



Product Documentation

PAM Users Guide

Contents

Contents	2
Getting Started	7
Technical Support	7
Other Documentation	7
Introduction	7
Technical Support	7
Navigating the User Interface	8
Navigation menu	8
User Settings	8
Records	8
All Records	9
Shared With Me	9
Personal Vault	9
Favorites	9
<Favorite Folders>	9
Administration	9
Global Permissions	9
Global Roles	9
Local Users	10
Local Groups	10
Discovery	10
Scripts	10
Record Types	10
Tokens	10
Workflows	10
Command Control	10
MFA	11
Behavior Profiles	11
Settings	11
Updates	11
Reports	11
Searches	12
Management	13
My Sessions	13
My Profile	13
Profile	13
Subscriptions	13
Anonymous Links	13
Preferences	14
My Alerts	14
My Workflows	14
About	14
Application Toolbar	14
Login and Logout	14
Record List	15
Go to Parent	16
Bulk Actions	16
Manage	17
Import	17
Permissions	17
Workflows	17
Local Users	17
Local Groups	17
Tokens	17
Reports	17
Paste	17

Add Container / Add Folder	17
Add Record	18
Refresh	18
Subscribe to Alerts	18
Add / Remove from Favorites	18
Records	19
Create a New Record	19
Create New Record Page	19
Viewing a Record	19
Split View	21
Editing a Record	21
Sharing a Record	21
Deleting a Record	24
Managing a Record	24
Archive/Restore Records	24
Working with Multiple Records (Bulk Actions)	24
Clipboard Actions (Copy, Cut, Paste, Link)	25
Finding Objects	26
Containers (Folders and Vaults)	27
Create a New Container	27
Opening or Editing a Container	27
Sharing a Container	27
Deleting a Container	30
Managing a Container	30
Container Scoped Objects	30
Container Scoped Local Users	31
Container Scoped Local Groups	31
Container Scoped API Tokens	31
Record Types	32
Working with Record Types	32
Creating Record Types	32
Fields	33
Formula	33
Tasks	34
Commands	34
Editing Record Types	34
Deleting Record Types	34
Inheritance	34
Permission, Roles and Security	35
Object Permissions	35
Record Control	35
Session Control	35
Task Control	36
Inheritance	36
Global Permissions	37
Global Roles	37
Auditor	38
System Administrator	38
Split View	38
Service	38
Blocked	38
Automation	38
Local Users and Groups	38
Create a Local User	39
Local User Password Formula	39
Managing Local Users	39
Create a Local Group	40
Connect	41
In-Session Menu	42

Join	43
Terminate	44
Automatically terminate	44
Windows Logoff Disconnection	44
Recording	45
Video Recording	45
Session Event Recording	46
RDP Client Proxy Sessions	47
Connecting to a Managed Windows Endpoint using an RDP Client	47
SSH Client Proxy Sessions	49
Connecting to the SSH Proxy Interface	49
Connecting Directly to a Managed Endpoint	50
Connecting with an SSH Tunnel	51
Windows Remote PowerShell access	51
Creating Tasks	52
Edit or Remove Tasks	53
Target Record	54
Policy Events	55
Shadow Account	57
Time Window	58
Reviewing Job Results	59
Fallback Jobs	59
Components	60
Managing Templates	61
Create a New Template	61
Edit a Template	62
Delete a Template	62
Manage Bindings	63
Create a New Binding	63
Check Instance Status	67
Terminate Requests Before Approval	68
Requestor	68
System Administrator	68
Terminate Requests After Approval	69
Requestor	69
Approver	69
System Administrator	69
Approve or Reject Requests	70
Interactive Approval	70
Email Approval	70
Local Users Password Formula	72
Scripts Library	73
Creating Custom Scripts	73
Editing Existing Scripts	73
Deleting Existing Scripts	74
Discovery Query	75
Creating a New Query	75
Managing Existing Queries	75
Viewing a Query Report	76
Deleting Queries	76
Scheduling Queries	77
Command Control Policies	78
Create Command Control Policies	78
Edit or Delete Command Control Policies	79
Apply Command Control Policies	79
Apply Policies to Record Types	79
Apply Policies to Records	79
	81
Behavior Profiles	84

Create Behavior Profiles	84
Edit or Delete Behavior Profiles	86
Edit or Delete Behavior Profiles Rules	86
Applying Behavior Profiles	86
Application Nodes	88
Proximity Groups	89
Database	90
Registration	91
Parameters	92
Mail Server	93
AD	94
Syslog	95
Check and Update PAM Online	95
Check and Update PAM Offline	97
Performing PAM software update manually	98
PAM and OS upgrade	99
Alert and Report Subscriptions	100
In-application and Email Alerts	100
Subscribe/Unsubscribe from Alerts	100
Emailed Reports	101
Subscribe / Unsubscribe from Reports	101
Working with the API	102
Authentication Tokens	102
Managing Tokens	102





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/>.

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](#)

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:

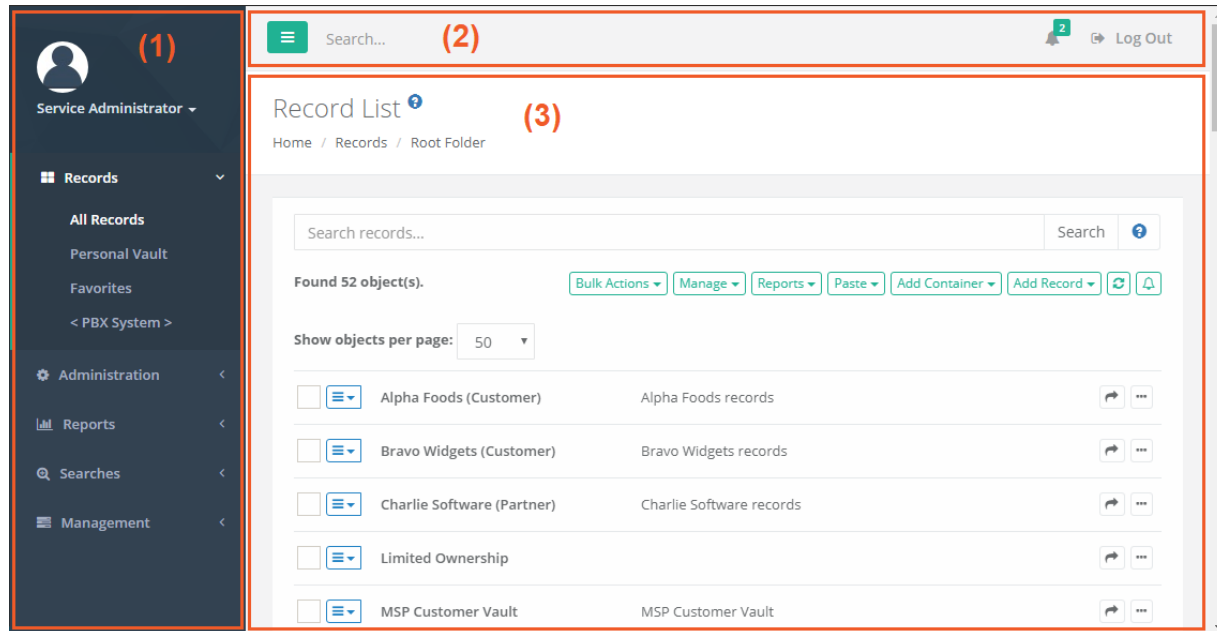
<https://support.imprivata.com/>.



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 be 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.



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:



Breadcrumb Path	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.
Go to Parent	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.
Connect	Creates a secure remote session to this managed asset or endpoint.
Execute	Executes the selected task that has been configured with an on-demand policy event.
Unlock/Lock 	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.
Audit Log	Displays the audit events specific to this record including <i>Timestamps</i> , <i>Users</i> , <i>IP Addresses</i> and <i>Events</i> .
Change History	Displays the <i>history of changes</i> that have been made to the values of this record.
Sessions	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</i> , <i>Events</i> , <i>Join</i> , <i>Terminate</i> and <i>Recording Export or Download</i> options.
Job History	Displays all the <i>Jobs</i> or <i>Tasks</i> that have been executed with this record, including details, timestamps and users.
Grant	Provides the option to Grant Access to this record using an existing Workflow Template and Binding.
Manage	Provides a menu of options to manage this record including <i>Command Control Policies</i> , <i>Formula</i> , <i>Permissions</i> , <i>Tasks</i> , <i>Workflows</i> and <i>Archive</i> state.
Edit	Switches the record into Edit mode so that the record values can be modified.
Subscribe to Alerts 	Allows the user to subscribe to alerts for this record.
Add/Remove Favorite  / 	Adds or Removes this record from the user's Favorites list.
Anonymous Link 	Generate an anonymous link associated to this record.



Request <Name> Request Connect	If you are bound by a workflow template, your <i>Connect</i> , <i>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%{| *****



Password

*****| e\$vseLMpqg[2



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.

Permissions 

Home / Production / Permissions

Permissions for Production / inherited from [Web Servers](#)

Found 5 entries.

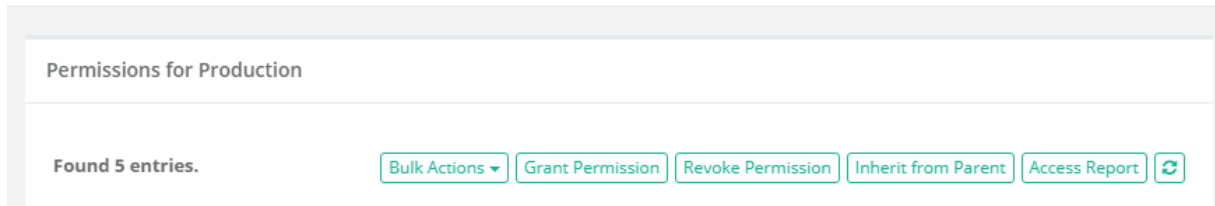
[Make Unique](#) [Access Report](#) 

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 command control policies that are associated to this record.
Formula	Defines the password complexity formula that will be used when generating passwords.
Permissions	Defines the users and groups that have permissions to this record.
Tasks	Defines all the tasks that are associated to this record.
Workflows	Defines all the workflow bindings 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	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. Objects created using <i>Paste</i> will inherit permissions from its new parent; <u>any unique permissions will be lost.</u>
Link	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. Objects created using <i>Link</i> will retain the inherited permissions from their original parent or their unique permissions as configured.

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.



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.



Permissions

Root Folder / IT Records / **Permissions**

Permissions for IT Records

Found 2 entries. [Bulk Actions](#) [Grant Permission](#) [Revoke Permission](#) [Inherit from Parent](#) [Access Report](#) 

Principal	Type	Record Control	Session Control	Task Control	Actions
-----------	------	----------------	-----------------	--------------	---------

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.



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 Add Record dropdown menu.
Description	Enter a description. The record type description will only be visible in the Record Type 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 Connect 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 Add Record dropdown menu.
Personal Vault	Check this box if you want to make this record type available to be used in Personal Vaults .



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. Unhidden 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 Locked and Unlocked .
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.



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 Local User Formula .
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.

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.

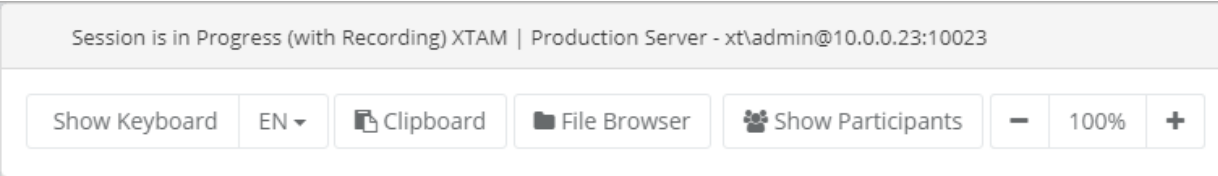


In-Session Menu

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.

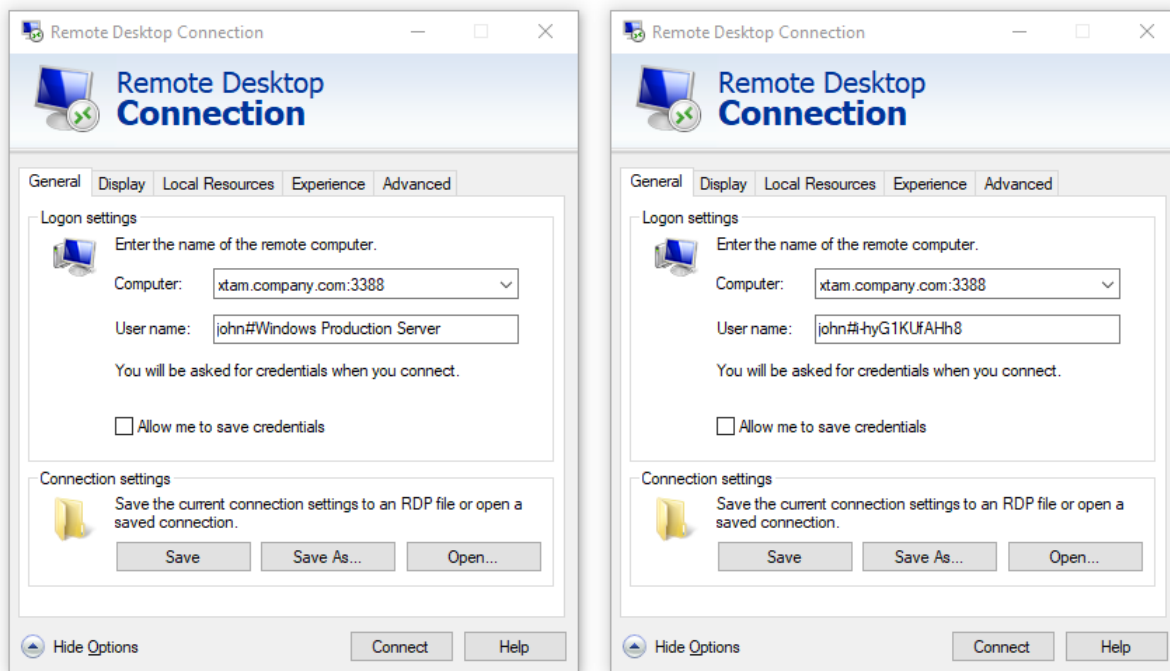
For example, the RDP Host or Computer you would enter into your RDP client would be `xtam.company.com` and the default port would be 3388.

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 to ignore case.
less	The Less command adds pagination to the list of available records. Use q 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)

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 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>n</i> th 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 <selected day>	<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 Execute menu and can be initiated when needed by a user with the required permissions.
Every <i>n</i> th 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 x to y 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 Run button to send this job to the queue. If the job is configured to run on a remote worker node, the Run 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 Cancel 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 Details 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.

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	<p>Select from the available types:</p> <ul style="list-style-type: none">• Automatic Approval – the system will automatically approve the request. No human interaction required.• Interactive Approval – requires user approval in the form of one or more approval steps.• Restrict Access - 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.• Delegated Approval- allows users to delegate their approval action to the system.
Step <i>n</i>	<p>Defines the list of approvers per step. Each listed approver will be notified when there is a request pending their approval.</p> <ul style="list-style-type: none">• When using Groups as an approver, each member of the group will be notified of pending requests.• Rank determines how many “approves” are required in total to advance the workflow to the next step.• When the last step is fully approved, only then will the requester gain the needed approval to use their request operation.• A requester may be included in their own approval template; however, they will not be permitted to approve their own request.• To add additional steps, click the Add Step button.

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">• Administration – 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 Workflow Binding article.• Record Control – Requires the user to have approved access before they can Unlock or Edit the object.• Connect Control – Requires the user to have approved access before they can Connect to a session.• Task Control - Requires the user to have approved access before they can Execute an on-demand task.
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>CRON EXPRESSION HELP</p> <p>Examples of time execution window formats:</p> <p>* * 1-7 ? * SUN,SAT * - between 1am and 7am, on every Sunday and Saturday</p> <p>* * 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</p> <p>System Administrators can define the time, day or date values of each time selector in Administration > Settings > 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">• 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.• Optional – The requester will decide to Check Out the record or not when making the access request.• Required – 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. <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">• Disabled – MFA will not be required.• Required – The user will be required to use MFA when the approved action is initiated. <p>Currently the option supports TOTP, Duo Security OTP and Radius MFA for Unlock and Connect actions.</p>
Behavior Profile	Applies the selected Behavior Profile 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 <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 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.



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.



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.



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.



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.



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

CSVPDFXLSXPDF ProtectedCSV ProtectedXLSX 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

- 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

Save

Cancel

Default ?

☐

Principals ?

Add

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.



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 > 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.



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.

C A U T I O N: 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.

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.

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.



Components

Found 1 components.

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

Update is scheduled for node: demo-server-xt01

Refresh

5. 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.

Node	Components	Available Version	Downloaded Version	Actions
demo-server-xt01 Working / 11/20/2017 09:10	Worker: 2.3.201711192301 GUI: 2.3.201711192301	2.3.201711192301		Current version is up to date

Refresh



Check and Update PAM Offline

To Check and Update PAM Offline:

1. Download the offline update from here: <https://bin.xtontech.com/product/pam-pkg.zip>
2. Copy the downloaded zip file to the PAM server.
3. Extract the zip file to a temporary location on the PAM server.
4. In this temporary location, navigate to `/pkg/pam` and copy the files `xtam.war` and `xtamWorker.war`.
5. Paste these files to `$PAM_HOME/content`, or the directory specified by the `Administration / Settings / Properties / Content Location` parameter.
6. Once copied, PAM will begin the update process automatically.
7. 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.

8. Download and then unpack the web archive <https://www.xtontech.com/wp-content/uploads/2017/12/web.zip>
9. 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.)
10. Restart the **PamManagement** (Windows) or **pammanager** (Linux) service.



Performing PAM software update manually

1. Login to PAM host server. Administrative privileges may be required.
2. Download the offline update (<https://bin.xtontech.com/product/pam-pkg.zip>) and extract to a temporary location.
3. Stop the **PamManagement/pammanager** service.
Note that this PAM node will now be offline until the update is complete.
4. Navigate to `$PAM_HOME/web/webapps` and delete both files `xtam.war` and `xtamWorker.war`
5. Also in this same location, delete both directories `xtam` and `xtamWorker`.
 - Optionally, rather than deleting these files and directories, you can move them to a temp location outside of `$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.



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.



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.