) for JSON parsing. Ensure these packages are deployed prior to executing the scripts or customize them to fit your needs.*

- [Create a Record](#)
- [Create a Folder](#)
- [Retrieve Root Folder](#)
- [List Folder Content](#)
- [Retrieve a Record](#)
- [Retrieve a Record with Password \(Unlock\)](#)
- [Retrieve a Record Field \(Unlock\)](#)
- [Update a Record](#)
- [Update One Record Field](#)
- [Download a File](#)
- [Share a Record or Folder](#)
- [Delete a Record](#)
- [Search for Objects \(Record or Folder\)](#)
- [List Record Types](#)
- [Database Export \(Decrypted\)](#)
- [Database Export \(Encrypted\)](#)
- [Database Import](#)
- [API Token](#)
- [Secure Authentication](#)

## Create a Record

Provides the ability to create a new record with the defined parameters.

```

1 | folderId="183320"    # ID of Parent Folder
2 | typeId="1724"       # ID of Record Type
3 | recordName="Record Name" # Record Name (required)
4 | recordDescription="Record Description" # Record Description (optional)
5 |
6 | rhost="host.company.com" # Host URL
7 | rport="22"             # Host Port
8 | ruser="user"           # Host User
9 | rpassword="myPassw0rd" # Host Password
10 | rparameters=
    {"Host\":"\
    $rhost\","\Port\":"\$rport\","\User\":"\$ruser\","\Password\":"\$rpassword\"}
11 |
12 | curl -s $auth -H "Accept: application/json" -H "Content-Type:application/x-www-
    form-urlencoded" -H "X-XSRF-TOKEN: $apitoken" -X POST \
13 | --data "name=$recordName&description=$recordDescription" --data-urlencode
    "custom=$rparameters" \
14 | $url/rest/record/new/$folderId/$typeId
15 |
16 | echo Done

```

## Create a Folder

Provides the ability to create a new folder with the defined parameters.

```

1 | folderId="183320"    # ID of Parent Folder

```

```

2 | folderName="Folder Name"    # Folder Name (required)
3 | folderDescription="Folder Description"    # Folder Description (optional)
4 |
5 | curl -s $auth -H "Accept: application/json" -H "Content-Type:application/json" -H
   | "X-XSRF-TOKEN: $apitoken" -X POST \
6 | --data "
   | {"name":\"
   | $folderName
   | \",\"description\": \"$folderDescription\"}" $url/rest/folder/create/$folderId
7 |
8 | echo Done

```

## Retrieve Root Folder

Provides the ability to retrieve the Root Folder (All Records) and its parameters including ID.

```

1 | rootFolder=$(curl -s $auth $url/rest/folder/root)
2 |
3 | rootFolderId=$(echo $rootFolder | jq -r '.id')
4 |
5 | #echo $rootFolder    # Retrieve all Root Folder parameters
6 | echo id:$rootFolderId    # Retrieve Root Folder ID
7 | echo Done

```

## List Folder Content

Provides the ability to list all content of the specified folder.

```

1 | folderId="183320"    # Folder ID
2 |
3 | allContent=$(curl -s $auth $url/rest/folder/list/$folderId)
4 |
5 | allNamesOnly=$(echo $allContent | jq '.[ ] | .name, .id')
6 |
7 | #echo $allContent    # Get all Content parameters
8 | echo $allNamesOnly    # Get all Content "Names" and ID only
9 |
10 | echo Done

```

## Retrieve a Record

Provides the ability to retrieve the parameters of an existing record excluding the password.

```

1 | recordId="168351"    # Record ID
2 |
3 | record=$(curl -s $auth $url/rest/record/get/$recordId)
4 | recordname=$(echo $record | jq -r '.name')
5 | check_status "Failed to unlock record"

```

```

6 |
7 | recorduser=$(get_custom "$record" "User")
8 | check_status "Failed to parse response"
9 |
10 | echo $recordname: $recorduser
11 | echo $record
12 | echo Done

```

## Retrieve a Record with Password Unlock

Provides the ability to retrieve the parameters of an existing record including the password.

```

1 | recordId="168351"    # Record ID
2 |
3 | record=$(curl -s $auth $url/rest/record/unlock/$recordId)
4 | recordname=$(echo $record | jq -r '.name')
5 | check_status "Failed to unlock record"
6 |
7 | recorduser=$(get_custom "$record" "User")
8 | recordpassword=$(get_custom "$record" "Password")
9 | check_status "Failed to parse response"
10 |
11 | echo $recordname: $recorduser / $recordpassword
12 | echo Done

```

## Retrieve a Record Field Unlock

Provides the ability to retrieve a single parameter from a record's field **including** the password.

```

1 | recordId="168351"    # Record ID
2 | $field="Password"    # The (internal) Name of the field
3 |
4 | record=$(curl -s $auth $url/rest/record/unlock/$recordId/$field)
5 | check_status "Failed to unlock record"
6 |
7 | recorduser=$(get_custom "$record" "User")
8 | recordpassword=$(get_custom "$record" "Password")
9 | check_status "Failed to parse response"
10 |
11 | echo $field: $record
12 | echo Done

```

## Update a Record

Provides the ability to update an existing record.

```

1 | recordId="183323"    # Record ID

```

```

2 | recordName="Updated Name"    # Updated Record Name
3 | recordDescription="Updated Description"    # Updated Record Description
4 |
5 | rhost="host1.company.com"    # Updated Host URL
6 | rport="3389"    # Updated Host Port
7 | ruser="user1"    # Updated Host User
8 | rpassword="myPassw0rd1"    # Updated Host Password
9 | rparameters=
10 | {"Host\":"\
11 | $rhost\","Port\":"\ $rport\","User\":"\ $ruser\","Password\":"\ $rpassword\"}
12 |
13 | curl -s $auth -H "Accept: application/json" -H "Content-Type:application/x-www-
14 | form-urlencoded" -H "X-XSRF-TOKEN: $apitoken" -X PUT \
15 | --data "name=$recordName&description=$recordDescription" \
16 | --data-urlencode "custom=$rparameters" \
17 | $url/rest/record/update/$recordId
18 |
19 | echo Done

```

## Update One Record Field

Provides the ability to update one record field.

```

1 | curl -s $auth -H "Accept: application/json" -H "Content-Type: application/json" -H
2 | "X-XSRF-TOKEN: $apitoken" -X PUT --data '{"string\":"FIELD-
3 | VALUE\"}" $base/record/updateField/$recordID/$fieldName

```

## Download a File

Provides the ability to download a file (certificate, SSH key, secured file) associated to a record.

```

1 | recordId="183323"    # Record ID
2 | fieldName="Cert"    # Internal Name of Field that contains the file
3 |
4 | curl -O -J $auth $url/rest/content/record/$recordId/$fieldName
5 |
6 | echo Done

```

## Share a Record or Folder

Provides the ability to share a record or folder with other users or groups.

```

1 | shareUser="user"    # Share object with User or Group Login
2 |
3 | shareUserParam=$(curl -s $auth $url/rest/user/ensure/$shareUser)
4 | shareUserId=$(echo $shareUserParam | jq -r '.id')
5 |
6 | objectId="186460"    # Record or Folder ID to Share
7 | userId=$shareUserId

```

```

8 | recordControl="View"    # Permission Options: View / Unlock / Edit / Admin
9 | sessionControl="None"  # Permission Options: None / Recording / Connect
10 | taskControl="None"     # Permission Options: None / Execute / Review / Manage
11 |
12 | curl -s $auth -H "X-XSRF-TOKEN: $apitoken" -X POST -d
    """
    $url
    /rest/permissions/share/
    $objectId/$userId/$recordControl/$sessionControl/$taskControl
13 |
14 | echo Done

```

## Delete a Record

Provides the ability to delete an existing record.

```

1 | recordId="186008"      # ID of Record to Delete
2 | folderId="183320"     # Parent Folder ID
3 |
4 | curl -s $auth -H "X-XSRF-TOKEN: $apitoken" -X DELETE
    $url/rest/record/delete/$folderId/$recordId
5 |
6 | echo Done

```

## Look up for Objects

Search for Objects Record or Folder.

Provides the ability to search for existing objects, like records or folders, using search query types.

A list of query types can be found [here](#) and will allow you to target specific objects like folders, ACLs or shadow accounts. For example, if you use the search term **folder:Production**, it will return all folders found using the term *Production*.

```

1 | searchTerm="object name" # Value to Search
2 | searchTerm=${searchTerm// /%20}
3 |
4 | results=$(curl -s $auth -X GET $url/rest/record/find/View/$searchTerm)
5 | searchResults=$(echo $results | jq '[] | .name, .id')
6 |
7 | echo Results:
8 | echo $searchResults      # Displays results as "Object Name" Object ID
9 | #echo $results           # Displays all parameters of Objects returned in results
10 | echo Search Complete

```

## List Record Types

Provides the ability to output a list of all currently available Record Types.



```

1 | recordTypes=$(curl -s $auth -X GET $url/rest/recordtype/list)
2 | recordTypeNamesId=$(echo $recordTypes | jq '.[ ] | .name, .id')
3 |
4 | echo $recordTypeNamesId      # Output as "Record Type Name" Record Type ID
5 | echo Done

```

## Database Export Decrypted

Provides the ability to output a list of all currently available Record Types.

```

1 | curl -s $auth -H "X-XSRF-TOKEN: $apitoken" -X PUT
   | $url/rest/application/export/false
2 |
3 | echo Done

```

## Database Export Encrypted

Provides the ability to output a list of all currently available Record Types.

```

1 | curl -s $auth -H "X-XSRF-TOKEN: $apitoken" -X PUT
   | $url/rest/application/export/true
2 |
3 | echo Done

```

## Database Import

Provides the ability to output a list of all currently available Record Types.

```

1 | exportName="xtamexp-20180313152316-120"      # Export file name
2 |
3 | curl -s $auth -H "X-XSRF-TOKEN: $apitoken" -X PUT
   | $url/rest/application/import/$exportName
4 |
5 | echo Done

```

## API Token

To provide protection against Cross-Site Request Forgery (CSRF) attacks each PAM API function that changes something in the system (mostly, POST, PUT and DELETE REST methods) requires an API Token passed using X-XSRF-TOKEN header.

To obtain a token, an PAM REST client has to request it from PAM server by calling /rest/user/whoami function that sets XSRF-TOKEN cookie with the value of the token.

Below is the example of Shell function that obtains the API token from PAM server by the server base URL and authentication string. See examples of using this token in the code samples above.

```

1 function api_token {
2     base=${1}
3     auth=${2}
4
5     whoami=$(curl -D whoami.tmp -s $auth $base/rest/user/whoami)
6     apitoken=$(cat whoami.tmp | grep "Set-Cookie" | cut -c 13- | cut -d "=" -f 2 |
7 cut -d ";" -f 1)
8     rm whoami.tmp
9     echo $apitoken
10 }

```

API token enforcement could be disabled by defining parameter `xtam.api.token.verification=false`

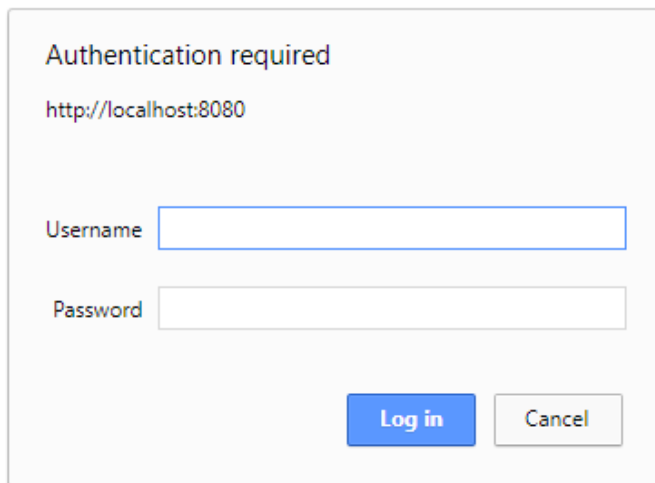
## Secure Authentication

PAM provides several methods for authenticating, first is a standard, non-federated username and password login, the second is a form-based login method, the third is a more robust [federated login experience](#) that supports multi-factor authentication and additional options and the fourth is using [Authentication Tokens](#).

Depending on how your PAM installation is configured, the following authentication methods will be used.

### Standard Authentication (non-federated)

If your login experience to PAM is a simple prompt like the one shown below, then you will use the following to authenticate using our REST APIs.



Authentication required

http://localhost:8080

Username

Password

```

1 #!/bin/bash
2
3 cookies=$(mktemp)
4 curl_opts="-s"
5
6 function cleanup {
7     rm -f ${cookies}
8 }

```

```

9
10 trap cleanup EXIT
11
12 function check_exe() {
13     which "$1" >/dev/null 2>&1
14     if [ "$?" -ne 0 ]; then
15         (>&2 echo "Required executable [$1] not found. Please install it using
system package manager.")
16         (>&2 echo "Exiting.")
17         exit 1
18     fi
19 }
20
21 function check_status() {
22     if [ $? != 0 ]; then
23         echo $1
24         exit 1
25     fi
26 }
27
28 function cas_auth {
29     base=${1}
30     cas_base=${2}
31     username=${3}
32     password=${4}
33
34     # get TGT ticket from Location header
35     tgt_location=$(curl ${curl_opts} -X POST -D - ${cas_base}/v1/tickets -d
"username=${username}" -d "password=${password}" | grep "^Location" | cut -d":" -
f 2- | tr -d \\r\\n)
36
37     if [ -z "${tgt_location}" ]; then
38         (>&2 echo "CAS authentication failed: unable to obtain TGT ticket")
39         exit 1
40     fi
41
42     # get service ticket from TGT
43     service_ticket=$(curl ${curl_opts} -X POST ${tgt_location} -d
"service=${base}/")
44
45     if [ -z "${service_ticket}" ]; then
46         (>&2 echo "CAS authentication failed: unable to exchange TGT to service
ticket")
47         exit 1
48     fi
49
50     # write session cookie to file
51     curl $curl_opts --cookie-jar ${cookies} $base/?ticket=$service_ticket
52
53     # print curl auth string to stdout
54     echo "--cookie ${cookies}"
55 }
56
57 function get_custom {
58     record=$1
59     field=$2
60

```

```

61 |     echo $record | jq -r ".custom | fromjson | .${field}"
62 | }
63 |
64 | check_exe curl
65 | check_exe jq
66 |
67 | url="https://pam.company.com/xtam"    # PAM URL
68 | user="admin"    # PAM User
69 | #password="myPassw0rd"    # Optionally define your PAM User's Password
70 |
71 | read -p "Enter $user password: " -s password    # Prompt for PAM User's Password
72 | echo
73 |
74 | auth="-u $user:$password"
75 |
76 | # Your code starts here

```

## Form-Based Authentication

If your login experience to PAM is a form-based login page like the one shown below, then you will use the following to authenticate using our REST APIs.

**Welcome to XTAM**

Copyright Xton Technologies © 2020

```


1 | url="https://pam.company.com/xtam"    # PAM URL
2 | user="admin"    # PAM User
3 | #password="myPassw0rd"    # Optionally define your PAM User's Password
4 |
5 | tc=$(mktemp)
6 | cookies=$(mktemp)
7 | curl -s -X GET -c ${tc} -D - ${base}/rest/user/whoami > /dev/null
8 | curl -s -X POST -b ${tc} -c ${cookies} -D - ${base}/j_security_check -d "j_
  | username=${username}" -d "j_password=${password}" > /dev/null
9 | auth="-b ${cookies}"
10 |
11 | # Your code starts here

```

## Federated Authentication

If your login experience to PAM is a federated sign-in page like the one shown below, then you will use the following to authenticate using our REST APIs.

# Log in to Imprivata Privileged Access Management



**Username:**

**Password:**

[Log in](#)

[? Forgot your password?](#)

For security reasons, please [log out](#) and exit your web browser when you are done accessing services that require authentication!

```
1 | #!/bin/bash
2 |
3 | cookies=$(mktemp)
4 | curl_opts="-s"
5 |
6 | function cleanup {
7 |     rm -f ${cookies}
8 | }
9 |
10 | trap cleanup EXIT
11 |
12 | function check_exe() {
```

```

13   which "$1" >/dev/null 2>&1
14   if [ "$?" -ne 0 ]; then
15       (>&2 echo "Required executable [$1] not found. Please install it using
system package manager.")
16       (>&2 echo "Exiting.")
17       exit 1
18   fi
19 }
20
21 function check_status() {
22     if [ $? != 0 ]; then
23         echo $1
24         exit 1
25     fi
26 }
27
28 function cas_auth {
29     base=${1}
30     cas_base=${2}
31     username=${3}
32     password=${4}
33
34     # get TGT ticket from Location header
35     tgt_location=$(curl ${curl_opts} -X POST -D - ${cas_base}/v1/tickets -d
"username=${username}" -d "password=${password}" | grep "^Location" | cut -d":" -
f 2- | tr -d \\r\\n)
36
37     if [ -z "${tgt_location}" ]; then
38         (>&2 echo "CAS authentication failed: unable to obtain TGT ticket")
39         exit 1
40     fi
41
42     # get service ticket from TGT
43     service_ticket=$(curl ${curl_opts} -X POST ${tgt_location} -d
"service=${base}/")
44
45     if [ -z "${service_ticket}" ]; then
46         (>&2 echo "CAS authentication failed: unable to exchange TGT to service
ticket")
47         exit 1
48     fi
49
50     # write session cookie to file
51     curl $curl_opts --cookie-jar ${cookies} $base/?ticket=$service_ticket
52
53     # print curl auth string to stdout
54     echo "--cookie ${cookies}"
55 }
56
57 function get_custom {
58     record=$1
59     field=$2
60
61     echo $record | jq -r ".custom | fromjson | .${field}"
62 }
63
64 check_exe curl

```

```

65 | check_exe jq
66 |
67 | url="https://pam.company.com/xtam"    # PAM URL
68 | cas_url="https://pam.company.com/cas" # PAM Signin Page URL
69 | user="admin"    # PAM User
70 | #password="myPassw0rd"    # Optionally define your PAM User's Password
71 |
72 | read -p "Enter $user password: " -s password    # Prompt for PAM User's Password
73 | echo
74 |
75 | auth=$(cas_auth $url $cas_url $user $password)
76 |
77 | # Your code starts here

```

## Token Authentication

If you are using Authentication Tokens, then you will use the following to authenticate using our REST APIs.

```

1 | #!/bin/bash
2 |
3 | cookies=$(mktemp)
4 | curl_opts="-s"
5 |
6 | function cleanup {
7 |     rm -f ${cookies}
8 | }
9 |
10 | trap cleanup EXIT
11 |
12 | function check_exe() {
13 |     which "$1" >/dev/null 2>&1
14 |     if [ "$?" -ne 0 ]; then
15 |         (>&2 echo "Required executable [$1] not found. Please install it using
system package manager.")
16 |         (>&2 echo "Exiting.")
17 |         exit 1
18 |     fi
19 | }
20 |
21 | function check_status() {
22 |     if [ $? != 0 ]; then
23 |         echo $1
24 |         exit 1
25 |     fi
26 | }
27 |
28 | function token_auth {
29 |     base=${1}
30 |     cas_base=${2}
31 |     token=${3}
32 |
33 |     # get service ticket from TGT
34 |     hdr=$(curl -si "${cas_base}/login?service=${base}/" -H "token:${token}" |
grep "^Location")

```

```

35     service_ticket=$(echo ${hdr} | cut -d"=" -f 2- | tr -d \\r\\n)
36
37     if [ -z "${service_ticket}" ]; then
38         (>&2 echo "CAS authentication failed: unable to exchange token to
service ticket")
39         exit 1
40     fi
41
42     # write session cookie to file
43     curl $curl_opts --cookie-jar ${cookies} $base/?ticket=$service_ticket
44
45     # print curl auth string to stdout
46     echo "--cookie ${cookies}"
47 }
48
49 function get_custom {
50     record=$1
51     field=$2
52
53     echo $record | jq -r ".custom | fromjson | .${field}"
54 }
55
56 check_exe curl
57 check_exe jq
58
59 url="https://pam.company.com/xtam" # PAM URL
60 cas_url="https://pam.company.com/cas" # PAM Signin Page URL
61 token="yourPAMtoken" # PAM Token
62
63 auth=$(token_auth $url $cas_url $token)
64
65 # Your code starts here

```

## Python

This article provides a small example of Python script calling PAM REST API.

The example access PAM REST API to retrieve current user information and XSRF REST API token.

Then the example demonstrates the functions to access secret data of a specified record and to create a new record in the specified folder.

The article also contains an example of accessing PAM REST API using API authentication token.

PAM

In addition to this detailed guide you can also view the list of other functions you can call using REST API by navigating to Administration > Settings > Application Nodes > API Documentation.

Looking for REST API examples using other scripts? Click [PowerShell examples](#), [Shell examples](#) or [VBScript examples](#) for additional information.

Below is the script demonstrating accessing records secret data and creating a new record. Details of the API calls are outlined in the comments.



Note the use of the XSRF token to call data modification functions. The script intention is to illustrate details of the protocol. As a result, the script does not process network errors leaving it to the implementation.

```
1  # -----
2  # PAM REST API access script example for Python
3  #
4  # The script will demonstrate the following functions
5  #   * to access secret fields of the existing record
6  #   * to create a new record
7  # -----
8
9  import requests
10 import json
11 from http.cookies import SimpleCookie
12
13 # -----
14 # Script parameters define PAM objects used in the script
15 # -----
16
17 # Authentication parameters
18 url = 'https://pam.company.com/xtam' # PAM REST API URL
19 login = 'pam_login'
20 password = 'pam_password'
21
22 # XTAM Object IDs and names used in the script
23 rid = 'i-2qhyGh2UB0V' # Record ID to retrieve
24 fid = 'i-2Zh30SUCq7c' # Folder ID to create a new record in
25 tid = 'i-83XfwpNvCHy' # Record Type ID for the new record creation
26 recordName = 'New Record' # Name for the new record
27 recordDescription = 'New record description' # Description of the new record
28 recordCustom = '{"Host":"host", "Port":24, "User":"user",
29 "Password":"password"}' # Custom data for the new record
30 # -----
31 # Call to /user/whoami function returns current user data.
32 # In addition, this call returns an REST API token for cross site scripting
33 # protection.
34 # -----
35 r = requests.get(url + '/rest/user/whoami', auth=(login, password))
36 user = r.json()
37
38 # Print user information retrieved from the PAM server
39 print('Hello ' + user['firstName'] + ' ' + user['lastName'])
40
41 # Access REST API token for cross-site scripting protection and save it in the
42 # xsrftoken variable
43 cookie = SimpleCookie()
44 cookie.load(r.headers['Set-Cookie'])
```

```

43 | xsrf = cookie['XSRF-TOKEN'].value
44 | #print(xsrf)
45 |
46 | # -----
47 | # Example call /record/unlock to retrieve secret data of a record
48 | # -----
49 | r = requests.get(url + '/rest/record/unlock/' + rid, auth=(login, password))
50 | record = r.json()
51 | custom = json.loads(record['custom'])
52 | print('{0}: {1} ({2}/{3})'.format(record['name'], custom['Host'], custom
53 |   ['User'], custom['Password']))
54 | # -----
55 | # Example call to /record/new to create a new record
56 | # Note that calls that modify PAM data must include REST API token
57 | # -----
58 | resp = requests.post(url + '/rest/record/new/' + fid + '/' + tid,
59 |   data={'name':recordName,'description':recordDescription,
60 |     'custom':recordCustom},
61 |   headers={'Content-Type':'application/x-www-form-urlencoded',
62 |     'Accept':'application/json', 'X-XSRF-TOKEN':xsrf},
63 |   auth=(login, password))
64 | print(resp)
65 | # -----
66 | # Example call to /folder/create to create a new folder to demonstrate json
67 | # Note that calls that modify PAM data must include REST API token
68 | # -----
69 | resp = requests.post(url + '/rest/folder/create/' + fid,
70 |   json={'name':'Py Folder','description':'Py Description'},
71 |   headers={'Content-Type':'application/json', 'Accept':'application/json', 'X-
72 |     XSRF-TOKEN':xsrf},
73 |   auth=(login, password))
74 | print(resp.text)

```

The next example demonstrates the technique of connecting to PAM REST API using API authentication tokens. As before, details of the script use are outlined in the comments.

```

1 | # -----
2 | # PAM REST API access script example for Python
3 | #
4 | # The script will demonstrate API access using API tokens

```

```

5  # -----
6
7  import requests
8  import json
9  from http.cookies import SimpleCookie
10
11 # -----
12 # Script parameters define PAM objects used in the script
13 # -----
14
15 # Authentication parameters
16 url = 'https://pam.company.com/xtam' # PAM URL
17 cas = 'https://pam.company.com/cas' # PAM Federated Sign-In URL
18 token = 'yourPAMtoken' # PAM Token
19
20 # -----
21 # Authentication using the token
22 # -----
23 # Exchange REST API Token for a service ticket in Federated Sign-In Service.
24 # Note that a service ticket is short lived so it should be quickly exchanged to
25 # more permanent session cookie
26 # Also note disabling of redirects to catch service ticket in the Location
27 # header.
28 r = requests.get('{0}/login?service={1}/'.format(cas,url), headers=
29 {'token':token}, allow_redirects=False)
30 location = r.headers['Location']
31
32 # Exchange service ticket for a session cookie in PAM.
33 # Save the session cookie to use in consecutive calls
34 r = requests.get(location, allow_redirects=False)
35 jar = r.cookies
36
37 # -----
38 # Call to /user/whoami function returns current user data.
39 # In addition, this call returns an REST API token for cross site scripting
40 # protection.
41 # -----
42 # Note the use of cookies parameter replacing auth parameter used for basic
43 # authentication
44 r = requests.get(url + '/rest/user/whoami', cookies=jar)
45 user = r.json()
46
47 # Print user information retrieved from the PAM server
48 print('Hello ' + user['firstName'] + ' ' + user['lastName'])
49
50 # Access REST API token for cross-site scripting protection and save it in the
51 # xsrf variable
52 cookie = SimpleCookie()
53 cookie.load(r.headers['Set-Cookie'])
54 xsrf = cookie['XSRF-TOKEN'].value
55 print('XSRF Token: ' + xsrf)

```

Out next example demonstrates the technique of connecting to PAM REST API using user and password when logging in to PAM server with enabled Federated Sign-In (CAS) component.

As before, details of the script use are outlined in the comments.

```
1  # -----
2  # PAM REST API access script example for Python
3  #
4  # The script will demonstrate API access using API tokens
5  # -----
6
7  import requests
8  import json
9  from http.cookies import SimpleCookie
10
11 # -----
12 # Script parameters define PAM objects used in the script
13 # -----
14
15 # Authentication parameters
16 url = 'https://pam.company.com/xtam' # PAM URL
17 cas = 'https://pam.company.com/cas' # PAM Federated Sign-In URL
18 username = 'PAM-user-name' # PAM Account
19 password = 'PAM-user-password' # PAM Account Password
20
21 # -----
22 # Authentication using user / password for Federated Sign-In component
23 # -----
24 # Get TGT ticket granting ticket from user and password.
25 # Note that a TGT ticket is short lived so it should be quickly exchanged to more
26 # permanent session cookie
27 # Also note disabling of redirects to catch service ticket in the Location
28 # header.
29 r = requests.post('{0}/v1/tickets'.format(cas), data=
30 {'username':username,'password':password}, headers={'Content-
31 Type':'application/x-www-form-urlencoded'}, allow_redirects=False)
32 location = r.headers['Location']
33
34 # get service ticket (ST) from TGT.
35 r = requests.post(location, data={'service':'{0}/'.format(url)}, allow_
36 redirects=False)
37 st=r.text
38
39 # Exchange service ticket for a session cookie in PAM.
40 # Save the session cookie to use in consecutive calls
41 r = requests.get('{0}/?ticket={1}'.format(url,st),allow_redirects=False)
42 jar = r.cookies
43
44 # -----
```

```

40 # Call to /user/whoami function returns current user data.
41 # In addition, this call returns an REST API token for cross site scripting
   # protection.
42 # -----
   ----
43 # Note the use of cookies parameter replacing auth parameter used for basic
   # authentication
44 r = requests.get(url + '/rest/user/whoami', cookies=jar)
45 user = r.json()
46
47 # Print user information retrieved from the PAM server
48 print('Hello ' + user['firstName'] + ' ' + user['lastName'])
49
50 # Access REST API token for cross-site scripting protection and save it in the
   # xsrf variable
51 cookie = SimpleCookie()
52 cookie.load(r.headers['Set-Cookie'])
53 xsrf = cookie['XSRF-TOKEN'].value
54 print('XSRF Token: ' + xsrf)

```

## VBScript

Below is a small example of calling PAM API using VBScript.

The majority of this example demonstrates the functions that parse JSon responses from PAM API and encode parameters.

Scroll down to the section “PAM API Example” to learn about the actual REST API call.

In addition to this detailed guide you can also view the list of other functions you can call using REST API by navigating to Administration > Settings > Application Nodes > API Documentation.

Looking for REST API examples using other scripts? Click [PowerShell examples](#), [Shell examples](#) or [Python examples](#) for additional information.

The example first connects to the PAM server and generates a new password for the specified record type (Windows Host). After that, the example uses this password to create a Windows Host record.

The generated password could be used to provision the actual Windows computer or an administrator account.

```

1 Option Explicit
2
3 Dim restReq, base, url, rtid, fid, userName, password, res, json, pwd, custom,
   recordName, description
4 Dim host, port, user
5
6 ' -----

```

```

7  ' PAM Connection Parameters
8  ' -----
9
10 base = "http://localhost:8080/xtam" ' PAM Server URL
11 userName = "pam_user" ' PAM Login
12 password = "pam_password" ' PAM user password
13
14 ' -----
15 ' Object Attributes
16 ' -----
17
18 rtid = "133" ' Record Type ID
19 fid = "1151" ' Folder ID
20 recordName = "Auto-created Record" ' Record name
21 description = "Record for auto-provisioned computer" ' Record description
22 host = "host.company.com" ' Host on record
23 port = "3389" ' Port on record
24 user = "Administrator" ' user on record
25
26 ' -----
27 ' JSON Parser
28 ' -----
29 Class aspJSON
30 Public data
31 Private p_JSONstring
32 private aj_in_string, aj_in_escape, aj_i_tmp, aj_char_tmp, aj_s_tmp, aj_line_tmp,
aj_line, aj_lines, aj_currentlevel, aj_currentkey, aj_currentvalue, aj_newlabel,
aj_XmlHttp, aj_RegExp, aj_colonfound
33
34 Private Sub Class_Initialize()
35     Set data = Collection()
36
37     Set aj_RegExp = new regexp
38     aj_RegExp.Pattern = "\s{0,}(\s{1}[\s,\S]*\s{1})\s{0,}"
39     aj_RegExp.Global = False
40     aj_RegExp.IgnoreCase = True
41     aj_RegExp.Multiline = True
42 End Sub
43
44 Private Sub Class_Terminate()
45     Set data = Nothing
46     Set aj_RegExp = Nothing
47 End Sub
48
49 Public Sub loadJSON(inputsource)
50     inputsource = aj_MultilineTrim(inputsource)
51     If Len(inputsource) = 0 Then Err.Raise 1, "loadJSON Error", "No data to
load."
52
53     select case Left(inputsource, 1)
54     case "{", "["
55     case else
56         Set aj_XmlHttp = CreateObject("Msxml2.ServerXMLHTTP")
57         aj_XmlHttp.open "GET", inputsource, False
58         aj_XmlHttp.setRequestHeader "Content-Type", "text/json"
59         aj_XmlHttp.setRequestHeader "CharSet", "UTF-8"
60         aj_XmlHttp.Send

```

```

61         inputsource = aj_XmlHttp.responseText
62         set aj_XmlHttp = Nothing
63     end select
64
65     p_JSONstring = CleanUpJSONstring(inputsource)
66     aj_lines = Split(p_JSONstring, Chr(13) & Chr(10))
67
68     Dim level(99)
69     aj_currentlevel = 1
70     Set level(aj_currentlevel) = data
71     For Each aj_line In aj_lines
72         aj_currentkey = ""
73         aj_currentvalue = ""
74         If Instr(aj_line, ":") > 0 Then
75             aj_in_string = False
76             aj_in_escape = False
77             aj_colonfound = False
78             For aj_i_tmp = 1 To Len(aj_line)
79                 If aj_in_escape Then
80                     aj_in_escape = False
81                 Else
82                     Select Case Mid(aj_line, aj_i_tmp, 1)
83                         Case ""
84                             aj_in_string = Not aj_in_string
85                         Case ":"
86                             If Not aj_in_escape And Not aj_in_string Then
87                                 aj_currentkey = Left(aj_line, aj_i_tmp - 1)
88                                 aj_currentvalue = Mid(aj_line, aj_i_tmp + 1)
89                                 aj_colonfound = True
90                                 Exit For
91                             End If
92                         Case "\"
93                             aj_in_escape = True
94                     End Select
95                 End If
96             Next
97             if aj_colonfound then
98                 aj_currentkey = aj_Strip(aj_JSONDecode(aj_currentkey), "")
99                 If Not level(aj_currentlevel).exists(aj_currentkey) Then level
100 (aj_currentlevel).Add aj_currentkey, ""
101             end if
102             End If
103             If right(aj_line,1) = "{" Or right(aj_line,1) = "[" Then
104                 If Len(aj_currentkey) = 0 Then aj_currentkey = level(aj_
105 currentlevel).Count
106                 Set level(aj_currentlevel).Item(aj_currentkey) = Collection()
107                 Set level(aj_currentlevel + 1) = level(aj_currentlevel).Item(aj_
108 currentkey)
109                 aj_currentlevel = aj_currentlevel + 1
110                 aj_currentkey = ""
111             ElseIf right(aj_line,1) = "}" Or right(aj_line,1) = "]" or right(aj_
112 line,2) = "}," Or right(aj_line,2) = "]," Then
113                 aj_currentlevel = aj_currentlevel - 1
114             ElseIf Len(Trim(aj_line)) > 0 Then
115                 if Len(aj_currentvalue) = 0 Then aj_currentvalue = aj_line
116                 aj_currentvalue = getJSONValue(aj_currentvalue)
117             End If
118         End For
119     Next
120 End For

```

```

114         If Len(aj_currentkey) = 0 Then aj_currentkey = level(aj_
currentlevel).Count
115         level(aj_currentlevel).Item(aj_currentkey) = aj_currentvalue
116     End If
117 Next
118 End Sub
119
120 Public Function Collection()
121     set Collection = CreateObject("Scripting.Dictionary")
122 End Function
123
124 Public Function AddToCollection(dictobj)
125     if TypeName(dictobj) <> "Dictionary" then Err.Raise 1, "AddToCollection
Error", "Not a collection."
126     aj_newlabel = dictobj.Count
127     dictobj.Add aj_newlabel, Collection()
128     set AddToCollection = dictobj.item(aj_newlabel)
129 end function
130
131 Private Function CleanUpJSONstring(aj_originalstring)
132     aj_originalstring = Replace(aj_originalstring, Chr(13) & Chr(10), "")
133     aj_originalstring = Mid(aj_originalstring, 2, Len(aj_originalstring) - 2)
134     aj_in_string = False : aj_in_escape = False : aj_s_tmp = ""
135     For aj_i_tmp = 1 To Len(aj_originalstring)
136         aj_char_tmp = Mid(aj_originalstring, aj_i_tmp, 1)
137         If aj_in_escape Then
138             aj_in_escape = False
139             aj_s_tmp = aj_s_tmp & aj_char_tmp
140         Else
141             Select Case aj_char_tmp
142             Case "\" : aj_s_tmp = aj_s_tmp & aj_char_tmp : aj_in_escape =
True
143             Case """" : aj_s_tmp = aj_s_tmp & aj_char_tmp : aj_in_string =
Not aj_in_string
144             Case "{", "["
145                 aj_s_tmp = aj_s_tmp & aj_char_tmp & aj_InlineIf(aj_in_string,
"", Chr(13) & Chr(10))
146             Case "}", "]"
147                 aj_s_tmp = aj_s_tmp & aj_InlineIf(aj_in_string, "", Chr(13) &
Chr(10)) & aj_char_tmp
148             Case ",": aj_s_tmp = aj_s_tmp & aj_char_tmp & aj_InlineIf(aj_in_
string, "", Chr(13) & Chr(10))
149             Case Else : aj_s_tmp = aj_s_tmp & aj_char_tmp
150             End Select
151         End If
152     Next
153
154     CleanUpJSONstring = ""
155     aj_s_tmp = split(aj_s_tmp, Chr(13) & Chr(10))
156     For Each aj_line_tmp In aj_s_tmp
157         aj_line_tmp = replace(replace(aj_line_tmp, chr(10), ""), chr(13), "")
158         CleanUpJSONstring = CleanUpJSONstring & aj_Trim(aj_line_tmp) & Chr(13) &
Chr(10)
159     Next
160
161
162

```



```

163     End Function
164
165 Private Function getJSONValue(ByVal val)
166     val = Trim(val)
167     If Left(val,1) = ":" Then val = Mid(val, 2)
168     If Right(val,1) = "," Then val = Left(val, Len(val) - 1)
169     val = Trim(val)
170
171     Select Case val
172     Case "true" : getJSONValue = True
173     Case "false" : getJSONValue = False
174     Case "null" : getJSONValue = Null
175     Case Else
176         If (Instr(val, "''") = 0) Then
177             If IsNumeric(val) Then
178                 getJSONValue = CDBl(val)
179             Else
180                 getJSONValue = val
181             End If
182         Else
183             If Left(val,1) = "''" Then val = Mid(val, 2)
184             If Right(val,1) = "''" Then val = Left(val, Len(val) - 1)
185             getJSONValue = aj_JSONDecode(Trim(val))
186         End If
187     End Select
188 End Function
189
190 Private JSONoutput_level
191 Public Function JSONoutput()
192     dim wrap_dicttype, aj_label
193     JSONoutput_level = 1
194     wrap_dicttype = "[]"
195     For Each aj_label In data
196         If Not aj_IsInt(aj_label) Then wrap_dicttype = "{}"
197     Next
198     JSONoutput = Left(wrap_dicttype, 1) & Chr(13) & Chr(10) & GetDict(data) &
Right(wrap_dicttype, 1)
199 End Function
200
201 Private Function GetDict(objDict)
202     dim aj_item, aj_keyvals, aj_label, aj_dicttype
203     For Each aj_item In objDict
204         Select Case TypeName(objDict.Item(aj_item))
205         Case "Dictionary"
206             GetDict = GetDict & Space(JSONoutput_level * 4)
207
208             aj_dicttype = "[]"
209             For Each aj_label In objDict.Item(aj_item).Keys
210                 If Not aj_IsInt(aj_label) Then aj_dicttype = "{}"
211             Next
212             If aj_IsInt(aj_item) Then
213                 GetDict = GetDict & (Left(aj_dicttype,1) & Chr(13) & Chr(10))
214             Else
215                 GetDict = GetDict & ("'" & aj_JSONEncode(aj_item) & "'" &
": " & Left(aj_dicttype,1) & Chr(13) & Chr(10))
216             End If
217             JSONoutput_level = JSONoutput_level + 1
218

```

```

219         aj_keyvals = objDict.Keys
220         GetDict = GetDict & (GetSubDict(objDict.Item(aj_item)) & Space
(JSONNoutput_level * 4) & Right(aj_dicttype,1) & aj_InlineIf(aj_item = aj_keyvals
(objDict.Count - 1), "" , ",") & Chr(13) & Chr(10))
221     Case Else
222         aj_keyvals = objDict.Keys
223         GetDict = GetDict & (Space(JSONNoutput_level * 4) & aj_InlineIf
(aj_IsInt(aj_item), "", """" & aj_JSONEncode(aj_item) & """: ") & WriteValue
(objDict.Item(aj_item)) & aj_InlineIf(aj_item = aj_keyvals(objDict.Count - 1), ""
, ",") & Chr(13) & Chr(10))
224     End Select
225 Next
226 End Function
227
228 Private Function aj_IsInt(val)
229     aj_IsInt = (TypeName(val) = "Integer" Or TypeName(val) = "Long")
230 End Function
231
232 Private Function GetSubDict(objSubDict)
233     GetSubDict = GetDict(objSubDict)
234     JSONNoutput_level= JSONNoutput_level -1
235 End Function
236
237 Private Function WriteValue(ByVal val)
238     Select Case TypeName(val)
239     Case "Double", "Integer", "Long": WriteValue = val
240     Case "Null" : WriteValue = "null"
241     Case "Boolean" : WriteValue = aj_InlineIf(val, "true",
"false")
242     Case Else : WriteValue = """" & aj_JSONEncode(val)
& """"
243     End Select
244 End Function
245
246 Private Function aj_JSONEncode(ByVal val)
247     val = Replace(val, "\", "\\")
248     val = Replace(val, """, "\"")
249     'val = Replace(val, "/", "\/")
250     val = Replace(val, Chr(8), "\b")
251     val = Replace(val, Chr(12), "\f")
252     val = Replace(val, Chr(10), "\n")
253     val = Replace(val, Chr(13), "\r")
254     val = Replace(val, Chr(9), "\t")
255     aj_JSONEncode = Trim(val)
256 End Function
257
258 Private Function aj_JSONDecode(ByVal val)
259     val = Replace(val, "\"", "")
260     val = Replace(val, "\\", "\")
261     val = Replace(val, "\/", "/")
262     val = Replace(val, "\b", Chr(8))
263     val = Replace(val, "\f", Chr(12))
264     val = Replace(val, "\n", Chr(10))
265     val = Replace(val, "\r", Chr(13))
266     val = Replace(val, "\t", Chr(9))
267     aj_JSONDecode = Trim(val)
268 End Function

```

```

269
270 Private Function aj_InlineIf(condition, returntrue, returnfalse)
271     If condition Then aj_InlineIf = returntrue Else aj_InlineIf = returnfalse
272 End Function
273
274 Private Function aj_Strip(ByVal val, stripper)
275     If Left(val, 1) = stripper Then val = Mid(val, 2)
276     If Right(val, 1) = stripper Then val = Left(val, Len(val) - 1)
277     aj_Strip = val
278 End Function
279
280 Private Function aj_MultilineTrim(TextData)
281     aj_MultilineTrim = aj_RegExp.Replace(TextData, "$1")
282 End Function
283
284 private function aj_Trim(val)
285     aj_Trim = Trim(val)
286     Do While Left(aj_Trim, 1) = Chr(9) : aj_Trim = Mid(aj_Trim, 2) : Loop
287     Do While Right(aj_Trim, 1) = Chr(9) : aj_Trim = Left(aj_Trim, Len(aj_Trim) -
1) : Loop
288     aj_Trim = Trim(aj_Trim)
289 end function
290 End Class
291
292 ' -----
293 ' URL Encoder
294 ' -----
295
296 Public Function URLEncode( StringVal )
297     Dim i, CharCode, Char, Space
298     Dim StringLen
299
300     StringLen = Len(StringVal)
301     ReDim result(StringLen)
302
303     'Space = "+"
304     Space = "%20"
305
306     For i = 1 To StringLen
307         Char = Mid(StringVal, i, 1)
308         CharCode = AscW(Char)
309         If 97 <= CharCode And CharCode <= 122 _
310         Or 64 <= CharCode And CharCode <= 90 _
311         Or 48 <= CharCode And CharCode <= 57 _
312         Or 45 = CharCode _
313         Or 46 = CharCode _
314         Or 95 = CharCode _
315         Or 126 = CharCode Then
316             result(i) = Char
317         ElseIf 32 = CharCode Then
318             result(i) = Space
319         Else
320             result(i) = "%" & Hex(CharCode)
321         End If
322     Next
323     URLEncode = Join(result, "")
324 End Function

```

```

325 |
326 | ' -----
327 | ' XTAM API Example
328 | ' -----
329 |
330 | base = base & "/rest"
331 |
332 | Set restReq = CreateObject("Microsoft.XMLHTTP")
333 |
334 | ' Example simple function call to check the current user name
335 |
336 | restReq.open "GET", base & "/user/whoami", false, userName, password
337 | restReq.send
338 | Set json = new aspJSON
339 | json.loadJSON(restReq.responseText)
340 |
341 | ' Call a function to generate new password based on the password formula assigned
    | for a Windows record type
342 |
343 | restReq.open "GET", base & "/password/generateByType/" & rtid, false, userName,
    | password
344 | restReq.send
345 | res = restReq.responseText
346 |
347 | Set json = new aspJSON
348 | json.loadJSON(res)
349 | pwd = json.data("string")
350 |
351 | ' Generated password is saved in the variable pwd
352 |
353 | ' Call a function to create a new Windows Host record using Administrator as a
    | user name and a generated password as a password on the record
354 |
355 | custom = "{" & ""Host"":"" & host & """, ""Port"":"" & port & """, ""User"":"" &
    | user & """, ""Password"":"" & pwd & ""}"
356 | custom = URLEncode(custom)
357 |
358 | recordName = URLEncode(recordName)
359 | description = URLEncode(description)
360 |
361 | restReq.open "POST", base & "/record/new/1151/" & rtid, false, userName, password
362 | restReq.setRequestHeader "Content-Type", "application/x-www-form-urlencoded"
363 | restReq.setRequestHeader "Accept", "application/json"
364 | restReq.send "name=" & recordName & "&description=" & description & "&custom=" &
    | custom
365 | res = restReq.responseText
366 |
367 | WScript.echo "Record created with generated password. Use variable pwd to reuse
    | the generated password"

```

## Ansible Integration

Integrating PAM's Vault with Ansible.

Ansible is a popular open-source agentless automation tool, or platform, used for IT tasks such as configuration management, application deployment, intra-service orchestration, and provisioning.

Ansible works by connecting to your nodes (such as computers or network devices) and pushing out small programs, called “Ansible modules” to them.

These programs are written to be resource models of the desired state of the system.

Ansible then executes these modules (over SSH by default), and removes them when finished.

To connect to the nodes Ansible needs to know the account credentials such as logins, passwords or keys.

Ansible Vault encrypts credentials right inside Ansible modules and decrypts them when they are needed.

PAM Vault is a server that securely stores and manages (including periodic update) credentials shared between multiple stakeholders in the organization including Ansible to ensure that every Ansible task execution uses the current set of credentials to connect to destination nodes.

There are two ways in which Ansible can use credentials from the PAM Vault: **Connection Brokering** and **Data Lookup**.

## Connection Brokering Integration

In the Connection Brokering scenario Ansible connects to remote nodes using SSH protocol with the traffic passed through the PAM SSH Proxy.

In this scenario Ansible does not retrieve credentials from PAM Vault but instead, relies on the PAM SSH Proxy to broker connections to the destination node using the host and credentials from the PAM Vault.

Ansible authenticates in the PAM Server using the same PAM service account using a public key.

PAM SSH Proxy substitutes the destination host and account credentials in the SSH traffic initiated by the Ansible tasks.

In this Connection Brokering scenario Ansible does not manage credentials to the destination nodes.

Instead, Ansible only knows how to connect to the PAM Server using SSH protocol with the private key to facilitate automation.

Please review the [article](#) about setting up a user in the PAM SSH Server with public key authentication.

After the private key connection to the PAM Server is established, Ansible should reference all nodes under management using the PAM SSH server host.

Ansible should reference accounts in the form **xtam-user%record-id** where *xtam-user* is an PAM service user with the public key SSH authentication enabled and *record-id* is the PAM record ID describing the remote node managed by Ansible.

Note that Ansible first uploads small pieces of code to the temporary folder on the destination computer. Sometimes the default place is in the current user home folder. The problem with that is that Ansible assumes that the home folder name matches the user name Ansible connects to the destinations server instead of deriving the home folder from the destination system environment (*whoami* would work better instead but default Ansible scripts do not use that). In reality there is no such user or such folder in the destination system because PAM substitutes the actual user credentials in the Ansible traffic to the real privileged account.

There are multiple ways to solve this problem. One of those is to make Ansible to maintain temporary files in the `/tmp` folder on the destination server to detach it from the user name Ansible thinks it uses to connect. To do that use a system environment variable

```
export ANSIBLE_REMOTE_TMP=/tmp
```

...or alternatively define Ansible variable

```
remote_tmp = /tmp/ansible
```

Also note that default Ansible configuration makes ssh to cache connections for some time to avoid making multiple consecutive connections. PAM manages the destination connection itself, so Ansible reusing client connections to PAM is not useful to access session completed previously on the PAM server. It makes every other command to fail to retrieve any data from the destination server because PAM is the entity managing connections and Ansible cached connections would not work.

To solve this issue, disable cached connections by Ansible by using the following environments variable although this operation could be probably done in many other ways in ssh, template, playbook or project level.

```
export ANSIBLE_SSH_ARGS="-o ControlMaster=no"
```

## Data Lookup Integration

In a Data Lookup scenario Ansible retrieves sensitive information from PAM Vault when needed using the Ansible PAM Lookup Plugin.

The Ansible PAM Lookup Plugin could be used in any place where Ansible can use lookups.

The plugin can retrieve any sensitive field from the PAM records to use in Ansible variables, rules or playbooks instead of hard coding this data in Ansible variables.

To enable data lookup integration, first download the Ansible PAM Lookup Plugin using the link below and then deploy it according to Ansible documentation in project-, user-, or global- scope.

Ansible PAM Lookup Plugin: <https://www.xtontech.com/wp-content/uploads/files/xtam.py>

The *Ansible PAM Lookup Plugin* uses the following environment variables to connect to the PAM Server

- **ANS\_XTAM\_URL** is the PAM server URL in the form of <https://xtam.company.com>. Note that the plugin in this case expects PAM to respond on the URL <https://xtam.company.com/xtam> and for Federated Sign-In on the URL <https://xtam.company.com/cas>. However, this parameter should only specify the URL without `/xtam/` or `/cas/` paths. In case of custom port use the URL in the form <https://xtam.company.com:port>
- **ANS\_XTAM\_LOGIN** – PAM service account for Ansible to access the vault for PAM Basic Authentication scenario. Note that this account has to have Record Control: Unlock permissions or higher for the records of interest.
- **ANS\_XTAM\_PASSWORD** – PAM service account password
- **ANS\_XTAM\_TOKEN** as an alternative to using **ANS\_XTAM\_LOGIN** and **ANS\_XTAM\_PASSWORD** for a Federated Sign-In scenario. Use the following link describing [Authentication Tokens configuration and their use](#).

Note that for newer Mac OS computers, per Ansible guidelines, you have also have to set the following environment variable:

**OBJC\_DISABLE\_INITIALIZE\_FORK\_SAFETY=YES**

After Ansible PAM connectivity for the Data Lookup Plugin is configured, PAM lookups could be used in any place Ansible allows lookups using the following syntax:

```
1 | lookup('xtam', 'RECORD-ID FIELD-NAME')
```

Where:

- **RECORD-ID** is the PAM record ID describing the remote node asset
- **FIELD-NAME** is the field name to return by this lookup (such as User, Password or any other out of the box or custom fields in the PAM record)

For example, below is the group variables definition for certain group scan retrieving the user and password data from PAM Vault record **i-4bbAmkj4QYq**:

```
1 | ansible_user: "{{lookup('xtam', 'i-4bbAmkj4QYq User')}}"
2 | ansible_password: "{{lookup('xtam', 'i-4bbAmkj4QYq Password')}}"
```

## Best Practices

### Using the API with Cross-Site Scripting Protection

This error (API token verification error) means that from the authentication perspective everything is fine.

For example, you can get any information from PAM at this point.

However, to use POST and PUT to create or change something, there is another level of protection from cross-site scripting attacks which is completely unrelated to authentication tokens.

The carrier of this protection is also called a token, (*API Token* or *XSRF Token*) but has nothing to do with authentication tokens that are referenced [here](#).

To get this token you need to call `/rest/user/whoami` function – which is a GET function, meaning you do not require an API Token to call this function (you still need Authentication Token and Auth Cookie).

It is the only function that generates an API token and returns it in the `XSRF-TOKEN` cookie (Set-Cookie response header).

Below is the link with the example of how to get this [XSRF-TOKEN](#):

[#api\\_token](#)

You need to pass a value of this **XSRF-TOKEN** as a **X-XSRF-TOKEN** header when POST or PUT anything.

Below is the link with the example how to send this API Token as a header (scroll to create record section).

Note that this example does not include how to retrieve the API token referenced previously. (This is because you need to get it for every function or get it in the beginning for all functions. For this reason, me moved the explanation to the bottom of this page as a separate example as to not bog down the [API examples](#).)

XSRF-TOKENS are relatively short lived so there is no point to save them – call **whoami** every time in the script.

The PAM GUI itself calls this function in the beginning. Therefore, you can log into PAM, open dev console, navigate to the network tab and refresh the page. You can then find the call to **whoami** to see the results it returns.

Something like update a record will use this token as a header which is also visible on the browser's dev console.

## Using the API with Federated Sign-in Module

To use the PAM APIs with the [Federated Sign-in Module](#) enabled please follow the procedure described in the Secure Authentication / Federated Authentication using [this API guide](#).

There is a **cas\_auth** function in the script example including the function itself and the example of its use.

For the token-based authentication for scripts (so to use it without user and password) look for the **token\_auth** function on the same page.

In short, the flow is that the script takes *user/password* or a *token* and exchanges it for ticket-granting-ticket (TGT) in the [Federated Sign-in Module](#) returned in the **Location** header.

Then it posts to this location exchanging a ticket-granting-ticket to a service ticket (ST).

Then it uses PAM to exchange Service Ticket for a cookie (JSESSION) that it can use for all subsequent REST API calls.

Tickets are short-lived, whereas cookies are not. It is a standard practice for the headless federated sign in and is outlined in the **cas\_auth/token\_auth** examples.

## Using the API with MFA Enabled

When MFA is enabled for the account PAM will not allow this account to call REST APIs.



The way to proceed in this situation is to use an account or a token generated for an account which does not require MFA authentication while all other accounts that login using GUI do [require MFA](#).

Please look at the article about [enabling granular control over MFA configuration for different users or groups of users](#).

Add an account that will be used for API access with none as a provider.

You might want to create a special service *Local Account* for this and grant it certain permissions or use the one that you used before.

Just keep in mind that this account will not be prompted for MFA token.

## Customization of Federated Sign-In Page text

When the PAM Administrator switching to use Federated Sign-in, Log in page text can be customized. The configuration files for the text modification are contained in the `pam-cas.zip` files.

The text shown on the Federated Sign-in page is updated whenever this file is redeployed.

The Federated Sign-in page text can be customized by editing the appropriate data in these files `custom_messages.properties` and `messages.properties`

### Page Title

In `$PAM_HOME/pam/web/webapps/cas/WEB-INF/classes/custom_messages.properties` file locate **`cas.login.pagetitle=`**

Default:

```
1 | cas.login.pagetitle=Log in to Imprivata Privileged Access Management
```

# Log in to Imprivata Privileged Access Management



**Username:**

**Password:**

Log in

[? Forgot your password?](#)

For security reasons, please [log out](#) and exit your web browser when you are done accessing services that require authentication!

Copyright (c) 2022, Imprivata, Inc.

## Bottom Security message

In `$PAM_HOME/pam/web/webapps/cas/WEB-INF/classes/messages.properties` file locate

`screen.welcome.security=`

Default:

```
1 | screen.welcome.security=For security reasons, please <a href="logout">log out</a>
  | and exit your web browser when you are done accessing \ services that require
  | authentication!
```

Note: During regular PAM's version update the text in these files may be also updated. Be sure to backup/record any changes you have made before update, so custom changes can be reconfigured as needed.

## Export your Data from PAM

PAM provides an export option so that your database (configuration, settings, logs and records) can be safely stored for security, import and [“break glass” procedures](#).

The export option can be performed automatically (encrypted) or on-demand (encrypted or decrypted).

If the export is performed with encryption (our recommendation), then your PAM [Master Password](#) will be required in order to decrypt the secured data.

## Automatically

### To export your PAM Database Automatically:

1. Login to PAM using a System Administrator account.
2. Navigate to Administration > Settings > **Parameters**.
3. Enter or accept the default location in the **Export Location** field to define the export storage location. Use \$PAM\_HOME to define the PAM installation location. Click the **Save** button to its right to save your change.
4. Enter a value (measured in minutes) into the **Export Schedule** field. This value will be the number of minutes between automated exports (enter a zero value to disable the automated export). Click the **Save** button to its right to save your change.
5. An event (Category: *Application*; Level: *Info*; Event: *Export*) will be created in the *Audit Log* when the export is complete.
6. The export is now saved to your Export Location in a archived `zip` format, possibly multi-part if the export is large. The naming convention is:

**xtamexp-YYYYMMDDHHMMSS-{EventID}-{multipart}.zip**

The first export will be immediately added to the PAM queue. Subsequent exports will take place in intervals based on the value entered into the Export Schedule parameter.

All automated exports will be executed with encryption.

## On-Demand

### To export your PAM Database On-Demand:

1. Login to PAM using a System Administrator account.
2. Navigate to Administration > Settings > **Parameters**.

3. Enter or accept the default location in the **Export Location** field to define the export storage location. Use \$PAM\_HOME to define the PAM installation location. Click the **Save** button to its right to save your change.
4. Navigate to Administration > Settings > Database.
5. Click the **Export Encrypted** or **Export Decrypted** button to queue the Export procedure.
6. An event (Category: *Application*; Level: *Info*; Event: *Export*) will be created in the *Audit Log* when the export is complete.
7. The export is now saved to your Export Location in a archived `zip` format, possibly multi-part if the export is large. The naming convention is:

**xtamexp-YYYYMMDDHHMMSS-{EventID}-{multipart}.zip**

The export will be immediately added to the PAM queue and will be performed a single time. If the export includes encryption (*recommended*), the PAM Master Password will be required to access its secured data; however if it is exported decrypted (*not recommended*), then the secured data can be accessed without requiring any passwords.

## System Export Retention

All system exports are stored indefinitely, however if you would like to implement a retention schedule for your exports (includes both Scheduled and On-Demand exports) then please configure the option described below.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Parameters > System Export Retention.
3. Enter a value (defined in Days). PAM will delete all system export files after this specified number of days. A value of 0 (zero) will disable the retention schedule.
4. Click the **Save** button next to this option.

Please note that this retention schedule is applied *Globally* for all system exports and exports that have been purged due to this schedule cannot be recovered.

## Import Data into PAM from Exported File

Importing your data to PAM from a previously created [Export](#) provides a System Administrator with the ability to recover from a lose of data or to rebuild a PAM deployment on a new host.

Some common use cases include:

- disaster recovery;
- data loss recovery;
- populating a test or UAT environment with data;
- switching to a different PAM database.

And as with all things, the following items must be considered when performing an import:

- This procedure is similar to a database import, meaning **all** data currently in PAM will be replaced with that from the import. The process will remove all data currently in PAM and import only what is contained in the export.
- If the import is using an [encrypted export](#) (*which we recommend*), then you will need to know the Master Password if importing to a new system.

- The PAM instance that will be importing must be equal or newer in version number to the PAM instance that created the export.

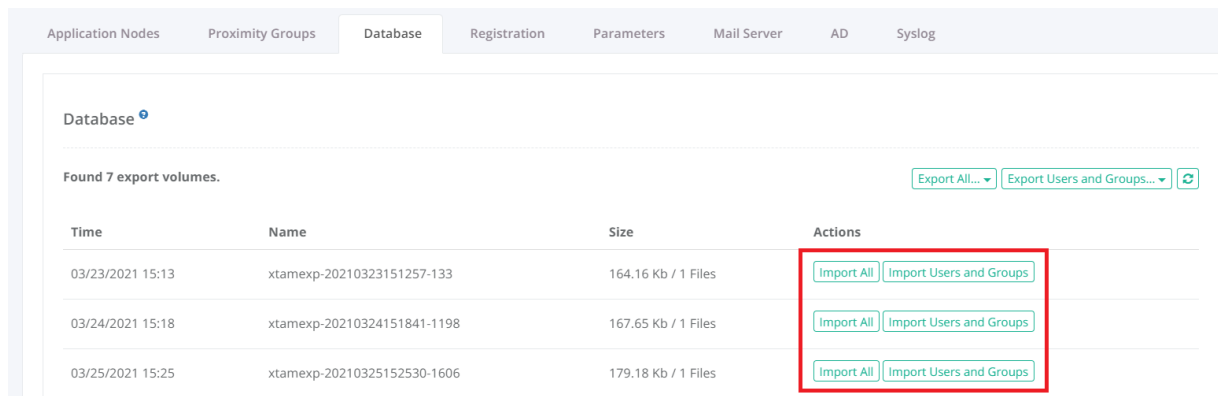
## Import back into the same PAM deployment

### How to Import back into the same PAM deployment using an Encrypted or Decrypted Export.

This procedure details the steps required to import data back into the same PAM system that created the export.

This procedure supports the use of encrypted or decrypted export files.

1. Login to PAM as a System Administrator.
2. Navigate to Administration > Settings > Database.
3. In the table list of available exported volumes, locate the one you wish to use and click the **Import** button to its right.



4. The Import operation will now be added to the PAM queue and will be executed shortly. Once the import begins, completion time depends on the amount of data that needs to be imported and may take several minutes to finish.

During the import process, the application's GUI may become temporarily unavailable. To check the status of the operation, you should open the PAM log file located at `$PAM_HOME/web/logs/pam.log` and when the message *Importing Complete* appears, the operation is finished.

5. Refresh the *All Records* page to review the imported data.

## Import into a new deployment with Encrypted Export

### How to Import into a new PAM deployment using an Encrypted Export.

This procedure details the steps required to import data into a new PAM system; one that did not create the export.

This procedure supports the use of encrypted export files.

1. Install a new PAM system where and as needed.
2. Once the installation is complete, open a command line on this new host server, navigate to the folder where PAM is installed (`$PAM_HOME`) and issue the following command to update your current PAM Master Password with the one that was used to create your encrypted export.

- a. For Windows, substitute **<MASTER PASSWORD>** with the master password used with your export and issue:

```
1 | bin\PamDirectory.cmd SetMasterPassword web <MASTER PASSWORD>
```

- b. For Unix or Linux, substitute **<MASTER PASSWORD>** with the master password used with your export and issue:

```
1 | bin/PamDirectory.sh SetMasterPassword web <MASTER PASSWORD>
```

3. Copy your exported file(s) to your new PAM system and paste them into `$PAM_HOME/export/` or the custom location you defined in Administration > Settings > Parameters > Export Location.
4. Login to PAM as a System Administrator.
5. Navigate to Administration > Settings > Database.
6. In the table list of available exported volumes, locate the one you wish to use and click the **Import** button to its right.

Application NodesProximity GroupsDatabaseRegistrationParametersMail ServerADSyslog

Database

Found 7 export volumes.

Export All...Export Users and Groups...🔄

Time	Name	Size	Actions
03/23/2021 15:13	xtamexp-20210323151257-133	164.16 Kb / 1 Files	<div>Import AllImport Users and Groups</div>
03/24/2021 15:18	xtamexp-20210324151841-1198	167.65 Kb / 1 Files	<div>Import AllImport Users and Groups</div>
03/25/2021 15:25	xtamexp-20210325152530-1606	179.18 Kb / 1 Files	<div>Import AllImport Users and Groups</div>

7. The Import operation will now be added to the PAM queue and will be executed shortly. Once the import begins, completion time depends on the amount of data that needs to be imported and may take several minutes to finish.

During the import process, the application's GUI may become temporarily unavailable. To check the status of the operation, you should open the PAM log file located at `$PAM_HOME/web/logs/pam.log` and when the message *Importing Complete* appears, the operation is finished.

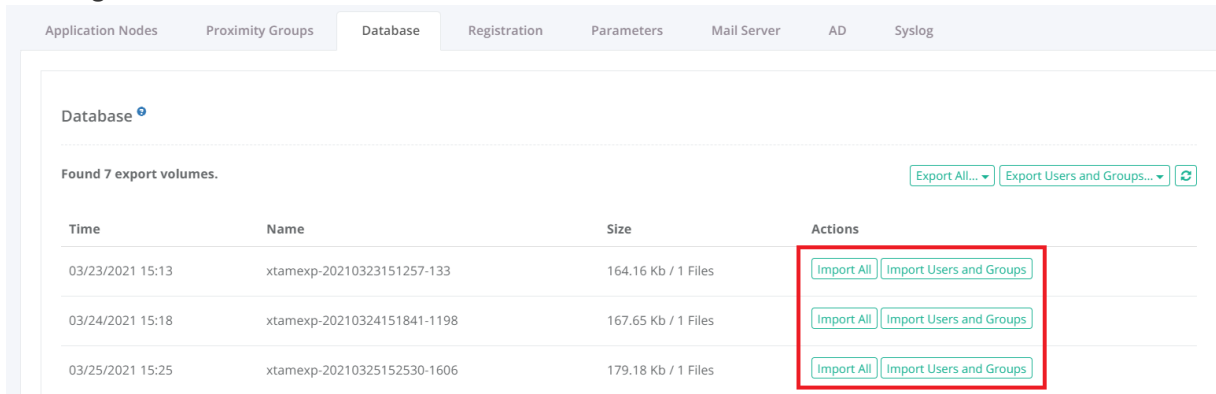
8. Refresh the *All Records* page to review the imported data.

## Import into a new deployment with Decrypted Export

### How to Import into a new PAM deployment using an Decrypted Export.

This procedure details the steps required to import data into a new PAM system; one that did not create the export. This procedure supports the use of decrypted export files.

1. Install a new PAM system where and as needed.
2. Copy your exported file(s) to your new PAM system and paste them into `$PAM_HOME/export/` or the custom location you defined in Administration > Settings > Parameters > Export Location.
3. Login to PAM as a System Administrator.
4. Navigate to Administration > Settings > Database.
5. In the table list of available exported volumes, locate the one you wish to use and click the Import button to its right.



6. The Import operation will now be added to the PAM queue and will be executed shortly. Once the import begins, completion time depends on the amount of data that needs to be imported and may take several minutes to finish.

During the import process, the application's GUI may become temporarily unavailable. To check the status of the operation, you should open the PAM log file located at `$PAM_HOME/web/logs/pam.log` and when the message *Importing Complete* appears, the operation is finished.

7. Refresh the *All Records* page to review the imported data.

## Java 8 to OpenJDK 11 Migration

Migrating the PAM Framework from Java 8 to OpenJDK 11.

Upgrading to the latest version of PAM provides you with enhanced security, improved performance, and access to all the newest features and enhancements we offer. To fully benefit from these improvements and ensure optimal compatibility, we encourage you to update your Java environment to at least the minimum supported version.

PAM now utilizes third-party libraries that are built on Java 9 or above. Without upgrading to OpenJDK 11, these new dependencies won't be properly supported. Upgrading PAM without updating your Java version can lead to system instability and negatively impact your experience. To ensure seamless functionality and avoid any disruptions, it's important to prioritize these changes.

If you want to migrate from PAM's default Java 8 deployment to OpenJDK 11 or to the latest Java 8 build, please read the following article.

## Prerequisites

- An operational PAM deployment with the latest version. Please update to the latest available version before proceeding.

## Considerations

- Each PAM node that is updated will be offline and inaccessible for the entirety of the migration.
- The user performing the migration will be required to update files and configurations on the PAM host server. Administrative privileges are required.
- We highly recommend deploying a test instance of PAM that mirrors your production instance as closely as possible to test the migration (DB type, [Federated Sign-In](#), [certificates](#), MFA/SSO, [AD Integration](#), etc). Once the migration is successful with the test instance you can reproduce the procedure on your production instance.

Please read the entire procedure outlined in the article before beginning. If you have any questions, please contact our Support team: <https://support.imprivata.com/communitylogin>.

### [Step 1. Download Migration Components](#)

### [Step 2. Stop the PAM Services](#)

### [Step 3. JRE to OpenJDK Migration](#)

### [Step 4. Start the PAM Services](#)

### [Step 5. Test and Verify](#)

### [Rollback](#)

### [Step 6. Cleanup](#)

## Step 1. Download Migration Components

1. Download the latest version of the OpenJDK 11 archive using the AdoptOpenJDK link below to your PAM host server (Windows or Linux) and extract the archive to your \$PAM\_HOME directory. The extracted archive will create a new directory with a name resembling `$PAM_HOME/jdk-11.x.x`.
  - <https://adoptopenjdk.net/releases.html>
2. Download the OpenJDK 11 compatible PAM Federated Sign-in Module from the below location. Once downloaded, extract this zip to a temporary location on the PAM host server. Do not extract this archive to \$PAM\_HOME. *Please note that if you are not using the Federated Sign-in Module, then you can skip this step.*
  - Download the latest supported Federated Sign-in Module for PAM to your PAM host server and extract the archive <https://bin.xtontech.com/product/pam-cas.zip> for legacy version 5.2 or <https://bin.xtontech.com/product/pam-cas.65.zip> (recommended) for product version 6.5.
3. Download the [PAM JDK Update Pack](#) to your PAM host server (Windows and Linux) and extract the archive to your \$PAM\_HOME directory. The extracted archive will create a new directory with the name `$PAM_HOME/pam-jdk11-pack`.

## Step 2. Stop the PAM Services

Once the services are stopped, PAM will become inaccessible until the entire migration is completed.



1. For Windows deployments, stop the **PamManagement** and **PamDirectory** services:

```
1 | net stop PamManagement
```

```
1 | net stop PamDirectory
```

2. For Linux deployments, stop the **pammanager** and **pamdirectory** services:

```
1 | service pammanager stop
```

```
1 | service pamdirectory stop
```

## Step 3. JRE to OpenJDK Migration

1. Replace the existing PAM **jre** directory.

- Rename `$PAM_HOME/jre` to `$PAM_HOME/jre.8`
- Rename `$PAM_HOME/jdk-11.x.x` to `$PAM_HOME/jre`

2. Copy JRE 8 Certificates and Configurations:

- Copy the file `$PAM_HOME/jre.8/lib/security/cacerts` to `$PAM_HOME/jre/lib/security` overwriting the current file.

Note: This step will migrate the existing certificates loaded into the previous PAM deployment including ADS, AD connection certificates as well as SSL certificate for CAS integration.

3. Update PAM container files.

- Copy all files from `$PAM_HOME/pam-jdk11-pack/bin` to `$PAM_HOME/bin` overwriting the current files.
- (Linux only) Copy all files from `$PAM_HOME/pam-jdk11-pack/web/bin` to `$PAM_HOME/web/bin`

Note: This step resolves two issues with the compatibility between Java versions: deprecated endorsed folder and endpoint identity verification for LDAPS integrations.

4. (Windows only) Redeploy Service:

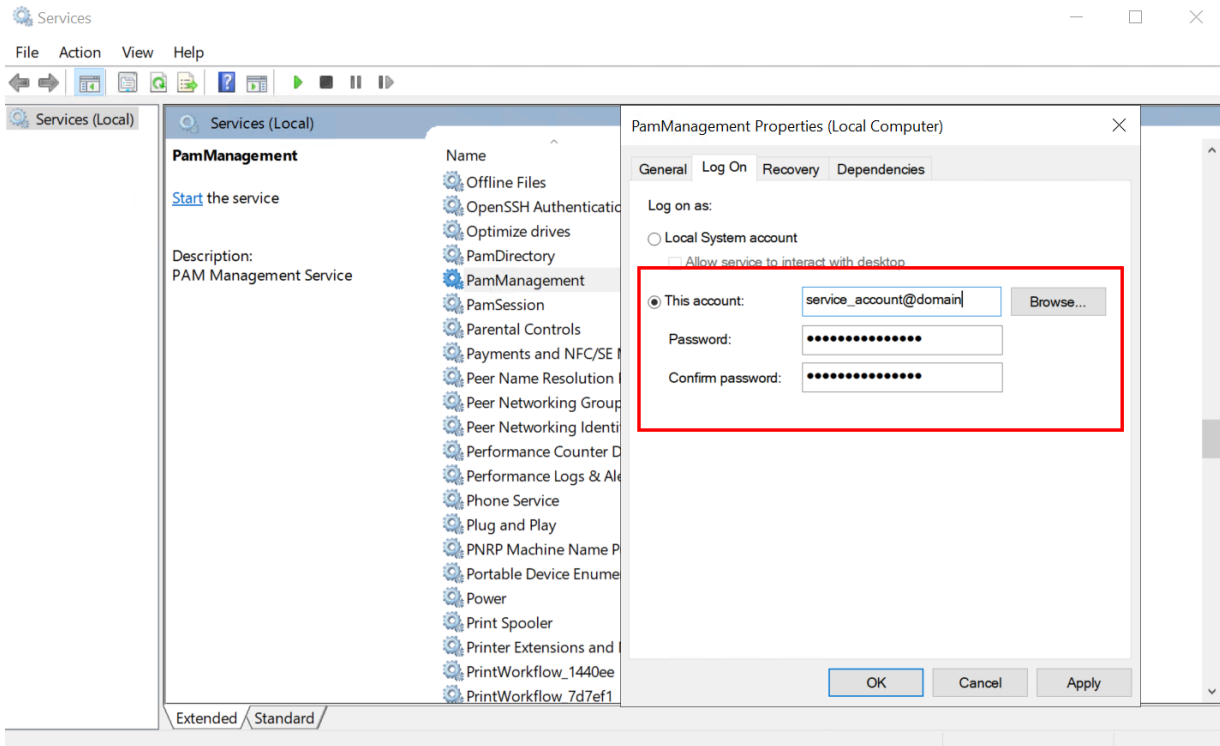
- From an administrative command prompt, navigate to `$PAM_HOME` and run the command:

```
1 | bin\ServiceManagement.cmd remove
```

- When the above command completes successfully, run the command:

```
1 | bin\ServiceManagement.cmd install
```

Note: The **PamManagement** service resets to the default *Local System account* Log on property once this service for PAM is reinstalled. If you are using a Log account other than an Local System account for this service then you must restore it prior to restarting the **PamManagement** service. Navigate to *Services* on Windows and find *PamManagement*, right-click and select **Properties**. Go to the *Log on* tab, select *This account:* and restore the required service account.



5. Redeploy the Federated Sign-In Module. If you are not using the Federated Sign-in Module, you can skip this step.

- Move `$PAM_HOME/web/webapps/cas` to `$PAM_HOME`
- Move `$PAM_HOME/web/webapps/cas.war` to `$PAM_HOME`
- Copy the downloaded cas.war from step (1b) to `$PAM_HOME/web/webapps`

Note: If you made any customizations to the Federated Sign-in Module, they may be lost and need to be redone after the migration is complete.

6. Update External Database Dependencies. If you are using the Internal PAM database, then this step can be skipped.

- Navigate to `$PAM_HOME/web/webapps/xtam/WEB-INF/lib`
- Select and copy all the files that start with jaxb- and are of extension `.jar` (i.e. `jaxb-*.jar`) to `$PAM_HOME/web/lib`

## Step 4. Start the PAM Services

1. For Windows deployments, start the **PamManagement** and **PamDirectory** services:

```
1 | net start PamManagement
```

•

```
1 | net start PamDirectory
```

•

2. For Linux deployments, start the **pammanager** and **pamdirectory** services:

```
1 | service pammanager start
```

```
1 | service pamdirectory start
```

## Step 5. Test and Verify

Once the services come back online, you should now login and thoroughly test the system. This should include, but not be limited to:

- Login with all applicable types of user accounts; Local, AD/LDAP, MFA and SSO.
- Accessing existing records (and creating new records) in both the Record List and Personal Vault, including the unlock action.
- Creating remote sessions.
- Executing jobs and tasks (on demand and scheduled).
- Viewing and exporting reports.

To confirm the migration, open the file `$PAM_HOME/web/logs/catalina.currentDate.log` and search for **JVM Version:**.

The displayed version should be **11.0.2+9** or the latest version that was downloaded.

## Rollback

If the migration or testing fails and you need to rollback to the previous Java 8 framework, then follow this procedure. If you do not need to rollback, proceed to the next section.

1. Stop the PAM services as described earlier
2. Rename the new `$PAM_HOME/jre` to `$PAM_HOME/jre.11`
3. Rename the previous `$PAM_HOME/jre.8` back to `$PAM_HOME/jre`
4. Delete the new `$PAM_HOME/web/webapps/cas`
5. Delete the new `$PAM_HOME/web/webapps/cas.war`
6. Move the previous `$PAM_HOME/cas` back to `$PAM_HOME/web/webapps/cas`
7. Move the previous `$PAM_HOME/web/webapps/cas.war` back to `$PAM_HOME/web/webapps/cas.war`
8. Start the PAM services as described earlier.

When the services come back online, PAM should be using the previous framework.

## Step 6. Cleanup

After all the testing is complete and the system is fully operational, you may remove the following directories:

- `$PAM_HOME/jre.8`
- `$PAM_HOME/pam-jdk11-pack`
- `$PAM_HOME/cas`
- `$PAM_HOME/cas.war`

## FAQs

We understand that upcoming changes to our PAM solution may raise questions, and we want to ensure you have all the information you need. This section is designed to help you better understand the enhancements we're making, how they benefit you, and what steps you might need to take. By providing clear answers to common questions, we aim to make the transition as smooth as possible and have representation about 'Why These Changes Are Better for Our Customers'. We encourage you to read through these FAQs, and as always, feel free to reach out to us if you have any further inquiries. If questions remain or issues arise while using PAM, please contact the Support team: <https://support.imprivata.com/communitylogin>.

**Question:** *What are the high-level benefits we will gain from the upgrade?*

**Answer:** Upgrading to the latest version of PAM provides you with enhanced security, improved performance, and access to all the newest features and enhancements we offer. To fully benefit from these improvements and ensure optimal compatibility, we encourage you to update your Java environment to at least the minimum supported version.

**Question:** *What could happen if I don't update to OpenJDK 11 by the required date?*

**Answer:** PAM now utilizes third-party libraries that are built on Java 9 or above. Without upgrading to OpenJDK 11, these new dependencies won't be properly supported. Upgrading PAM without updating your Java version can lead to system instability and negatively impact your experience. To ensure seamless functionality and avoid any disruptions, it's important to prioritize these changes.

## Updating Original PAM Deployment to Latest Framework and WEB Container

This guide is designed for original PAM deployments that wish to update to the latest Framework and WEB Container components.

To verify if this guide is applicable to your PAM deployment, navigate to Management > About and check both the **Framework** and **WEB Container** versions.

If the Framework version begins with 1.8x and the WEB Container begins with 8.0.x, then this guide can be used to update your PAM deployment to the latest supported versions.

If the Framework version begins with 11.x or higher, then please use this [guide to update the Framework](#).

If the WEB Container version begins with 9.0.x, then please use this [guide to update the WEB Container](#).

## Prerequisites

- An operational PAM deployment with the latest version. Please update to the latest available version before proceeding.

## Considerations

- Each PAM node that is updated will be offline and inaccessible for the entirety of the migration.
- The user performing the migration will be required to update files and configurations on the PAM host server. Appropriate privileges are required.
- We highly recommend deploying a test instance of PAM that mirrors your production instance as closely as possible to test the migration (DB type, Federated Sign-In, certificates, MFA/SSO, AD Integration, etc). Once the migration is successful with the test instance you can reproduce the procedure on your production instance.

Please read the entire procedure outlined in the article before beginning. If you have any questions, please contact the Support team: <https://support.imprivata.com/communitylogin>.

## Step 1. Download Migration Components

1. Download the latest framework packaged for PAM Server using the appropriate links below to your PAM host server and extract archive outside the `$PAM` directory.
  - **Windows:** <https://bin.xtontech.com/product/pam-framework.zip>
  - **Linux:** <https://bin.xtontech.com/product/pam-framework.tgz>
  - **Linux ARM:** <https://bin.xtontech.com/product/pam-framework.aarch64.tgz>
2. Download the latest WEB Container packaged for PAM Server to your PAM host server and extract archive outside the `$PAM_HOME` directory.
  - Windows and Linux: <https://bin.xtontech.com/product/pam-web.zip>
3. Download the OpenJDK 11+ compatible PAM Federated Sign-in Module from the below location. *Please note that if you are not using the Federated Sign-in Module, then you can skip this step.*
  - [Federated Sign-in Module](#)
  - [Federated Sign-in Module for RADIUS](#)
4. Download the [JDK Update Pack](#) to your PAM host server (Windows and Linux) and extract the archive to your `$PAM_HOME` directory. The extracted archive will create a new directory with the name `$PAM_HOME/pam-jdk13-pack`.

## Step 2. Stop the PAM Services

Once the services are stopped, PAM will become inaccessible until the entire migration is completed.

1. For Windows deployments, stop the **PamManagement** and **PamDirectory** services:

```
1 | net stop PamManagement
```

```
1 | net stop PamDirectory
```

1. For Linux deployments, stop the **pammanager** and **pamdirectory** services:

```
1 | service pammanager stop
```

```
1 | service pamdirectory stop
```

## Step 3. Updating Framework and WEB Container Version

1. Replace the existing PAM jre directory.
  - Rename `$PAM_HOME/jre` to `$PAM_HOME/jre.old` folder
  - Move `jre` directory downloaded in the Step 1a to `$PAM_HOME/jre`
2. Copy existing PAM Certificates and Configurations:
  - Copy the file `$PAM_HOME/jre.old/lib/security/cacerts` to `$PAM_HOME/jre/lib/security` overwriting the current file.

Note: This step will migrate the existing certificates loaded into the previous PAM deployment including ADS, AD connection certificates as well as SSL certificate for CAS integration.

3. Update WEB Container:
  - Copy existing `$PAM_HOME/web` directory to the `$PAM_HOME/web.old` to create a backup.
  - Copy all files from the directory `web/bin` downloaded in the Step 1b to `$PAM_HOME/web/bin`,
  - Copy all files from the directory `web/lib` downloaded in the Step 1b to `$PAM_HOME/web/lib`.
4. Update PAM container files. *This step should be performed for existing deployments that were done before March, 2019. All deployments performed after March, 2019 already include modifications in these files.*
  - Copy all files from `$PAM_HOME/pam-jdk13-pack/bin` to `$PAM_HOME/bin` overwriting the current files.

Note: This step resolves two issues with the compatibility between Java versions: deprecated endorsed folder and endpoint identity verification for LDAPS integrations.

5. (Windows only) Redeploy Service. *This step should be performed for existing deployments that were done before March, 2019. All deployments performed after March, 2019 already include these modifications.*

- From an administrative command prompt, navigate to `$PAM_HOME` and run the command:

```
1 | bin\ServiceManagement.cmd remove
```

- When the above command completes successfully, run the command:

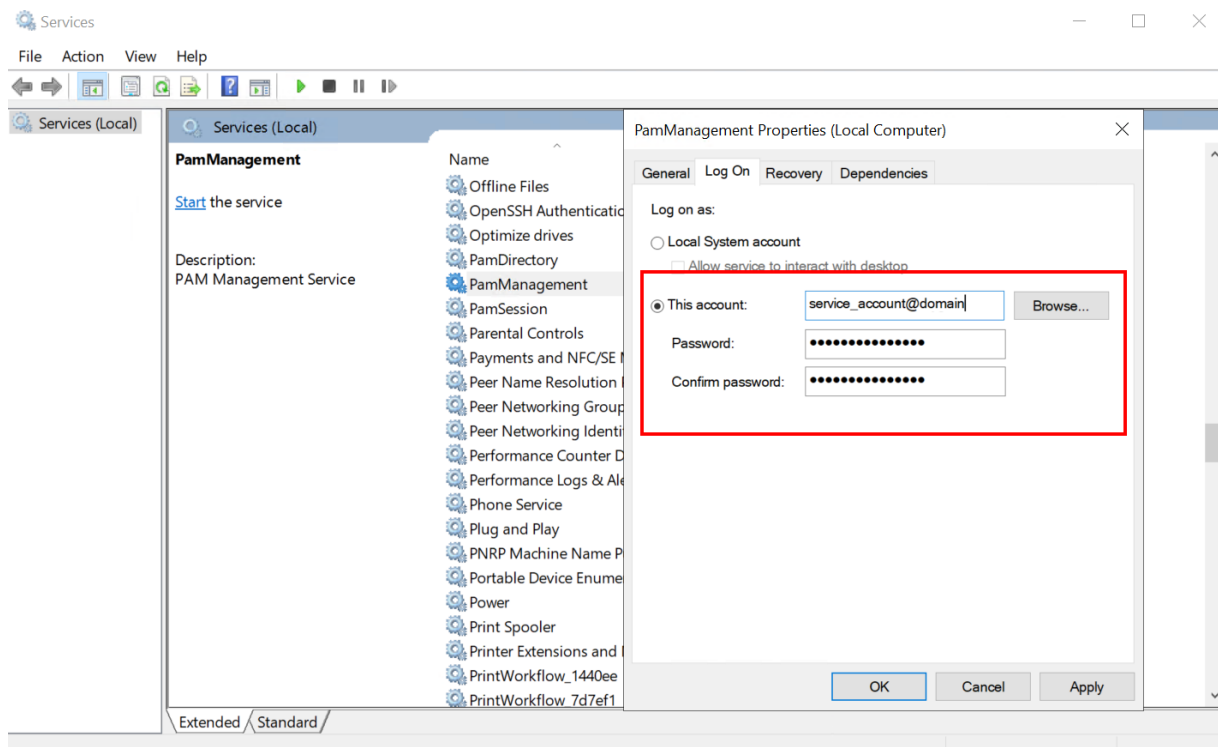
```
1 | bin\ServiceManagement.cmd install
```

6. Redeploy the Federated Sign-In Module. If you are not using the Federated Sign-in Module, you can skip this step. *This step should be performed for existing deployments that were done before March, 2019. All deployments performed after March, 2019 already include modifications in these files.*

- Copy the downloaded `cas.war` from step (1c) to `$PAM_HOME/web/webapps`.

Note: If you made any customizations to the Federated Sign-in Module, they may be lost and need to be redone after the migration is complete.

Note: The **PamManagement** service resets to the default *Local System account* Log on property once this service for PAM is reinstalled. If you are using a Log account other than an Local System account for this service then you must restore it prior to restarting the **PamManagement** service. Navigate to *Services* on Windows and find *PamManagement*, right-click and select **Properties**. Go to the *Log on* tab, select *This account:* and restore the required service account.



## Step 4. Start the PAM Services

1. For Windows deployments, start the **PamManagement** and **PamDirectory** services:

```
1 | net start PamDirectory
```

```
1 | net start PamManagement
```

2. For Linux deployments, start the **pammanager** and **pamdirectory** services:

```
1 | service pamdirectory start
```

```
1 | service pammanager start
```

## Step 5. Test and Verify

Once the services come back online, you should now login and thoroughly test the system.

This should include, but not be limited to:

- Login with all applicable types of user accounts; Local, AD/LDAP, MFA and SSO.
- Accessing existing records (and creating new records) in both the Record List and Personal Vault, including the unlock action.
- Creating remote sessions.
- Executing jobs and tasks (on demand and scheduled).
- Viewing and exporting reports.

To confirm the migration, check Framework and WEB Container versions on the bottom of Administration / Settings / Database screen.

The displayed versions should match version that was downloaded.

## Rollback

If the migration or testing fails and you need to roll back to the previous Java framework and a WEB Container, then follow this procedure. If you do not need to rollback, proceed to the next section.

- Stop the PAM services as described earlier
- Rename the new `$PAM_HOME/jre` to `$PAM_HOME/jre.new`
- Rename the previous `$PAM_HOME/jre.old` back to `$PAM_HOME/jre`
- Rename the new `$PAM_HOME/web` to `$PAM_HOME/web.new`
- Rename the previous `$PAM_HOME/web.old` back to `$PAM_HOME/web`
- Start the PAM services as described earlier.

When the services come back online, PAM should be using the previous framework.

You should now perform the testing and validation again.

## Step 6. Cleanup

After all the testing is complete and the system is fully operational, you may remove the following directories:



- `$PAM_HOME/jre.old`
- `$PAM_HOME/web.old`
- `$PAM_HOME/pam-jdk13-pack`
- Files downloaded in [Step 1](#) and extracted archives.

## PAM Software Binary Distribution and Signatures

### PAM Binary Components with MD5, SHA512 and PGP signatures

[Windows Interactive Setup](#) ([md5](#), [sha512](#), [pgp](#))

[Windows CLI Setup](#) ([md5](#), [sha512](#), [pgp](#))

[Linux Setup](#) ([md5](#), [sha512](#), [pgp](#))

[Offline Setup](#) ([md5](#), [sha512](#), [pgp](#))

[WEB GUI and Worker Module](#) ([md5](#), [sha512](#), [pgp](#))

[Directory Service Module](#) ([md5](#), [sha512](#), [pgp](#))

[Runtime Framework for Windows](#) ([md5](#), [sha512](#), [pgp](#))

[Runtime Framework for Linux x86](#) ([md5](#), [sha512](#), [pgp](#))

[Runtime Framework for Linux ARM](#) ([md5](#), [sha512](#), [pgp](#))

[WEB Session Manager for Windows](#) ([md5](#), [sha512](#), [pgp](#))

[WEB Session Manager for Linux x86](#) ([md5](#), [sha512](#), [pgp](#))

[WEB Session Manager for Linux ARM](#) ([md5](#), [sha512](#), [pgp](#))

[Federated Sign-In Module](#) ([md5](#), [sha512](#), [pgp](#))

[WEB Container Module](#) ([md5](#), [sha512](#), [pgp](#))

PGP public key fingerprint:

```
85CA89FD4F9619F02E5DFB5486C9E8312C12ADD2
```

## PAM Component Integrity

To verify the integrity of each PAM binary, we provide the MD5 and SHA-512 checksums and an OpenPGP signature. After you download any binary, you should calculate a checksum for your download and make sure it matches ours above. You may also match the OpenPGP signature against the provided key file.

## Windows Integrity Check

You can use Microsoft methods to check the binary's checksum or any other method you are comfortable using. In the example below, we will use CertUtil in PowerShell to calculate the hashes.

Copy both the downloaded binary and the MD5 or SHA512 hash file to the same directory and from within this location execute the command:

- MD5:

```
CertUtil -hashfile <FILE> MD5
```

- SHA512:

```
CertUtil -hashfile <FILE> SHA512
```

Compare the computed hash to make sure it matches the value from the download hash file.

You can verify the PGP signature using the below command, if available, or another Windows-based OpenPGP verification tool like Gpg4win.

- PGP:

```
gpg --verify <FILE.asc>
```

## Linux Integrity Check

To verify hashes on Linux, copy both the downloaded binary and the MD5 or SHA512 hash file to the same directory and from within this location execute the command:

- MD5:

```
md5sum <FILE>
```

- SHA512:

```
shasum -c <FILE.sha512>
```

Compare the computed hash to make sure it matches the value from the download hash file.

You can verify the PGP signature using the below command from this same directory with the downloaded PGP file:

- PGP:

```
gpg --verify <FILE.asc>
```

- PGP2:

```
gpg2 --verify <FILE.asc>
```

PGP public key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
mQINBGSRl4EBEADNGVbiiPcNZt8kfewufYK2IAPMAoMA5qzLcQca593zpMx9XIcF
FSphu0HGf0+jweP6CYRuyoh9TE76y4CV0Lj7RB/KAkcf94YEO25Y8tiN1Y8m86e
Xo01+isrDBqDoK8sVhISPghMeuarZlVCeHZ/J1SU/cfRA3X07fnfjUWUEHnycnP+
FE9Q5UkJ75nNNNGaEkGkKkCKpPqG4LjujJF0o5Kyuhj04BedLSd0tS10ia4sQR3N
qTYBsKZoyaaocgfVepMhk+7ytXIY6NRTlZbkkvxzc2qHTQZCcolr4ySPQ049a79l
LCAUsXZisyz6/NdxTIDgn8rlanxs2WLDcXqaw5EoYbEBcf6zTwtdSiXqINLmF9HR
6K0mlvqEtL/lw3uzVZmujbLkREPiG0rkpsxdp8eZD8IbNkvIbcVxUQlncwc7sx8W
2qPZ2J5a5ILrWEvUH5w9Dsuhmvo0QJm1rkMNkC2k/goGSgjszZgJYhYEydzjU3ug
v9Jv8xe8EoB/RWrppuuGqPLiNFox6PZG0a/Cp6eSgyekNONydrxc1kriAuNzRniJ
EETk+ODMNufUnk2wIEvLYD4pbdK57i7o0ZksAJ18tjMUTuw4qWG1GC77bgsTTjsY
a5hajl7lZUDQaPDfBU0MfYnquLd0qidxFzsNME3zh/n0sz0m4+EUGSySkwARAQAB
tCdJbXByaXZhdGEgUGFtT3BzIDxwYW1vcHNAaW1wcm12YXRhLnNvbT6JAK4EEwEK
ADgWIQSFyon9T5YZ8C5d+1SGyegxLBKt0gUCZJGXgQIbAwULCQgHAgYVCgkICWIE
FgIDAQIEAQIXgAAKCRGyegxLBKt0mCpD/4hEYLSL0foJdBqcndNkwQvQq/01yYW
eSfmHMwwfN157UzdTB7bAw5vN/saINT0alsT72GImpWpKPJUcjvUeKp0zV4zqzks
7koq7Ny0i9+nI6YpideduQuFTdXn2USda2oGLQnSLtJRLATFNceZKZPYWnXtgsJ0
X05JHLRxt94IhxknuFb0ZBxN1V3lnU4jLiVdYkc9lbEEG0G4LxYLR2LegX1Kb20
W1kd/sM+IxGAQvCToNbHoXdoa0TAu/o0osdTGEg0J7ztmCnprMHL/u6e/IpahdT
AapMMJv1UVqmlHU5L75mU9+8WYBvuuSEdbK/RhAa7R070dpRskSC0QRtboQ4s3+d
vXMWqsS8CY9NrEyAYIKaGkfRSDIZz03wF/G/zk9IM7S0pSQRrnc66jooWBS513jS
9u+HU9I6HmAt9syG0ixj17+BggLvZTBvWyad/+ZxMGk2fV/c6NYgHIFipq19uLfz
FZHsAk1EWuKno7F5LKe6647ByDXsH8QfeqLu1heY21s3AhcCgo5a4siWZbs+sd1K
QBbm9tYqTRCZLwrTS8AphAKTiQFE0uwOCL2Gyu619ZWL8k3K7dxhCFh/zDA9WCy4
RTkF4ysBrCNMTAsL+9HNNsYPeNSP5oifC77a3T7ol6Hngw3FgDWXECYbkH8de3Tq
mi4Q4ubk0X1Mjw==
=VlyT
-----END PGP PUBLIC KEY BLOCK-----
```

# PDF Downloads

- [Windows Installation Guide \(PDF\)](#)
- [Unix / Linux Installation Guide \(PDF\)](#)
- [Quick Start Guide \(PDF\)](#)
- [User Manual \(PDF\)](#)
- [Best Practices Guide \(PDF\)](#)
- [Security Hardening Guide \(PDF\)](#)
- [Administrator's Guide \(PDF\)](#)
- [System Properties Reference Guide \(docx\)](#)
- [Command Line Utility Reference Guide \(docx\)](#)

# Company Information

## Technical Support

If questions remain or issues arise while using PAM, please contact our Support team using this link:  
<https://support.imprivata.com/communitylogin>.

# Imprivata Contact Support

## Support: Americas

North America: +1 800 935 5958

Chile: +56 229 382 447

Brazil: +55 113 198 6183

Mexico: +52 554 170 7697

Other locations: +1 408 987 6072

## Support: EMEA

UK: +44 (0)2035 144149

Austria: +43 720883092

Belgium: +32 (0)2 808 55 86

Denmark: +45 70143085

France: +33 (0)1 84 88 00 15

Italy: +39 06 9480 0186

Netherlands: +31 (0)20 808 5143

Switzerland: +41 (0)22 518 11 79

Other locations: +1 408 854 7891

## Support: APAC

Australia: 1800 219 435

New Zealand: 0800 002 323

Malaysia: 1800 818 111

Other locations: +61 1 800 219 435

# Imprivata Headquarters

## Imprivata Worldwide headquarters

20 City Point, 6th floor

480 Totten Pond Rd.

Waltham, MA 02451

Phone: +1 781 674 2700

Toll-free: +1 877 663 7446

Fax: +1 781 674 2760

## Imprivata European headquarters

6-9 The Square

Stockley Park

Uxbridge, England UB11 1FW

Phone: +44 (0)208 744 6500

Fax: +44 (0)208 744 6501

## Imprivata Germany

3rd Floor, ZeltnerEck Building

Zeltnerstr. 1-3

90443 Nuremberg

Germany

Phone: +49 911 8819 7330

## Imprivata BENELUX

Haagsche Hof

Parkstraat 83

2514 JG The Hague

Netherlands

## Imprivata Australia

Level 19 / 644 Chapel St,

South Yarra, Melbourne VIC 3141

Phone: +61 3 8844 5533

Jul. 01, 2025