PAM

Installation Guide - Windows

Contents

Introduction

This guide is designed to show system administrators how to install, initialize and run Privileged Access Management (PAM) on a Windows host.

Technical Support

If at any time you encounter an issue, have questions or need guidance, please contact us using the information provided in our documentation site.

If questions remain or issues arise while using PAM, please contact our Support team: https://support.imprivata.com/.

Privileged Access Management

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

The purpose of this guide is to perform a new installation and first time system initialization.

At the conclusion of this guide, PAM will be ready for system configuration and use.

The target audience is system administrators with knowledge of computer administration, Active Directory and (optionally) database connectivity.

PAM is installed to a Windows or Unix computer (physical or virtual), with optional connection to Active Directory or LDAP.

The system consists of several modules; a database that contains secrets, configuration, passwords and audit events, a service to establish, monitor and record privileged sessions, a user directory to maintain local users and groups and a job engine to execute scripts and tasks.

Privileged Account Management

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

Privileged Session Management

The ability to establish a privileged session to an underlying system (Windows, Unix, Linux, Mac) through a standard web browser while providing the means to monitor, join, record or terminate this session.

Privileged Job Management

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

Software Components

To accomplish the requirements above, PAM needs to install, configure and run the following software and services. These components are deployed during the installation process (single server deployment) or they can be distributed to multiple servers (farm deployment) to scale performance.

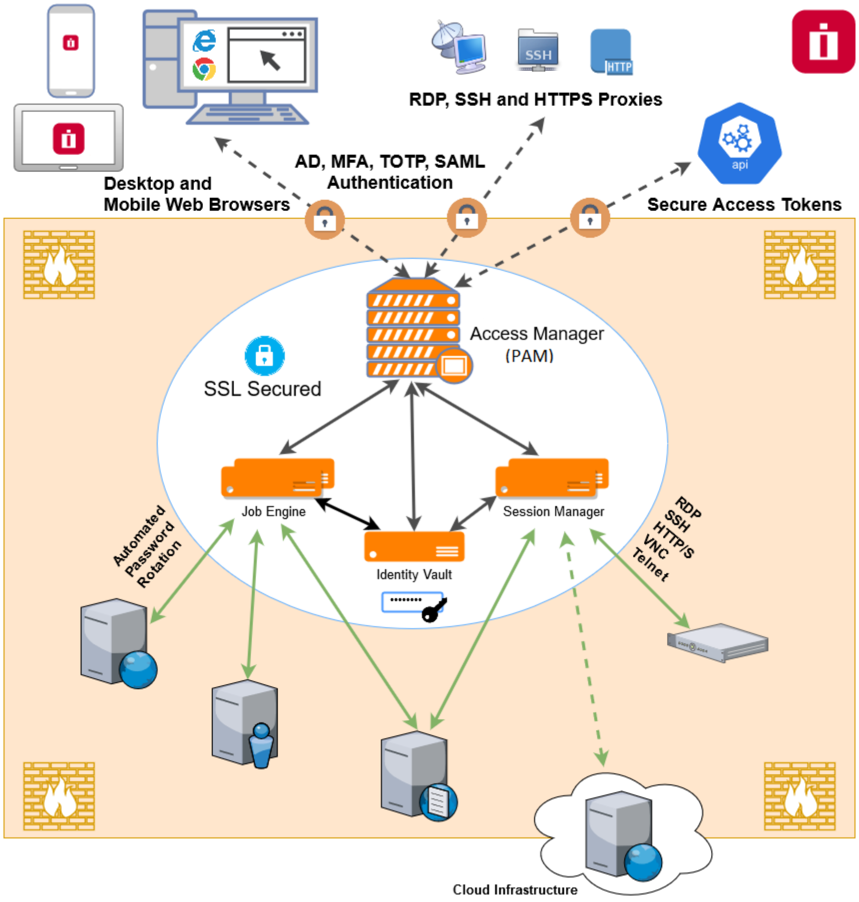
Single server deployments can be scaled to farm deployments when additional resources become needed.

Architectural Diagram

PAM sits within the firewall in its own SSL secured network.

Client computers make requests, establish sessions and run jobs from inside or outside the firewall to computers also located inside or outside the firewall using only their native web browser of choice.

The Database of Secrets secures all records using an AES 256-bit encrypted protocol and only delivers these secrets to authorized remote requests.



Privileged Access Management Architectural Diagram

Services

Depending on your installation, the following services may be deployed to Automatically startup on your computer.

Service	Function
PamDirectory	Provides the directory service to manage local users and groups in PAM.
PamManagement	Provides the service to manage the PAM system.
PamSession	Provides the service to establish, maintain, control and record privileged sessions via a user's web browser.

Table: PAM Services

Active Directory or LDAP Integration

Integration with Active Directory or LDAP provides the ability to add Active Directory Users or Groups to PAM to manage or use the system.

PAM will use this Active Directory integration to:

- Authenticate user logins;
- Read Active Directory group membership;
- Reset Active Directory passwords.

Planning your Installation and Deployment

The key to a successful deployment is proper planning. Before you begin the installation process, please understand the following.

- The full scope of your user base. How many individual users will be working with PAM and of those how many will be accessing the system at the same time. This will help in planning the amount of resources and servers that are required to run the system efficiently.
- Setup a test environment. This could be a basic single server VM or a dedicated workstation, but ensure PAM is configured and running in your test environment before deploying to production. This can also act as a test bed for future software releases.
- Decide if you want to integrate with Active Directory or LDAP for users, groups and authentication or to maintain a local directory for users and groups.
- If you want to use a SSL certificate to ensure a secure connection between the client computers and PAM, then it is highly recommended to obtain and deploy the certificate prior to installation.

Getting Started Guidelines

Before you begin your installation of PAM, please be sure to have the following readily available.

- Your operating system (OS) of choice. Use our recommendations to determine which is best for your needs.

- Your external database connection parameters. If you are using an external database for PAM, make sure you have the database, connection string and proper credentials to provide the required connectivity.

- Your Active Directory connection parameters. If you are integrating PAM with your Active Directory, make sure you have the required connection string and credentials to provide the required connectivity.

- Your enterprise's SSL certificate. If you plan on replacing our temporary self-signed certificate with your own trusted SSL certificate, make sure you have access to the certificate so that it can be imported into PAM.

Installing Privileged Access Management

This section will work through the process of installing Privileged Access Management (PAM) to a Windows computer.

System Requirements

The following are minimum requirements to use PAM for Single Server and medium use Production farms.

Please contact us https://support.imprivata.com/ to discuss architecture and system recommendations for large scale farm deployments.

	Single Server, Test or Quick Trial	**Medium Use Production Farm**
Windows O/S (64-bit only)	Windows Server 2012+ / Windows 10	Windows Server 2012+
Other O/S (64-bit only)	Red Hat, Ubuntu, Debian, CentOS	Red Hat, Ubuntu, Debian, CentOS
Database	Included*	MS SQL, MySQL, Oracle, PostgreSQL
Memory (reserved for PAM use)	4GB+	8GB+
Disk Space (reserved for PAM use)	20GB+	50GB+

Table: System Requirements

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

Software Requirements

- Web Browsers *(latest version is recommended if not specified)*
  - Windows Edge, Google Chrome, Mozilla Firefox or Apple Safari

External Database

The default installation includes an internal database that can be deployed. If you would prefer to use an existing database in your environment, the following are supported. Please be prepared to supply a valid connection string to your database as well as an appropriate user and password to successfully establish this connection. Please contact your Database Administrator if you need assistance.

NOTE: The installation process does **not** create its own database or tablespace but rather makes use of an existing one. Also, for Oracle DB you just need to create a user (you do not need to create a new data base). With that in mind, please ensure one with the name “PamDB” already exists as this will be used by the application.

- Apache Derby version 10.12.1.1+
- Microsoft SQL version 2016+ (SQL Authentication only)
- MySQL Community or Enterprise Edition version 5.7+
- Oracle version 11.2+
- PostgreSQL version 9.5+

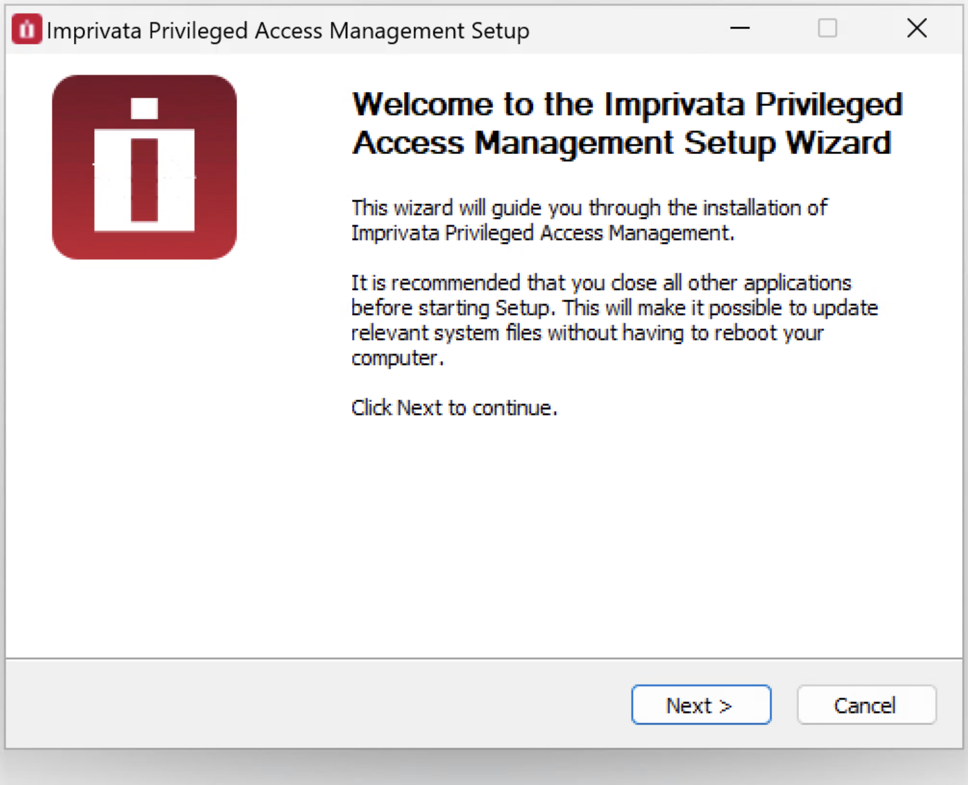
Installation

The following section will describe each option that is available in the installation wizard.

Software binaries can be downloaded from https://help.xtontech.com/content/more-information/binary-distribution-and-signatures.htm.

To begin, run the setup file from your computer and follow through the wizard.

Depending on the options selected, the following configuration parameters may be available.



Welcome to the Imprivata Privileged Access Management Setup Wizard

This wizard will guide you through the installation of Imprivata Privileged Access Management.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

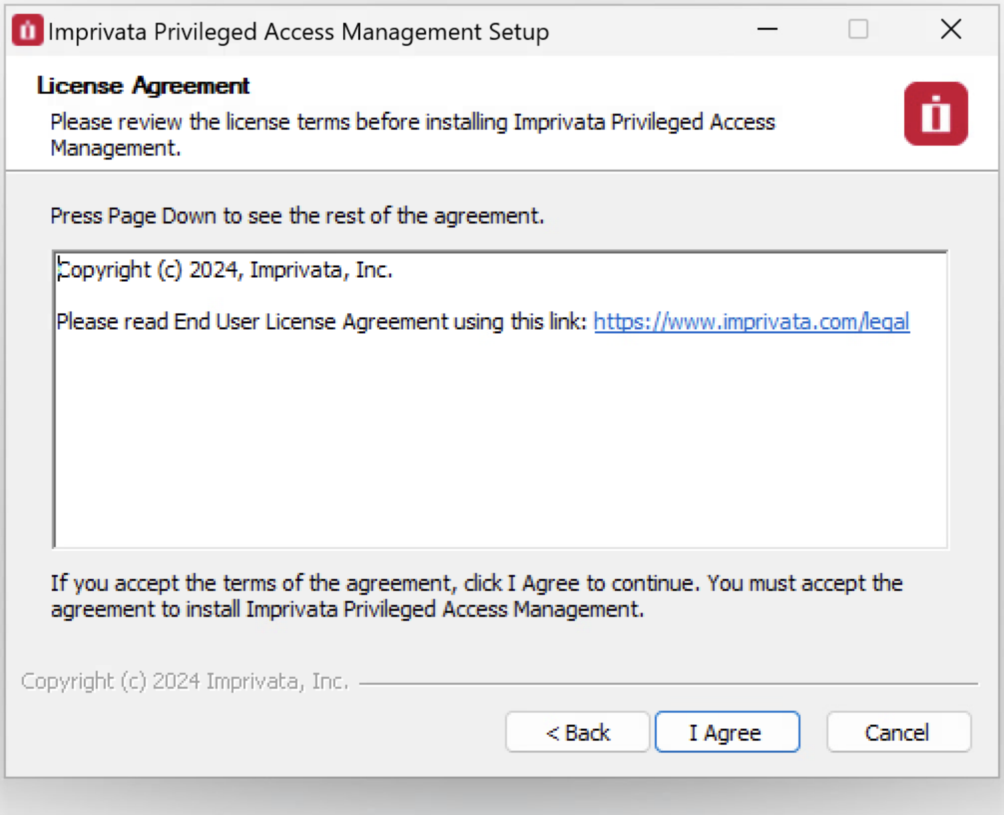
Click Next to continue.

Setup Welcome Page

License Agreement

Read and accept the license agreement by clicking the **I Agree** button to proceed.

The license agreement must be accepted to install the software.



License Agreement

Please review the license terms before installing Imprivata Privileged Access Management.

Press Page Down to see the rest of the agreement.

Copyright (c) 2024, Imprivata, Inc.

Please read End User License Agreement using this link: https://www.imprivata.com/legal

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Imprivata Privileged Access Management.

Copyright (c) 2024 Imprivata, Inc.

Read and Accept the License Agreement

Components

Choose from the available list of components to install on this computer. If you are looking to deploy a quick test environment, the recommendation is to leave the default options and simply click **Next** to continue.

If you would like to customize the installation, then please review the following sections to understand the purpose of each component.

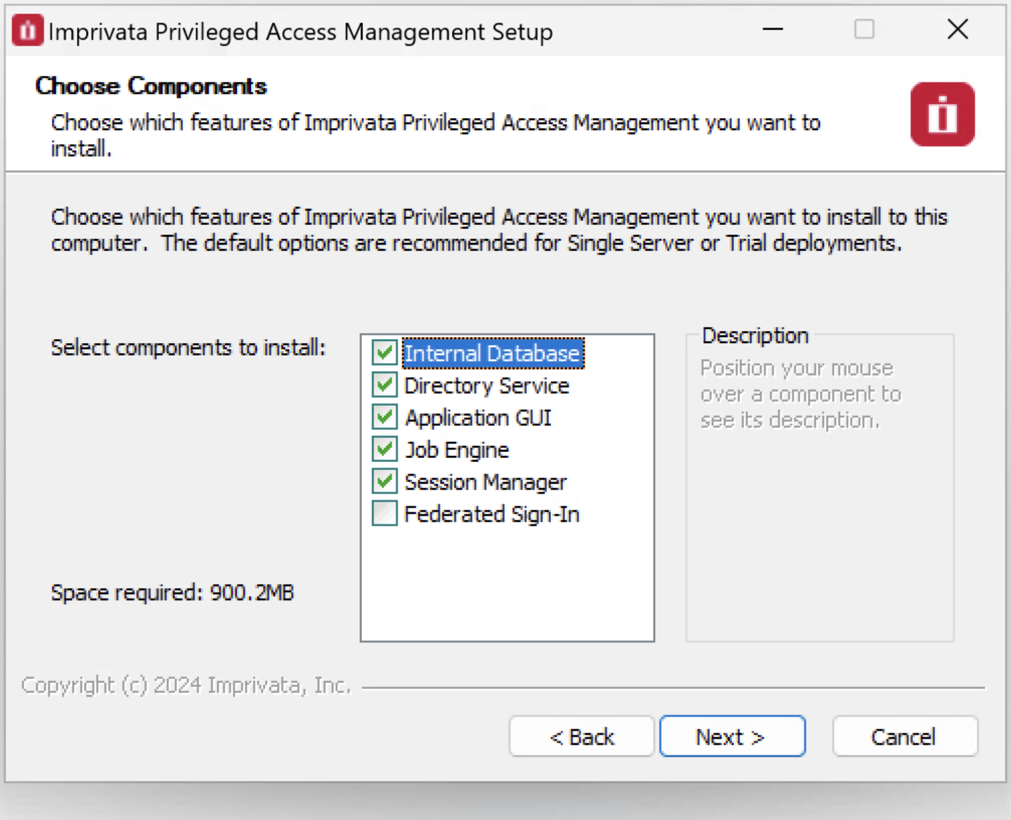
When you are finishing customizing your component selection, click **Next** to continue.

Please note that while you can choose to not install some components on this system, they may still be required for proper software operations.

For example, you may wish to install the Session Manager service on another system for performance optimization.

In this situation, you would choose to not deploy this service on your primary host and then after this initial installation is complete, you would then run this same installer on your other host and only choose the **Session Manager** option.

Later on in the configuration of the software, you will have the ability to define which workstation is running each service.



Choose Components

Choose which features of Imprivata Privileged Access Management you want to install.

Choose which features of Imprivata Privileged Access Management you want to install to this computer. The default options are recommended for Single Server or Trial deployments.

Select components to install:

- ☑ Internal Database
- ☑ Directory Service
- ☑ Application GUI
- ☑ Job Engine
- ☑ Session Manager
- □ Federated Sign-In

Description

Position your mouse over a component to see its description.

Space required: 900.2MB

Copyright (c) 2024 Imprivata, Inc.

Choose Components

Internal Database

This option will define which database to use.

When enabled (checked) the installation will deploy, configure and use its internal database.

If disabled (unchecked), you will be prompted to supply an existing database in your environment to use (connection string, user and password).

Please review the requirements section for more information about External Database support.

For single server or test environments, the recommendation is to enable (check) this option to use the included database.

Directory Service

This option will define which user store to use.

When enabled (checked) the installation will include a local user store that can be used to create users and groups and a database to secure the master password.

When disabled (unchecked) the installation will not deploy this component to the computer; however, this is a required component so it must be deployed to only one other computer and configured post installation in PAM.

To install this component on another host, simply run the installer on that system and enable (check) this option.

The recommendation is to include this option during installation.

Application GUI

This option will define the deployment of the PAM interface (GUI).

When enabled (checked) the installation will include the manager interface (GUI) to this host computer.

When disabled (unchecked) the installation will not deploy the GUI requirements to this host computer.

To install this component on another host, simply run the installer on that system and enable (check) this option.

The recommendation is to include this option during installation.

Job Engine

The Job Engine is required to execute background operations like discovery queries and password resets.

This option defines the deployment of a worker role to this host computer.

When enabled (checked) a Job Engine role will be deployed. When disabled (unchecked) a Job Engine role will not be deployed to this computer.

To install this component on another host, simply run the installer on that system and enable (check) this option.

Please note that at least one job engine should be present in the farm to execute password reset, remove script execution or discovery queries.

The recommendation is to include this option during installation.

Session Manager

The Session Manager component is required to establish, control and record privileged sessions.

This option defines the deployment of a session manager service to this host computer.

When enabled (checked) a session manager service will be deployed, configured and run from this host. When disabled (unchecked) a session manager service will not be deployed.

To install this component on another host, simply run the installer on that system and enable (check) this option.

Review the following section if you intend to install Session Manager on a remote computer(s): Remote Session Manager Configuration

Please note that if a session manager service is not defined during installation, you will need to add one during system configuration before sessions can be established.

The recommendation is to include this option during installation.

Federated Sign-In

This option defines the deployment of a federated sign-in component that can be used to establish user authentication.

When enabled (checked) you will need to supply your federated sign-in server connection parameters.

When disabled (unchecked) a SSO server will not be configured and the default login authentication will be used.

To install this component on another host, simply run the installer on that system and enable (check) this option.

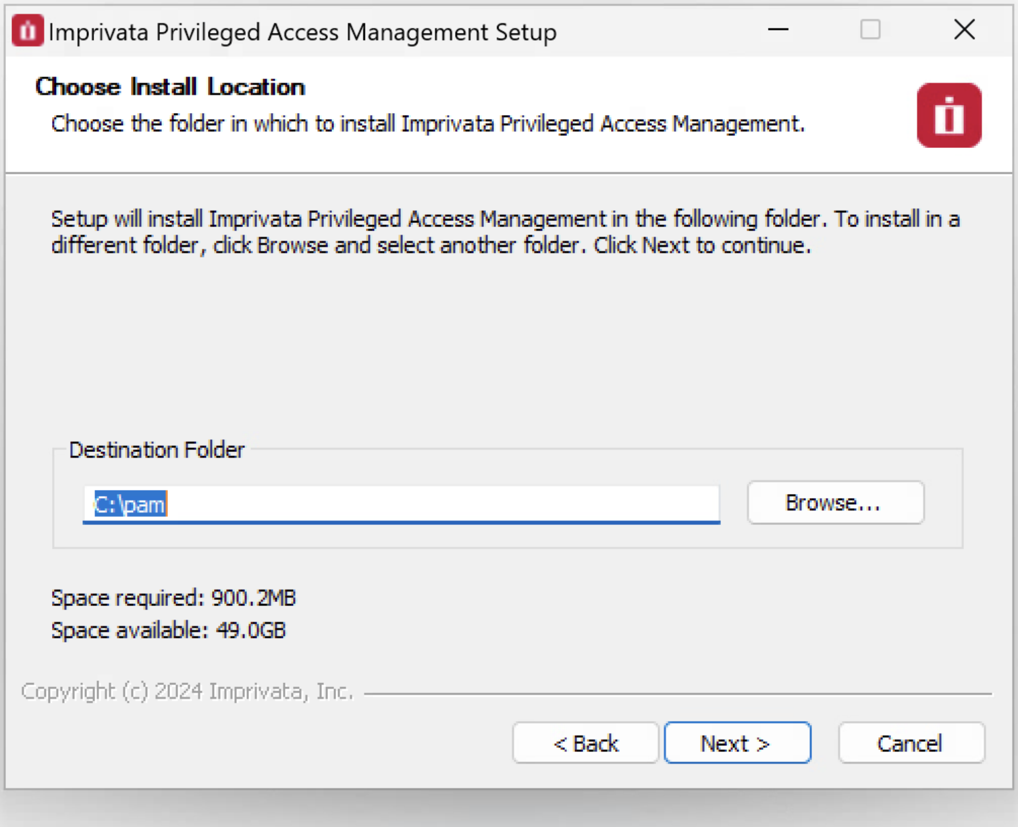
This is an advanced option and should only be included if necessary. For single server or test environments, the recommendation is to not include this option.

NOTE: The Federated Sign-In component requires the use of a properly trusted (not self-signed) SSL certificate which is used to communicate over a secure HTTPS connection. This ensures that both the client browsers and server side components trust the certificate. If you do not want to deploy and configure a trusted certificate, then do not include this component during installation.

Installation Location

Enter or select the location where the PAM software will be downloaded and installed.

Click **Next** to continue.



Imprivata Privileged Access Management Setup

Choose Install Location

Choose the folder in which to install Imprivata Privileged Access Management.

Setup will install Imprivata Privileged Access Management in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder

C:\pam

Space required: 900.2MB

Space available: 49.0GB

Copyright (c) 2024 Imprivata, Inc.

Choose Installation Location

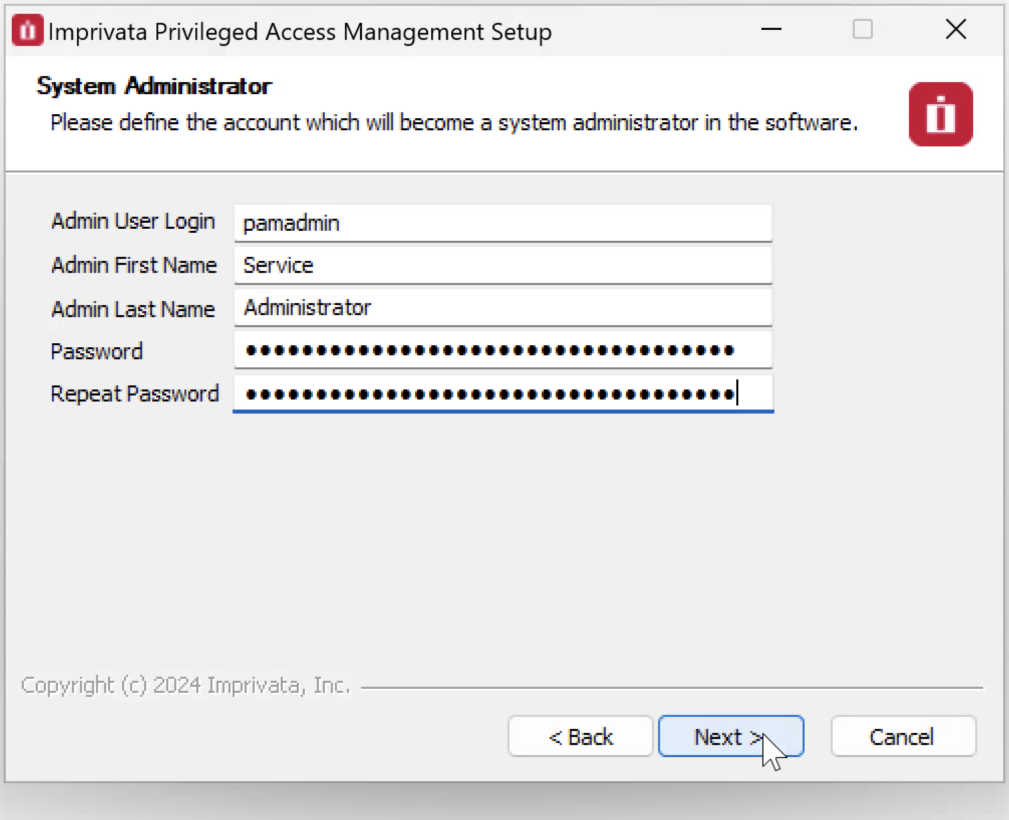
System Administrator

Enter the required parameters to create your default System Administrator login to PAM.

The account specified here may be used as the first System Administrator, so be sure to choose a memorable login (default login is “**pamadmin**”) with a strong password (maximum of 30 characters).

Both the user login and password will be displayed later when they can be saved to a file for safe keeping.

Click **Next** to continue.



System Administrator

Please define the account which will become a system administrator in the software.

Admin User Login: pamadmin
Admin First Name: Service
Admin Last Name: Administrator
Password: ••••••••••••••••••••••••••••••••••
Repeat Password: ••••••••••••••••••••••••••••••••••

Copyright (c) 2024 Imprivata, Inc.

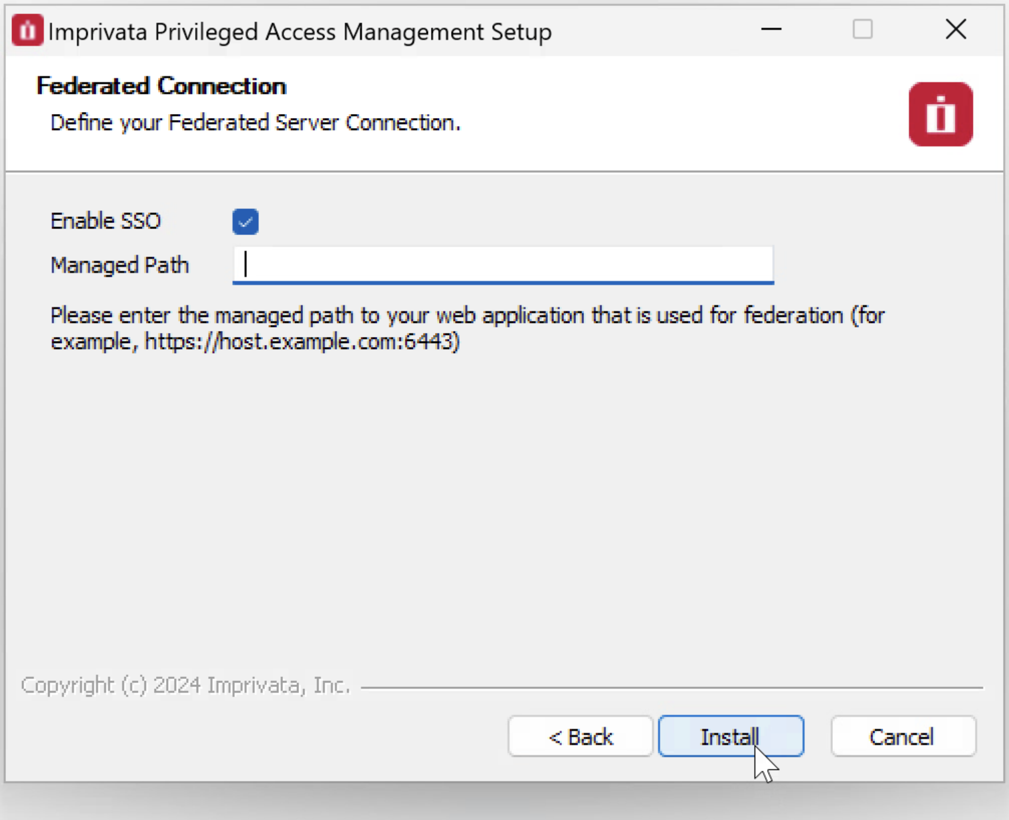
Create PAM System Admin Account

SSO Connect

To define a managed path to be used with federated sign in, enable (check) the **Enable SSO** box and then enter that valid path in the **Managed Path** field.

If PAM is to be used with an SSL certificate, then this option should be enabled and the managed path needs to be defined with a secure path (for example, https://host.example.com).

Click **Next** to continue.



Imprivata Privileged Access Management Setup

Federated Connection

Define your Federated Server Connection.

Enable SSO ☑

Managed Path

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

Copyright (c) 2024 Imprivata, Inc.

Enable and Define Federated Connection (optional)

External Database

If the Database option was left disabled (unchecked) earlier, then you will now need to define your connection to your external database.

Select your **Database** type and then enter the required parameters to establish a successful connection.

If further assistance is required, please contact your Database Administrator.

Click **Next** to continue.

NOTE: The installation process does **not** create its own database or tablespace but rather makes use of an existing one. With that in mind, please ensure oe with the name “PamDB” already exists as this will be used by the application.

Example strings are listed below.

- *Apache Derby*
    - Example connection string: db-host or db-host:port
- *Microsoft SQL Server*
    - Example connection string: db-host or db-host:port
        - A database with the name “PamDB” must already exist and will be used for the application. Ensure the supplied account is the “owner” of this database and it is a SQL account for authentication. Active Directory accounts are not supported.
- *MySQL*
    - Example connection string: db-host or db-host:port
        - A schema with the name “pamdb” must already exist and will be used for the application. Ensure the supplied account has ALL schema privileges assigned.
- *Oracle*

    - Example service: db-host/db-service

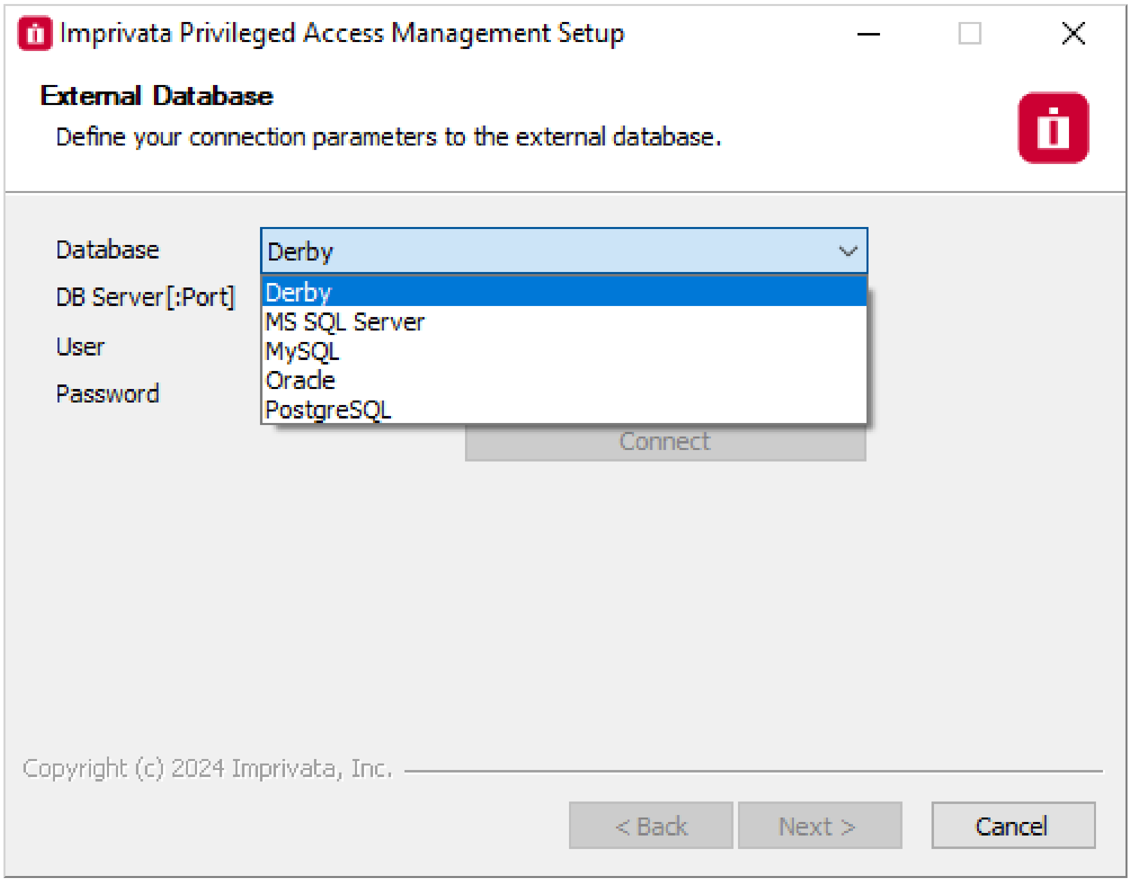
    - Example instance: db-host:port:SID

        - Grant *(at a minimum)* “CONNECT, RESOURCE, UNLIMITED TABLESPACE” to the supplied user account.

- *PostgreSQL*

    - Example connection string: db-host or db-host:port

        - A database with the name “PamDB” must already exist and will be used for the application. Ensure the supplied account is the “owner” of this database or has been provided with “ALL” privileges to it (CTc).


Imprivata Privileged Access Management Setup

External Database

Define your connection parameters to the external database.

Database: Derby

Connect to an External Database (optional)

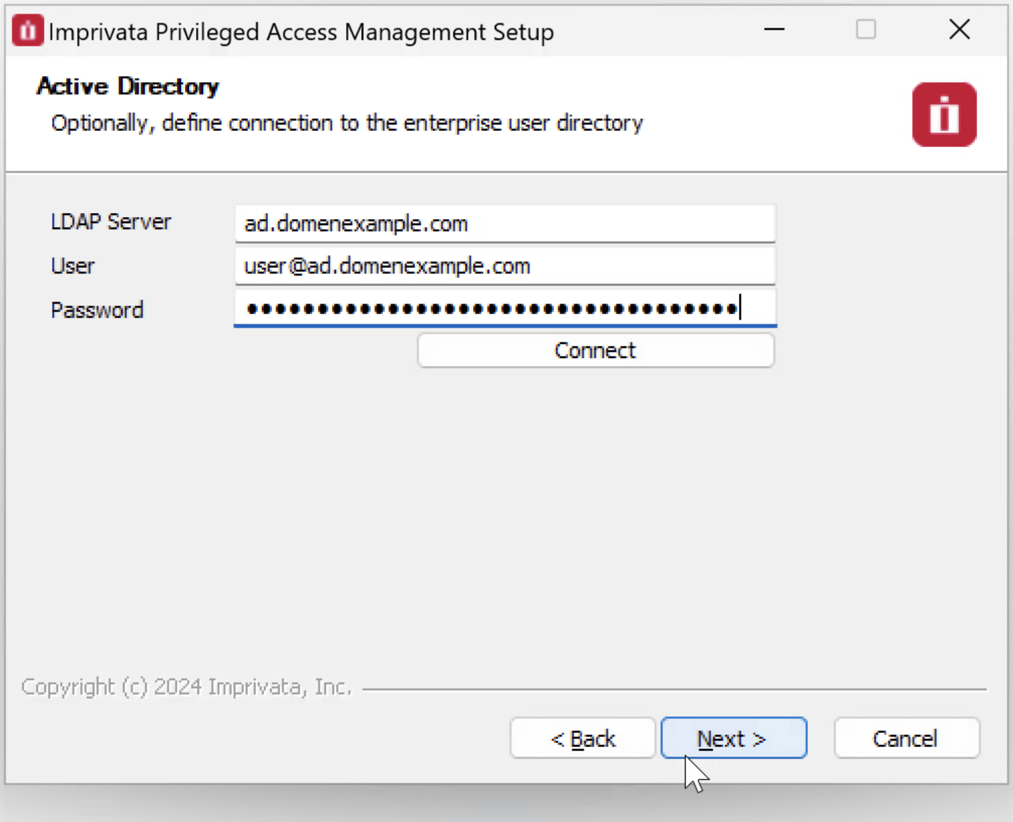
Active Directory Integration

Optionally, you may choose to integrate PAM with your existing Active Directory or LDAP server. Enter your **LDAP Server** FQDN, your Active Directory or LDAP **User** (user@domain.com or domain\user), its **Password** and then click **Connect**.

If the connection is successful, this user may become a System Administrator in PAM and you may continue.

If you cannot or do not want to integrate with Active Directory or LDAP, you may leave these parameters empty.

Click **Next** to continue.



Imprivata Privileged Access Management Setup

Active Directory

Optionally, define connection to the enterprise user directory

LDAP Server: ad.domenexample.com

User: user@ad.domenexample.com

Password: ••••••••••••••••••••••••••••••••••••

Copyright (c) 2024 Imprivata, Inc.

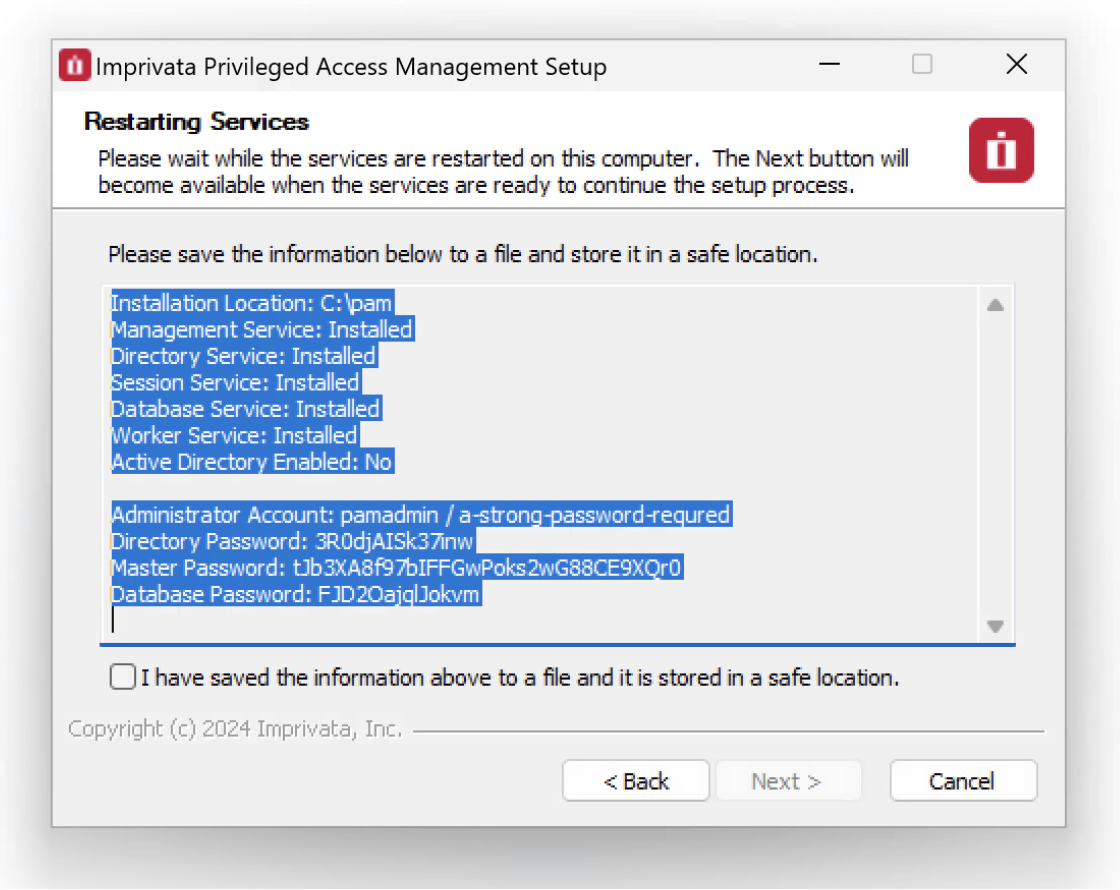
Active Directory or LDAP Server Integration

Summary

The summary screen will display all the services, accounts and password that were created during installation.

It is **extremely** important that all this information be saved to a file and kept in a safe location.

The Master Password displayed will be required in a “break glass" or database transfer scenario and no one will be able to identify nor update this password if it is ever lost.



Imprivata Privileged Access Management Setup

Restarting Services

Please wait while the services are restarted on this computer. The Next button will become available when the services are ready to continue the setup process.

Please save the information below to a file and store it in a safe location.

```
Installation Location: C:\pam
Management Service: Installed
Directory Service: Installed
Session Service: Installed
Database Service: Installed
Worker Service: Installed
Active Directory Enabled: No

Administrator Account: pamadmin / a-strong-password-requred
Directory Password: 3R0djAISk37inw
Master Password: tJb3XA8f97bIFFGwPoks2wG88CE9XQr0
Database Password: FJD2OajqlJokvm
```

□ I have saved the information above to a file and it is stored in a safe location.

Copyright (c) 2024 Imprivata, Inc.

Summary Screen with Passwords (save this information to a file for safe keeping)

If you do not see these passwords or receive any errors in this Summary screen the installation was not successful.

Complete the installation and then uninstall to try again.

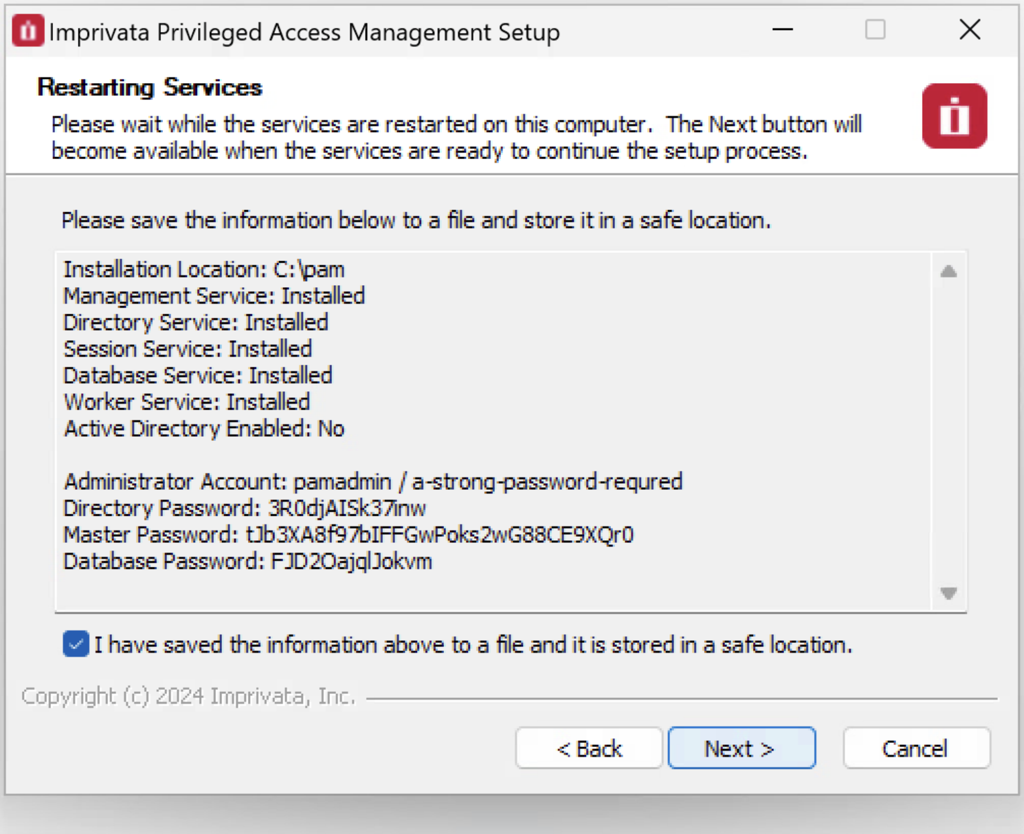
Do not initialize Privileged Access Management without a successful deployment and a safe and secure copy of the logins and passwords shown in the example Summary screen.

The **Next** button will be disabled until all the services have been started and are available on this computer.

This process may take a few minutes to complete.

When the services are ready, check the box to confirm that your passwords have been saved to a file in a safe location and then the **Next** button will become available.

Click **Next** to continue.



Restarting Services

Please wait while the services are restarted on this computer. The Next button will become available when the services are ready to continue the setup process.

Please save the information below to a file and store it in a safe location.

```
Installation Location: C:\pam
Management Service: Installed
Directory Service: Installed
Session Service: Installed
Database Service: Installed
Worker Service: Installed
Active Directory Enabled: No

Administrator Account: pamadmin / a-strong-password-requred
Directory Password: 3R0djAISk37inw
Master Password: tJb3XA8f97bIFFGwPoks2wG88CE9XQr0
Database Password: FJD2OajqlJokvm
```

☑ I have saved the information above to a file and it is stored in a safe location.

Summary Screen with Confirmation

NOTE: It is extremely important that all the passwords displayed in this section are saved to a file and this file is stored in a safe location. These passwords cannot be retrieved by software developers or anyone else once the installation is complete.

Completing the Installation

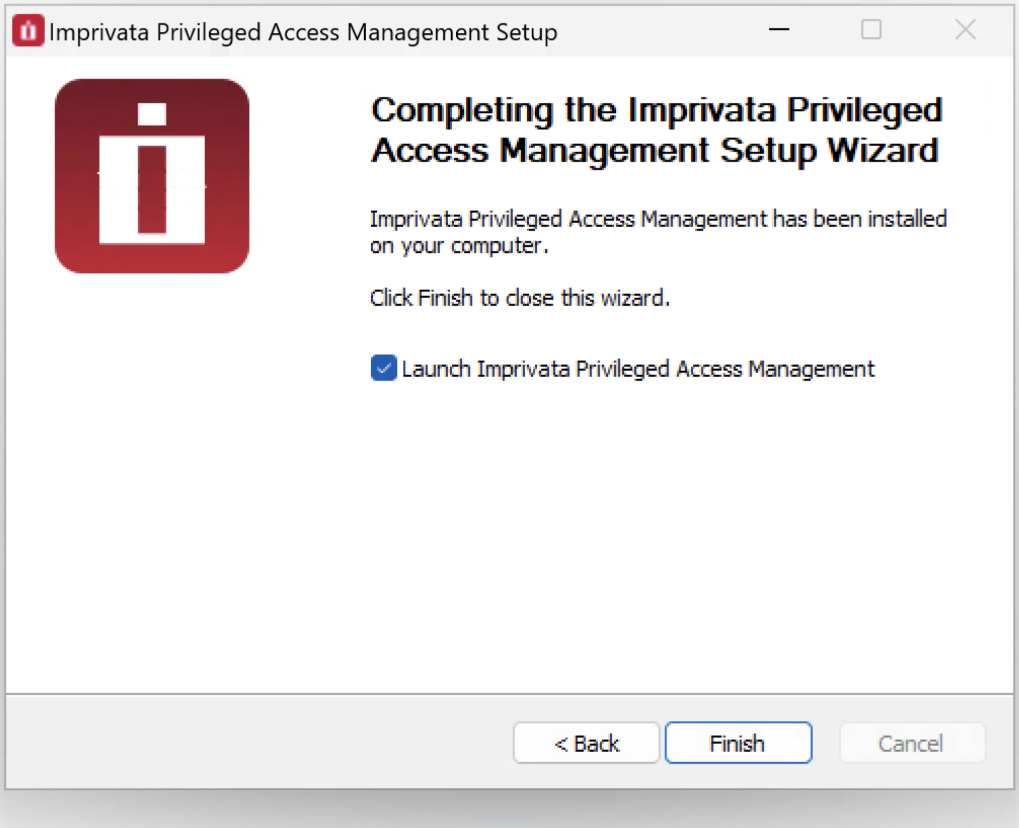
On the final page, confirmation that the installation has been completed will appear.

Enable (check) the box to launch the sign-in page or disable (uncheck) the option to not open the page.

Click **Finish** to close the installation wizard.

The software is now installed.

The default location for PAM is https://localhost:6443/xtam/.



Completing the Imprivata Privileged Access Management Setup Wizard

Imprivata Privileged Access Management has been installed on your computer.

Click Finish to close this wizard.

☑ Launch Imprivata Privileged Access Management

Installation Complete

Logging into Privileged Access Management

Open your web browser and navigate to the login screen of PAM or double click the shortcut on your desktop.

- Non-secured login: http://localhost:8080/xtam
- Secured login: https://localhost:6443/xtam
  - (Click here to understand your browser certificate warning)

At the login prompt, you can sign in with one of the following system administrator logins:

- The System Administrator account that was created during the installation process.
- The Active Directory or LDAP account that was (optionally) used to establish integration during the installation process.

Enter the System Admin user and password and click the **Login** button.

Upon successful login, you will be directed to the initialization page of PAM.

The account used as the first login will become a System Administrator.

Browser SSL Certificate

A default installation of PAM comes with a pre-created PAM Self-signed SSL certificate to encrypt traffic.

Because this SSL certificate is self-signed and therefore not trusted by your browser or certificate authority, a security warning will appear when the login page opens.

It is safe to accept the security warning for this self-signed certificate only; however, you may consider these options:

1. You may use the non-secured login at this location: http://localhost:8080/xtam to avoid the browser warning and continue using the software without encrypting your traffic.

2. You may accept the warning, install the certificate and use it as supplied. Although it is self-signed, it will still encrypt the traffic.

3. You may substitute our non-trusted, self-signed certificate with your own trusted, signed certificate by following the procedure described in this article.

While our self-signed SSL certificate is acceptable for trial or PoC deployments, they should not be used for any production deployments.

We **strongly** recommend the use of a well-known trusted SSL certificate or one generated by your own Certificate Authority.

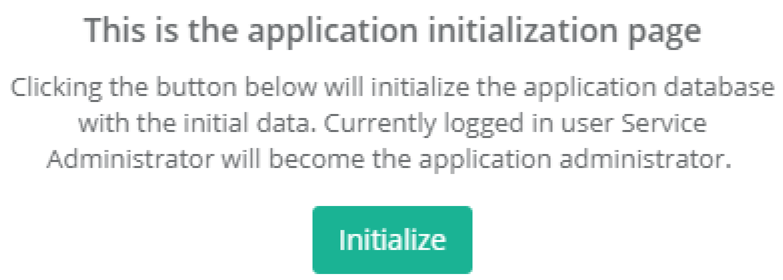
Initialize

The first login (and only the first) after a new installation will require a system initialization.

When logged in for the first time, click the Initialize button to begin this process.

During this time, the system will create all its needed configuration in the database and services.

Depending on the complexity of your configuration, this process may take anywhere from a few seconds to 1-2 minutes to finish.



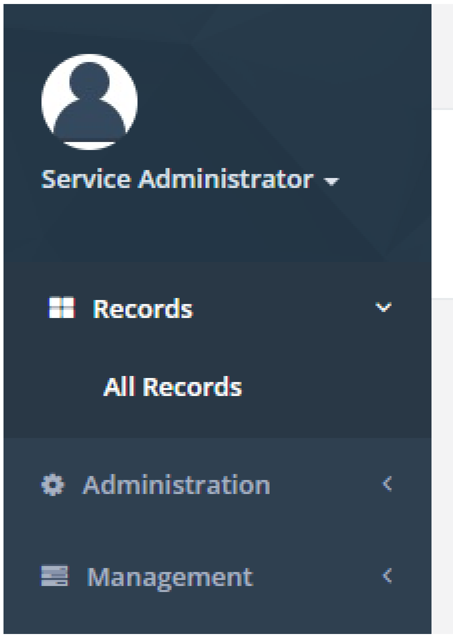
This is the application initialization page

Clicking the button below will initialize the application database with the initial data. Currently logged in user Service Administrator will become the application administrator.

PAM “first-time” Initialization

When the initialization is complete, the system will redirect you to the landing page.

You should see a few menu headings on the left side including Records, Administration and Management indicating that the process is complete.

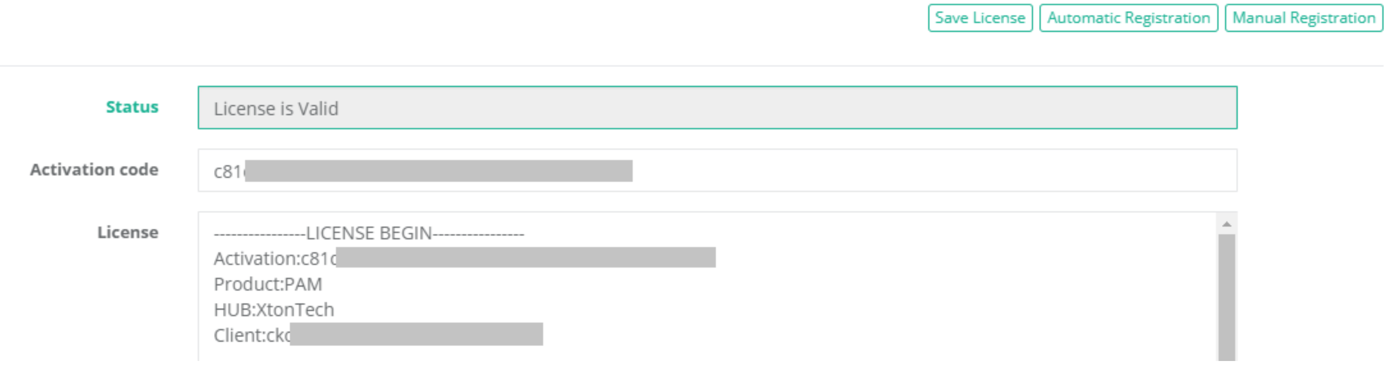


Initialization Complete

License Registration

If you have a license key, then you should activate it now.

1. Navigate to Administration > Settings > Registration.
2. On the registration screen, copy and paste your key into the “Activation Code” field and then click **Automatic Registration**.
3. When the license is retrieved successfully (status should display “License is Valid”), click the **Save License** button to finalize.
4. The software is now activated and ready for use.



Status License is Valid

Activation code c81[redacted]

License

```
----------------LICENSE BEGIN----------------
Activation:c81[redacted]
Product:PAM
HUB:XtonTech
Client:ck[redacted]
```

License Activation

Manual Registration

If the computer is not connected to the internet or cannot establish a connection to the license server for registration, then the following procedure will register the software manually.

1. Click the **Manual Registration** button. A new browser window will appear.

2. Copy or transfer this URL to a computer with an internet connection and load the page.

3. Select the copy the license information between and including the LICENSE BEGIN header and LICENSE END footer.

4. Save this information to a file or paste it directly into the **“License”** field in PAM.

5. Click the **Save** License button.

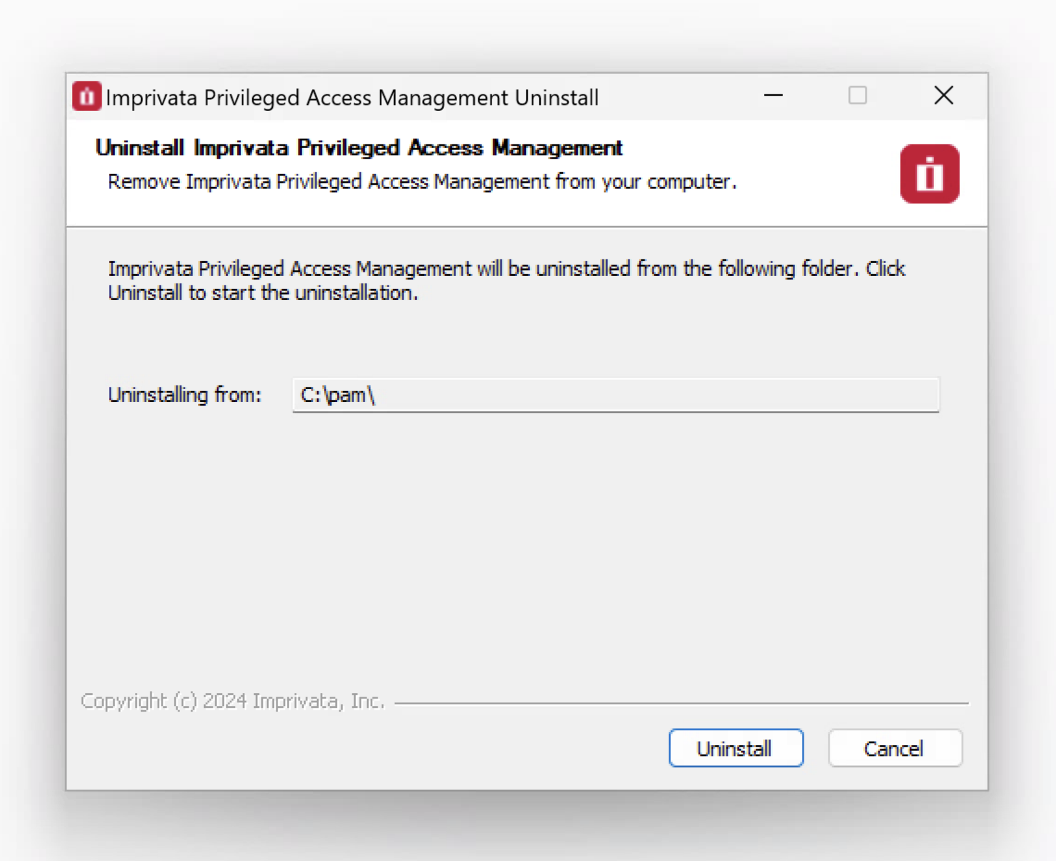
6. The license status will read **“License is Valid”** and the software is now registered.

Uninstalling Privileged Access Management

You can uninstall PAM by simply running the uninstall executable located in its installation directory.

Uninstaller

1. First, logout and close any open Sessions in PAM as well as any open sessions in your Web Browser.
2. Double click the uninstall executable and follow the wizard.



Imprivata Privileged Access Management Uninstall

Uninstall Imprivata Privileged Access Management

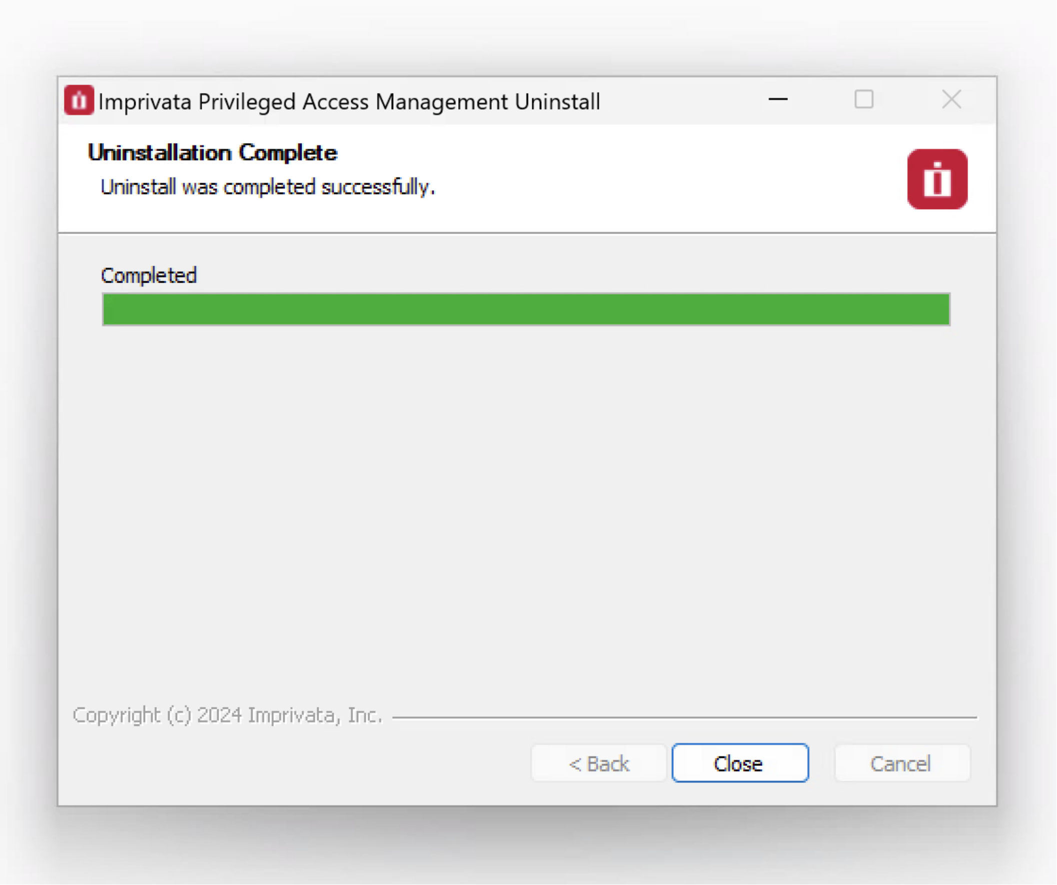
Remove Imprivata Privileged Access Management from your computer.

Imprivata Privileged Access Management will be uninstalled from the following folder. Click Uninstall to start the uninstallation.

Uninstalling from: C:\pam\

Copyright (c) 2024 Imprivata, Inc.

3. When the wizard completes, the software and its services will be removed from your computer.



Uninstallation Complete

Uninstall was completed successfully.

Completed

Copyright (c) 2024 Imprivata, Inc.

4. If you deployed additional services to other servers, then you will need to run the uninstall executable on each of these computers to remove the components.

Database Cleanup

If you have configured PAM with the use of an external database, then you will need to manually remove these database objects.

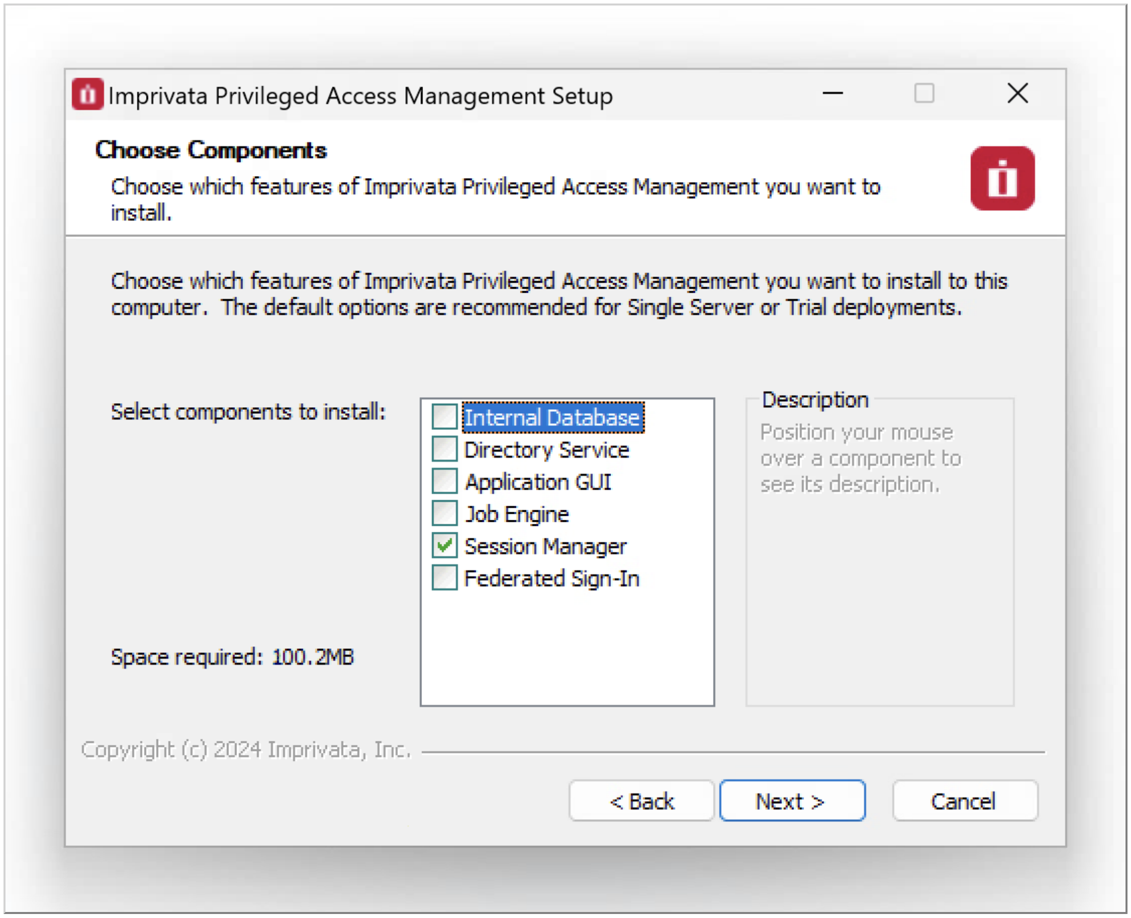
Please contact your database administrator for assistance.

Appendix

Remote Session Manager Configuration

When installing the Session Manager component on a remote Windows computer(s), then the following steps should be taken.

1. Ensure that PAM is Installed and configured on your master computer.
2. Run the setup file on the remote computer where Session Manager is to be deployed.
3. On the Welcome screen, click **Next** to begin the installation on this computer.
4. Read and accept the License Agreement by clicking the **I Agree** button to continue.
5. Uncheck all Component options except Session Manager. Click **Next** to continue.



Imprivata Privileged Access Management Setup

Choose Components

Choose which features of Imprivata Privileged Access Management you want to install.

Choose which features of Imprivata Privileged Access Management you want to install to this computer. The default options are recommended for Single Server or Trial deployments.

Select components to install:

- □ Internal Database
- □ Directory Service
- □ Application GUI
- □ Job Engine
- ☑ Session Manager
- □ Federated Sign-In

Space required: 100.2MB

Description

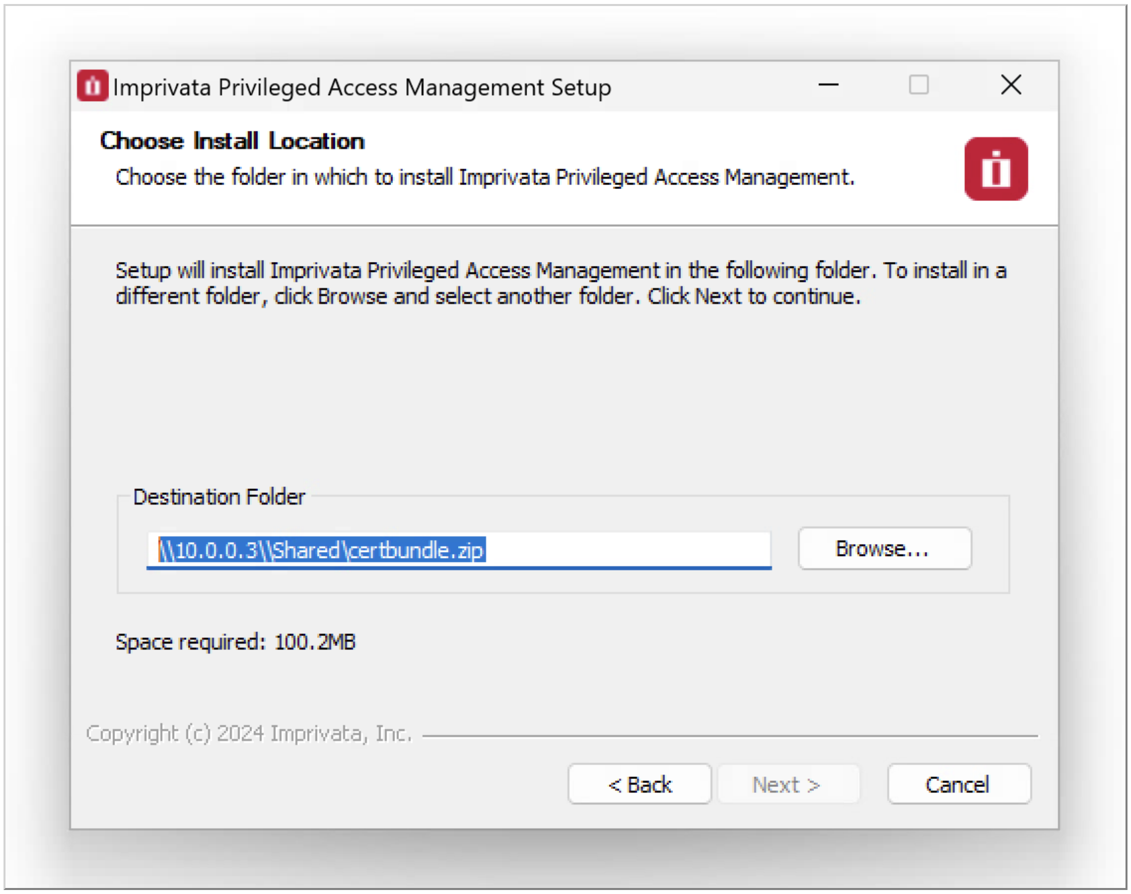
Position your mouse over a component to see its description.

Copyright (c) 2024 Imprivata, Inc.

Select the Session Manager Component

6. Choose your installation location and click **Next** to continue.

7. When prompted, locate and select the certificate bundle that was deployed to your master computer where PAM was installed earlier. Click **Next** to continue.



Imprivata Privileged Access Management Setup

Choose Install Location

Choose the folder in which to install Imprivata Privileged Access Management.

Setup will install Imprivata Privileged Access Management in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder

\\10.0.0.3\\Shared\certbundle.zip

Space required: 100.2MB

Copyright (c) 2024 Imprivata, Inc.

Locate and Select certbundle.zip

- The certificate bundle is in the root PAM installation directory on your master computer. The default file location is C:\pam\certbundle.zip

- You may select the zip file from this default location (if possible), copy it to a shared network location or simply copy the zip file to this remote computer and select it locally.

NOTE: This step is optional, so if you wish to not supply the certificate you may simply click **Next** to continue. By skipping this option, you are acknowledging that the communication between PAM on the master computer and this remote Session Manager computer will not be secured. Because of this, it is recommended that you supply the certificate when prompted and do not skip this step.

8. The Session Manager service will now startup on this computer. Click **Next** to continue.
9. Click **Finish** to complete the installation.