Privileged Account Manager

Installation Guide

December 2019

Legal Notice

For information about Micro Focus legal notices, see https://www.microfocus.com/about/legal.

© Copyright 2019. Micro Focus or one of its affiliates.

Contents

About This book and the Library **5**

1 NetIQ Privileged Account Manager Overview **7**

Components 7
Procedural Overview 8

2 Planning Your Privileged Account Manager Installation **9**

Privileged Account Manager Installation Checklist 9

3 Installing the Framework Manager **11**

Installing a Framework Manager 11
Linux Framework Manager Installation 11
Windows Framework Manager Installation 12
Accessing the Console 12
Downloading and Installing NetIQ Privileged Account Manager License 13
Stopping and Restarting the Framework 14
Linux 14
Windows. 14
Removing the Framework Manager 14
Linux Manager Uninstall 15
Windows Manager Uninstall. 15

4 Installing the Agents **17**

Agent Installation Overview 17
Creating a Host Name for Each Agent (Optional) 17
Opening Firewall Ports 18
Installing and Registering a Framework Agent 18
AIX Agent Install 18
HP-UX Agent Install 19
Linux Agent Installation 20
Windows Agent Installation 21
Solaris Agent Install 22
Removing the Agent Components 23
AIX Agent Uninstall 23
HP-UX Agent Uninstall 23
Linux Agent Uninstall 24
Solaris Agent Uninstall. 24
Windows Agent Uninstall 25

5 Configuring Application Single Sign-On **27**

Application SSO Modes 27
RemoteApp Mode 27

Direct Access Mode 28
Setting Up Application SSO 29
Prerequisites 30
Disabling Task Manager Keyboard Shortcut Keys and Sticky Keys in Windows 30
Installations for Application SSO. 31
Creating an Active Directory User 31
Extending the Schema and Assigning User Rights 32
Configuring Application SSO 33
Configuring Application SSO Credential Vault and Rule. 38

6 Configuring Privileged Account Manager 39

Enabling FIPS Mode 39
Disabling CBC Mode 40

7 Upgrading Privileged Account Manager 41

About This book and the Library

This guide explains the hardware requirements for the Privileged Account Manager components, then explains how to install the components.

Audience

This guide is intended for users who install and manage the Privileged Account Manager product.

Other Information in the Library

Privileged Account Manager Administration Guide

1 NetIQ Privileged Account Manager Overview

NetIQ Privileged Account Manager delivers a robust and scalable architecture, intuitive management console, and reusable script and command libraries that enable administrators to reduce management overhead and infrastructure costs in your environment.

Privileged Account Manager helps an organization protect critical assets and maintain compliance requirements by securing, managing and monitoring privileged accounts for privileged access. It is capable of managing the shared accounts and also auditing those accounts. You can monitor all the actions performed in the servers for Windows, Linux, database, or any application such as, LDAP.

This guide will help you to install, or upgrade the Manager for Privileged Account manager and Agent for Privileged Account Manager.

Components

Privileged Account Manager consists of a Framework Manager, where you manage and configure the system, and an agent, which is installed on each machine where you want to monitor and control superuser access.

From the Home page, you have access to the following administrative consoles:

- **Compliance Auditor:** Proactive auditing tool that pulls events from the event logs for analysis, according to predefined rules. It pulls filtered audit events at hourly, daily, weekly or monthly intervals. This enables auditors to view prefiltered security transactions, play back recordings of user activity, and record notes for compliance purposes. In an era of increasing regulatory compliance requirements, the ability to supply demonstrable audit compliance at any time provides a more secure system and reduces audit risk.
- **Framework User Manager:** Manages users who log in to the Framework Manager through role-based grouping.
- **Hosts:** Centrally manages Privileged Account Manager installation and updates, load-balancing, redundancy of resources, and host alerts.
- **Reporting:** Provides easy access and search capability for event logs and allows you review and color-code user keystroke activity through the Command Risk Analysis Engine.
- **Command Control:** Uses an intuitive graphical interface to manage security policies for privilege management.
- **Package Manager:** Lets you easily update any Privileged Account Manager application.
- **Access Dashboard:** Lets you manage the requests for emergency access, and view the details of password checkout. If required you can check-in the checked out password.
- **Enterprise Credential Vault:** Lets you store and manage the domains with related credentials.

Procedural Overview

The following steps are required to install Privileged Account Manager:

1. Install a Framework Manager. See Chapter 3, "Installing the Framework Manager," on page 11.
2. When the installation has completed, access and log in to the console. See "Accessing the Console" on page 12.
3. Install the Privileged Account Manager license. See "Downloading and Installing NetIQ Privileged Account Manager License" on page 13.

   By default, new installations are provided with a 90-day license for five agents, one of which is the manager. You need to install your license before the default license expires.
4. Set up a Package Manager so you can install additional packages on the agents and push package updates to your framework components. See Configuring the Package Manager.
5. Install and register a Framework Agent on the computers that you want to manage. See Chapter 4, "Installing the Agents," on page 17.

   When you have installed and registered the Framework agents, you have completed the installation of the Framework.
6. For configuration information, see the *Privileged Account Manager Administration Guide*.

2 Planning Your Privileged Account Manager Installation

This chapter guides you through planning your Privileged Account Manager installation.

Privileged Account Manager Installation Checklist

Use the following checklist to plan, install, and configure Privileged Account Manager:

If you are upgrading from a previous version of Privileged Account Manager, do not use this checklist. For information about upgrading, see Chapter 7, "Upgrading Privileged Account Manager," on page 41.

	Tasks	See
❑	Ensure that the computers on which you want to install Privileged Account Manager components meet the specified requirements.	Privileged Account Manager 3.7 System Requirements and Sizing Guidelines
❑	Install the Framework manager.	Chapter 3, "Installing the Framework Manager," on page 11
❑	Install the agents.	Chapter 4, "Installing the Agents," on page 17
❑	Configure Privileged Account Manager.	Chapter 6, "Configuring Privileged Account Manager," on page 39

3 Installing the Framework Manager

- "Installing a Framework Manager" on page 11
- "Accessing the Console" on page 12
- "Downloading and Installing NetIQ Privileged Account Manager License" on page 13
- "Stopping and Restarting the Framework" on page 14
- "Removing the Framework Manager" on page 14

Installing a Framework Manager

Currently, the Framework Manager is available for installation on the platforms listed below. For more information about the supported platforms, see the System Requirements in PAM Documentation website.

NOTE: After the Framework Manager is installed, the manager console runs on the default port 443 and can be accessed with `https://<ip>`. The default port can be changed by changing the port number in the `connector.xml` file located at `<install_path>/service/local/admin/connector.xml`.

For detailed installation instructions for your platform, select from the list below:

- "Linux Framework Manager Installation" on page 11
- "Windows Framework Manager Installation" on page 12

Linux Framework Manager Installation

Linux hosts use the RPM packaging system for installation, upgrade, and removal.

By default, the installation program installs the software into `/opt/netiq/npum`. To change this, create a directory in the required part of the file system and create a symbolic link to `/opt/netiq/npum`.

Prerequisites

- When you are installing framework manager in SLES 12 or later, ensure that LSB (Linux Standard Base) version 3.0 or later is installed.
- If you want to use Enhanced Access Control feature, you must install 32bit `glibc` (GNU C library) library in 64 bit RHEL manager.

To install the Linux manager:

1. Copy the installation package to a temporary location and use the following command to install the file:

   ```
   rpm -i <filename>.rpm
   ```

2 After installation is complete, check that the service is running by viewing the log file. The log file is located in `/opt/netiq/npum/logs/unifid.log`, if the default install location was used. If the manager installed correctly, services should be listening on 0.0.0.0:29120 and 0.0.0.0:443.

3 If you have been supplied with a license, log in to the Framework Console and install the license. For information, refer to "Accessing the Console" on page 12, and then "Downloading and Installing NetIQ Privileged Account Manager License" on page 13.

Windows Framework Manager Installation

In Windows environment, you can install Framework Manager in the following ways: Interactive installation and Silent installation. The silent or unattended installation is useful when you need to install Framework Manager in more than one server.

To install the Windows Framework Manager:

1 (Conditional) **For interactive installation, perform the following:**

1a Run the following install executable to start the installation:

`<filename>.msi`

1b Follow the steps in the install wizard.

The Framework Manager service can be installed on any part of the normal file system. It defaults to the `C:\Program Files\Netiq\npum` folder.

2 (Conditional) **For silent installation, use the following command:**

Syntax: `msiexec /i <Installer Filename> /passive`

For more information about other `msiexec` command-line options, see Microsoft documentation.

3 After installation is complete, check that the service is running by viewing the log file. The log file is located in `C:\Program Files\Netiq\npum\logs\unifid.log`, if the default install location was used. If the manager installed correctly, services should be listening on 0.0.0.0:29120 and 0.0.0.0:443.

4 If you have been supplied with a license, log in to the Framework Console and install the license.

For information, refer to "Accessing the Console" on page 12, and then "Downloading and Installing NetIQ Privileged Account Manager License" on page 13.

Accessing the Console

1 Open a Web browser on your chosen platform.

2 In the address bar, enter the URL for the Framework Console as follows:

`https://<hostname>`

Replace *<hostname>* with one of the following:

- The DNS name of the server where the Framework Manager is installed.
- The DNS name of a server that has the Administration Agent package installed.

3 If you are presented with a security alert, verify the details and select **Yes** to continue.

4 If your browser is not already equipped with Adobe Flash Player, the browser attempts to install it. Verify the details and select **Install** to continue.

   A reboot or browser restart might be required.

5 Log in to the Framework Console.

   After you enter the URL for the Framework Console, the initial logon screen is displayed in the browser window. You must authenticate to the system by using a username and password defined on the system.

6 (Conditional) If this is the first time to log in to the console, specify the username `admin` and password `novell`, then click **Logon**.

7 (Conditional) If this is the first time to log in to the Framework Console, you are prompted to change the default password.

   Your new password should be a minimum of eight characters. If the new password is acceptable to the system, you are logged in to the console.

   IMPORTANT: To navigate in the Framework Console, you can use the show/ hide drop down that is displayed when you hover the mouse on the **Console** menu. Do not use your browser's Forward or Back buttons; instead hover the mouse on the **Console** menu at the top of each page and select the required administrative console from the drop down list.

   Click **Home** to return to main console menu.

   ---

8 Continue with "Downloading and Installing NetIQ Privileged Account Manager License" on page 13.

Downloading and Installing NetIQ Privileged Account Manager License

---

NOTE: By default, new installations are provided with a 90-day license for five agents, one of which is the manager.

---

1 Downloading NetIQ Privileged Account Manager license:

   1. Log in to the NetIQ Customer Center.
   2. Click **Software > Entitled Software**.
   3. Click **Keys** against the required Privileged Account Manager release to download the license.

2 Installing NetIQ Privileged Account Manager license:

   1. Log in to the Framework Console.
   2. From the **Task Pane**, click **About Framework**.
   3. Click **Register Framework**.
   4. Copy the supplied license and paste it into the text area.
   5. Click **Finish > Close**.

      Your license details can be viewed by selecting the **About Framework** option from the **Task Pane**.

3 Continue with one of the following:
   - Configuring the Package Manager
   - Chapter 4, “Installing the Agents,” on page 17

Stopping and Restarting the Framework

The Framework services and processes start automatically after installation and system reboot, so there is normally no need to stop and restart them. If you need to stop and restart the services and processes manually, follow the instructions below for your platform:

- “Linux” on page 14
- “Windows” on page 14

Linux

The following instructions apply to all distributions.

To stop the Framework process:

```
/etc/init.d/npum stop
```

To start the Framework process:

```
/etc/init.d/npum start
```

To check the status:

```
/etc/init.d/npum status
```

Windows

To stop the Framework service:

1. Select the **Start** button.
2. Select **Control Panel**.
3. Select **Administrative Tools**.
4. Select **Services**.
5. Select the **Framework Manager** service.
6. Select **Stop**.

To start the Framework service, follow the above instructions and select **Start**.

Removing the Framework Manager

- “Linux Manager Uninstall” on page 15
- “Windows Manager Uninstall” on page 15

Linux Manager Uninstall

1 Enter the following command:

```
rpm -e netiq-npam
```

IMPORTANT

- To uninstall Privileged Account Manager that was upgraded from Privileged User Manager 2.3 or earlier version, run the following command:

  ```
  rpm -e novell-npum
  ```

- To uninstall Privileged Account Manager that was upgraded from Privileged User Manager 2.5 or earlier versions of 2.4, run the following command:

  ```
  rpm -e netiq-npum
  ```

- This action cannot be undone.

2 Delete the `/opt/netiq/npum` directory structure.

Deleting the directory structure removes the existing Framework Host settings from the server, allowing for clean re-installation.

NOTE: If you have upgraded to Privileged Account Manager 3.5 from an earlier version, run the following commands:

```
rm -rf /opt/novell/npum
unlink /opt/netiq/npum
```

Windows Manager Uninstall

1 Select the **Start** button from the Windows task bar.

2 Select **Control Panel**.

3 Select **Add or Remove Programs**.

4 Select **NetIQ Privileged Account Manager** and click **Remove**.

5 Delete the `C:\Program Files\netiq\npum` folder.

NOTE: If you have upgraded to Privileged Account Manager 3.5 from an earlier version, delete the `C:\Program Files\novell\npum` folder.

IMPORTANT: This action cannot be undone.

4 Installing the Agents

- "Agent Installation Overview" on page 17
- "Creating a Host Name for Each Agent (Optional)" on page 17
- "Opening Firewall Ports" on page 18
- "Installing and Registering a Framework Agent" on page 18
- "Removing the Agent Components" on page 23

Agent Installation Overview

For each computer that you want to manage with the Framework console, you need to do the following:

- "Creating a Host Name for Each Agent (Optional)" on page 17
- "Installing and Registering a Framework Agent" on page 18

Creating a Host Name for Each Agent (Optional)

The host name is created automatically when you register with framework manager. You can also create a host name for the agent using the following steps:

NOTE: Hosts can be organized and grouped into domains.

---

1. Log in to the Framework Manager console.
2. In the **Navigation Pane,** click **Hosts**.

   The **Navigation Pane** displays the current hierarchy for your Framework.
3. (Conditional) If you want to add a subdomain, click **Hosts** in the **Navigation Pane**.

   3a Click **Add Domain** in the **Task Pane**.

   3b Specify a domain name.

   3c Click **Finish**.
4. Select the required domain from the **Navigation Pane**.
5. Click **Add Hosts** from the **Task Pane**.
6. Specify the agent names for the hosts. You can type the names one at a time using one name per line, or paste a list of names.

   When you add a host to the Framework, the name does not need to relate to the existing DNS name used to locate the host on your network.
7. Click **Next**.

   A list of agent names is displayed.

8 Click **Finish**.

The status of the host is unregistered until the agent is installed and registered.

9 Continue with "Installing and Registering a Framework Agent" on page 18.

Opening Firewall Ports

Port 29120 is used for all communications among the Framework managers and the agents. Port 29120 is also used for communications among the Framework agents.

If firewalls separate your Privileged Account Manager machines, this port must be opened to traffic in both directions for NetIQ Privileged Account Manager to work properly.

The port is specified when the agent is registered with the Framework Manager. If you need to specify a different port because an application is already using port 29120, this new port needs to be opened in the firewall for communication.

Installing and Registering a Framework Agent

Currently the Framework Agent is available for installation on the platforms listed below. For more information about the supported platforms, see the System Requirements in PAM Documentation website.

For detailed installation instructions for your platform, select from the list below:

- "AIX Agent Install" on page 18
- "HP-UX Agent Install" on page 19
- "Linux Agent Installation" on page 20
- "Windows Agent Installation" on page 21
- "Solaris Agent Install" on page 22

NOTE: Agents must be registered with the Framework Manager after installation. For more information about the command used to registering an agent, see the section Registering an Agent in the Privileged Account Manager Administration Guide.

AIX Agent Install

The AIX installation package is compressed through gzip. In order to install the package, you must unzip the package through gunzip.

By default, the installation program installs the software into `/opt/netiq`. To change this, create a directory in the required part of the file system and create a symbolic link to `/opt/netiq`.

To install the AIX agent:

1 Copy the installation package to a temporary location and use the following command to extract the installation files:

```
gunzip <Installation package name>
```

2 After the AIX installation package is uncompressed, use one of the following methods to perform the installation.

- The AIX smitty program
- The following command:

```
installp -acgNQqwX -d <directory of .bff file> netiqnpam
```

3 When installation is complete, check that the service is running by viewing the log file.

The log file is located in `/opt/netiq/npum/logs/unifid.log`, if the default install location was used. If the agent installed correctly, it should be listening on 0.0.0.0:29120.

4 Use the following command to register the agent with the Framework Manager. This command must be issued from the machine where the agent is installed.

```
/opt/netiq/npum/sbin/unifi regclnt register
```

Four items of information are required:

The registration server hostname: The hostname or IP address of the Framework Manager.

The registration server port: Accept the default unless another application is using this port. After the host is registered, this port cannot be modified.

The name or IP address of this host: The DNS name or IP address by which any other agent in the Framework can resolve the location of this machine on your network.

The name of this agent: The name of the agent when it was created in the Framework Console (refer to "Creating a Host Name for Each Agent (Optional)" on page 17).

NOTE: When the above details have been provided, a valid username and password for the Framework Manager are required to complete the registration of the agent.

For more information about the command used to registering an agent, see the section Registering an Agent in the Privileged Account Manager Administration Guide.

5 Verify that the registration has been successful by viewing the host details on the Framework Console.

HP-UX Agent Install

The HP-UX installation package is compressed through gzip. In order to install the package, you must unzip the package through gunzip.

By default, the installation program installs the software into `/opt/netiq`. To change this, create a directory in the required part of the file system and create a symbolic link to `/opt/netiq`.

To install the HP-UX agent:

1 Copy the installation package to a temporary location and use the following command to extract the installation files:

```
gunzip <Installation package name>
```

2 After the HP-UX installation package is uncompressed, use the following command to install the agent:

```
swinstall -s /<directory of .depot file>/<filename>.depot \*
```

3 After installation is complete, check that the service is running by viewing the log file.

The log file is located in `/opt/netiq/npum/logs/unifid.log`, if the default install location was used. If the agent installed correctly, it should be listening on 0.0.0.0:29120.

4 Use the following command to register the agent with the Framework Manager. This command must be issued from the machine where the agent is installed.

```
/opt/netiq/npum/sbin/unifi regclnt register
```

Four items of information are required:

The registration server hostname: The hostname or IP address of the Framework Manager.

The registration server port: Accept the default unless another application is using this port. After the host is registered, this port cannot be modified.

The name or IP address of this host: The DNS name or IP address by which any other agent in the Framework can resolve the location of this machine on your network.

The name of this agent: The name of the agent when it was created in the Framework Console (refer to "Creating a Host Name for Each Agent (Optional)" on page 17).

NOTE: When the above details have been provided, a valid username and password for the Framework Manager are required to complete the registration of the agent.

For more information about the command used to registering an agent, see the section Registering an Agent in the Privileged Account Manager Administration Guide.

5 Verify that the registration has been successful by viewing the host details on the Framework Console.

Linux Agent Installation

Linux hosts use the RPM packaging system for installation, upgrade, and removal.

By default, the installation program installs the software into `/opt/netiq`. To change this, create a directory in the required part of the file system and create a symbolic link to `/opt/netiq`.

Prerequisites

- When you install PAM agent in SLES 12 or later, ensure that LSB (Linux Standard Base) version 3.0 or later is installed.
- If you want to use Enhanced Access Control feature, you must install 32bit `glibc` (GNU C Library) library in 64 bit RHEL agent.

To install the Linux agent:

1 Copy the installation package to a temporary location and use the following command to install the file:

```
rpm -i <installation package name>.rpm
```

2 After installation is complete, check that the service is running by viewing the log file.

The log file is located in `/opt/netiq/npum/logs/unifid.log`, if the default install location was used. If the agent installed correctly, it should be listening on 0.0.0.0:29120.

3 Use the following command to register the agent with the Framework Manager. This command must be issued from the machine where the agent is installed.

```
/opt/netiq/npum/sbin/unifi regclnt register
```

Four items of information are required:

The registration server hostname: The hostname or IP address of the Framework Manager.

The registration server port: Accept the default unless another application is using this port. After the host is registered, this port cannot be modified.

The name or IP address of this host: The DNS name or IP address by which any other agent in the Framework can resolve the location of this machine on your network.

The name of this agent: The name of the agent when it was created in the Framework Console (refer to "Creating a Host Name for Each Agent (Optional)" on page 17).

NOTE: When the above details have been provided, a valid username and password for the Framework Manager are required to complete the registration of the agent.

For more information about the command used to registering an agent, see the section Registering an Agent in the Privileged Account Manager Administration Guide.

4 Verify that the registration has been successful by viewing the host details on the Framework Console.

Windows Agent Installation

In Windows environment, you can install the agents in the following ways: Interactive installation and Silent installation. The silent or unattended installation is useful when you need to install the agent in more than one server.

1 (Conditional) **For interactive installation, perform the following:**

   1a Run the following install executable to start the installation:

   <Installation file name>.msi

   1b Follow the steps in the install wizard.

   The Agent service can be installed on any part of the normal file system. It defaults to the `C:\Program Files\Netiq\npum` folder.

2 (Conditional) **For silent installation, use the following command:**

   Syntax: `msiexec /i <Installer Filename> /passive`

   For more information about other `msiexec` command-line options, see Microsoft documentation.

3 After installation is complete, check that the service is running by viewing the log file.

   The log file is located in `C:\Program Files\Netiq\npum\logs\unifid.log`, if the default install location was used. If the agent installed correctly, services should be listening on 0.0.0.0:29120 and 0.0.0.0:443.

4 Run the following command to register the agent with the Framework Manager, from the machine where the agent is installed.

```
<install_path>/netiq/npum/bin/unifi.exe regclnt register
```

NOTE: Open `cmd.exe` with the **Run as administrator** option to run this command.

Four items of information are required:

The registration server hostname: The hostname or IP address of the Framework Manager.

The registration server port: Accept the default unless another application is using this port. After the host is registered, this port cannot be modified.

The name or IP address of this host: The DNS name or IP address by which any other agent in the Framework can resolve the location of this machine on your network.

The name of this agent: The name of the agent when it was created in the Framework Console (refer to "Creating a Host Name for Each Agent (Optional)" on page 17).

NOTE: When the above details have been provided, a valid username and password for the Framework Manager are required to complete the registration of the agent.

For more information about the command used to registering an agent, see the section Registering an Agent in the Privileged Account Manager Administration Guide.

5 If you have been supplied with a license, log in to the Framework Console and install the license.

For information, refer to "Accessing the Console" on page 12, and then "Downloading and Installing NetIQ Privileged Account Manager License" on page 13.

Solaris Agent Install

The Solaris installation package is compressed through gzip. In order to install the package, you must unzip the package through gunzip.

By default, the installation program installs the software into `/opt/netiq`. To change this, create a directory in the required part of the file system and create a symbolic link to `/opt/netiq`.

To install the Solaris agent:

1 Copy the installation package to a temporary location and use the following command to extract the installation files:

```
gunzip <Installation package name>
```

2 After the Solaris installation package is uncompressed, use the following command to install the agent:

```
pkgadd -d /<directory of .pkg file>/<installation package name>.pkg
```

3 After installation is complete, check that the service is running by viewing the log file.

The log file is located in `/opt/netiq/npum/logs/unifid.log`, if the default install location was used. If the agent installed correctly, it should be listening on 0.0.0.0:29120.

4 Use the following command to register the agent with the Framework Manager. This command must be issued from the machine where the agent is installed.

```
/opt/netiq/npum/sbin/unifi regclnt register
```

Four items of information are required:

The registration server hostname: The hostname or IP address of the Framework Manager.

The registration server port: Accept the default unless another application is using this port. After the host is registered, this port cannot be modified.

The name or IP address of this host: The DNS name or IP address by which any other agent in the Framework can resolve the location of this machine on your network.

The name of this agent: The name of the agent when it was created in the Framework Console (refer to "Creating a Host Name for Each Agent (Optional)" on page 17).

NOTE: When the above details have been provided, a valid username and password for the Framework Manager are required to complete the registration of the agent.

For more information about the command used to registering an agent, see the section Registering an Agent in the Privileged Account Manager Administration Guide.

5 Verify that the registration has been successful by viewing the host details on the Framework Console.

Removing the Agent Components

The following sections contains the instructions for uninstalling agents in different platforms:

- "AIX Agent Uninstall" on page 23
- "HP-UX Agent Uninstall" on page 23
- "Linux Agent Uninstall" on page 24
- "Solaris Agent Uninstall" on page 24
- "Windows Agent Uninstall" on page 25

AIX Agent Uninstall

1 Use one of the following methods:
   - The AIX smitty program
   - The following command:

     ```
     installp -u netiqnpam
     ```

IMPORTANT

- This action cannot be undone.

---

2 Delete the `/opt/netiq/npum` directory.

   Deleting the directory structure removes the existing Framework Host settings from the server, allowing for clean re-installation.

NOTE: If you have upgraded to Privileged Account Manager 3.5 from an earlier version, run the following commands:

```
rm -rf /opt/novell/npum
unlink /opt/netiq/npum
```

HP-UX Agent Uninstall

1 Enter the following command:

```
swremove netiq-npam
```

IMPORTANT

- This action cannot be undone.

2 Delete the `/opt/netiq/npum` directory structure.

Deleting the directory structure removes the existing Framework Host settings from the server, allowing for clean re-installation.

NOTE: If you have upgraded to Privileged Account Manager 3.5 from an earlier version, run the following commands:

```
rm -rf /opt/novell/npum
unlink /opt/netiq/npum
```

Linux Agent Uninstall

1 Enter the following command:

```
rpm -e netiq-npam
```

IMPORTANT

- This action cannot be undone.

2 Delete the `/opt/netiq/npum` directory structure.

Deleting the directory structure removes the existing Framework Host settings from the server, allowing for clean re-installation.

NOTE: If you have upgraded to Privileged Account Manager 3.5 from an earlier version, run the following commands:

```
rm -rf /opt/novell/npum
unlink /opt/netiq/npum
```

Solaris Agent Uninstall

1 Enter the following command:

```
pkgrm netiq-npam
```

IMPORTANT

- This action cannot be undone.

2 Delete the `/opt/netiq/npum` directory structure.

Deleting the directory structure removes the existing Framework Host settings from the server, allowing for clean re-installation.

NOTE: If you have upgraded to Privileged Account Manager 3.5 from an earlier version, run the following commands:

```
rm -rf /opt/novell/npum
unlink /opt/netiq/npum
```

Windows Agent Uninstall

Prerequisite

If you are planning to uninstall an agent that is used for application SSO, you must uninstall the `appsso` package before uninstalling the agent. For steps to uninstall a package, see Uninstalling Packages from a Host .

To uninstall an Agent:

1. Select the **Start** button from the Windows task bar.
2. Select **Control Panel**.
3. Select **Add or Remove Programs**.
4. Select **NetIQ Priviledged User Manager** and click **Remove**.
5. Delete the `C:\Program Files\netiq\npum` folder.

IMPORTANT: This action cannot be undone.

5 Configuring Application Single Sign-On

Privileged Account Manager allows you to grant privileged access to enterprise applications and enable single sign-on (SSO) to the application seamlessly using Application SSO. Application SSO improves security by hiding the application credentials from the application administrator. Using this feature, you can monitor the privileged session to enterprise applications without installing the PAM agent on the target computer while capturing the session activities in the form of keystrokes and video audits.

Using Application SSO, you can enable SSO to applications such as:

- Enterprise Applications (VMware server using vSphere client)
- Databases (Oracle using Toad)
- Windows Computers using RDP client.
- Linux or Unix Computers using PuTTY, WinSCP, and so on.
- Network Devices (HP switches, Cisco devices and so on using PuTTY)
- Web Applications (ESXi web client)

Application SSO Modes

You can configure Application SSO in the following modes:

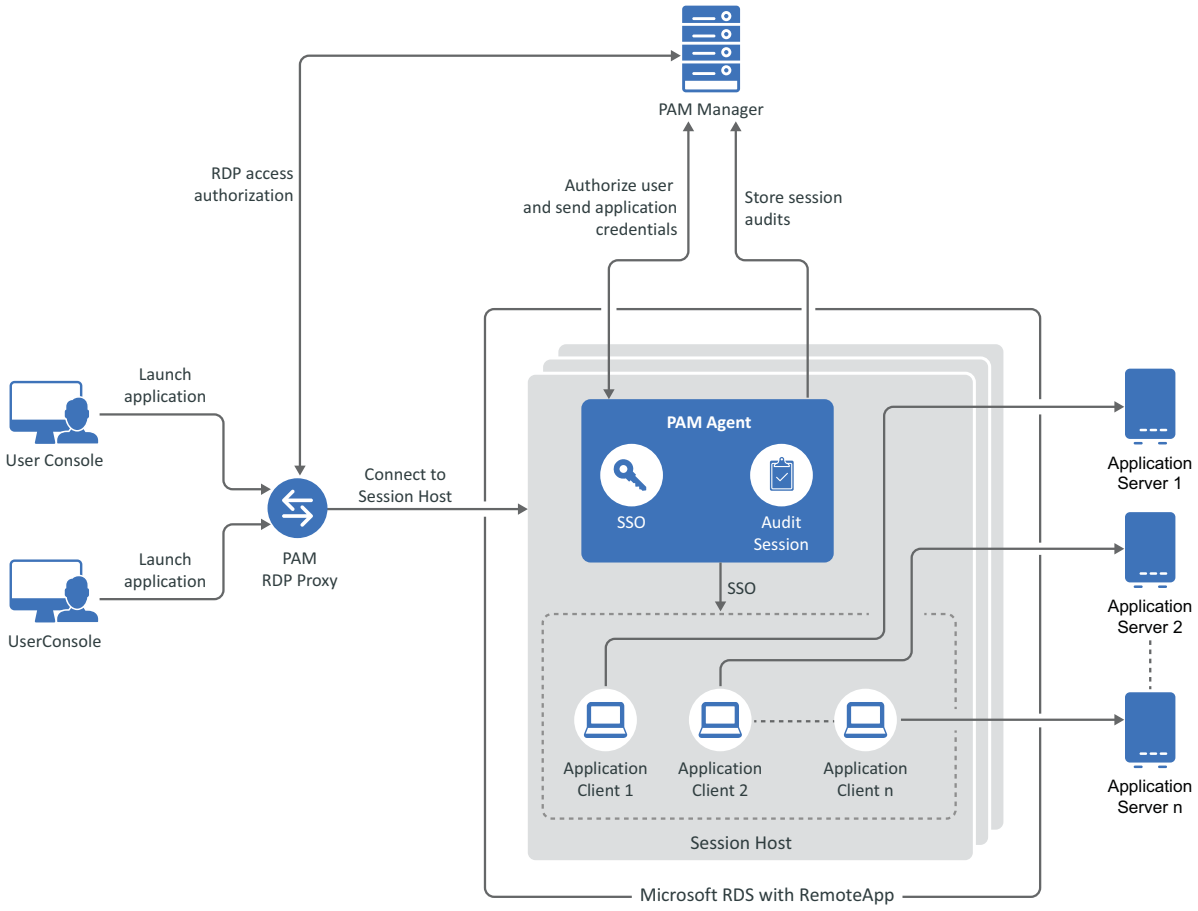
- RemoteApp Mode
- Direct Access Mode

You can configure either one or both of the modes as required.

RemoteApp Mode

In this mode, applications are published as Microsoft RemoteApps on a cluster of servers. The user can access these applications remotely using the PAM web portal (user console) and PAM performs SSO to the application. The user must launch a separate session for every application from the user console. This mode can be used when direct access to the server hosting the application is restricted.

The following illustration explains the working of Application SSO using RemoteApp:

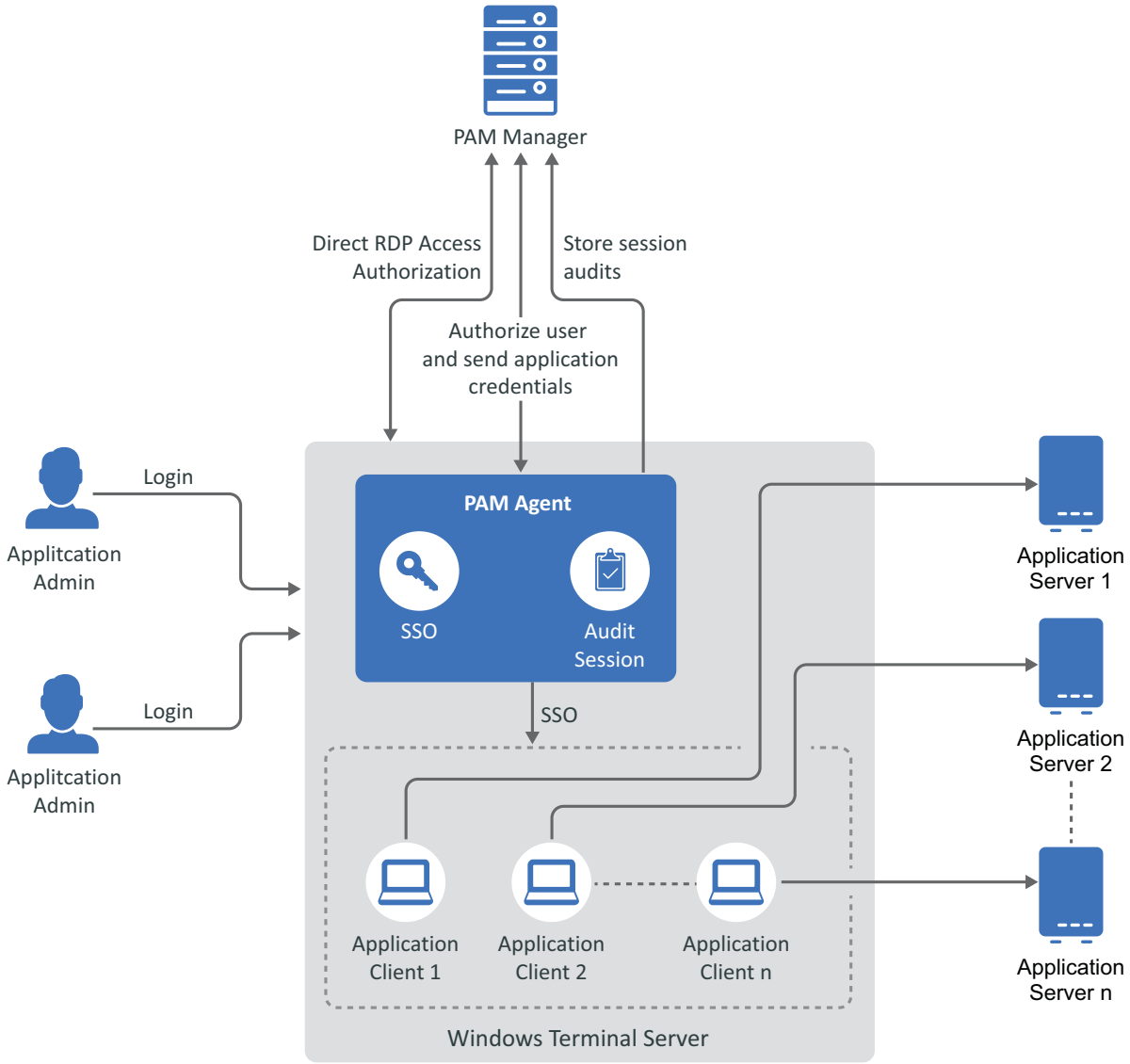


Direct Access Mode

In this mode, the application is installed on a remote server. The user can launch the application directly and PAM performs SSO using the SSO module installed on the remote server. The user will not experience any change in the way of accessing the application and the user can continue to use any native tool for RDP connection to the remote server.

In this mode, the user can launch multiple applications simultaneously in one session. This mode can be used when the server hosting the application is protected by firewall.

The following illustration explains the working of Application SSO using direct access mode:



Setting Up Application SSO

This section explains installation and configuration steps that must be performed to use the Application SSO feature:

- Prerequisites
- Disabling Task Manager Keyboard Shortcut Keys and Sticky Keys in Windows
- Installations for Application SSO
- Creating an Active Directory User
- Extending the Schema and Assigning User Rights
- Configuring Application SSO

Prerequisites

- Application SSO is an add-on option provided by PAM. To use this capability, you must purchase additional license. For more information please contact the NetIQ customer support.
- Review the platforms supported for Application SSO before installing. For information about the supported platforms, see the System Requirements in PAM Documentation website.

CAUTION: Ensure that you disable Sticky Keys and Keyboard Shortcut keys for Task Manager in Windows while configuring Remote Application SSO feature. For more information, see "Disabling Task Manager Keyboard Shortcut Keys and Sticky Keys in Windows" on page 30.

Disabling Task Manager Keyboard Shortcut Keys and Sticky Keys in Windows

You can disable Sticky keys using Group Policy or through Control Panel for Windows.

To disable the Keyboard Shortcut keys for Task Manager, you can use Group policy or one of the following methods:

1. Access the Windows Registry by typing `regedit` in the Windows search box on the taskbar and press `Enter`.
2. Go to `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System`.
3. Create a new `DWORD(32-bit)` value with `Name` as `DisableTaskMgr` and `Data` value as `1`.

To disable the use of Keyboard Shortcut Keys for Task Manager, using a script, follow the below procedure:

1. Copy the following text in a notepad:

   ```
   Windows Registry Editor Version
   5.00[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
   "DisableTaskMgr"=dword:00000001
   ```

2. Save the file with a `.reg` extension.

   For example:

   `DisableCtrlShiftEscape.reg`

3. In a different notepad, copy `REGEDIT /s \\servername\share\filename.reg`. Replace the `servername`, `share`, and `reg` file information appropriately.
4. Save the file with a `.bat` extension.
5. Double-click on the saved batch file and the registry key will be imported.
6. Verify the procedure by entering the key combination **Ctrl + Shift + Esc**.

Installations for Application SSO

- Installations for RemoteApp Mode
- Installations for Direct Access Mode

Installations for RemoteApp Mode

- Install the following Remote Desktop (RD) role services in the domain:
  - RD Connection Broker
  - RD Gateway
  - RD Licensing
  - RD Session Host

  For more information about installing the remote desktop role services, see the Microsoft documentation.
- Install the applications for which you want to allow SSO in all the session hosts.

  Ensure that all the session hosts and applications used for Application SSO are part of the same RD session collection. For more information about configuring the RD session collection, see the Microsoft documentation.
- Install the PAM agent on all the session hosts that will be used for Application SSO and register the agent with PAM. These are the Application SSO agents.

  For more information about installing and registering the agent, see Installing and Registering a Framework Agent .

Installations for Direct Access Mode

- Install the PAM agent on all the remote Windows servers that will be used for Application SSO and register the agent with PAM. These are the Application SSO agents.

  For more information about installing and registering the agent, see Installing and Registering a Framework Agent .
- Install the applications for which you want to allow SSO on all the remote Windows servers.
- You must get appropriate Windows terminal license for the remote Windows server based on the number of concurrent connections to the server.

Creating an Active Directory User

PAM uses a service account to perform SSO to the target enterprise application. You must create this account as a domain user and add this account to the domain admins group of the Active Directory.

If you are using RemoteApp mode, ensure that the user has privileges to publish the remoteapp.

Extending the Schema and Assigning User Rights

Privileged Account Manager requires Active Directory (AD) or Active Directory Lightweight Directory Service (AD LDS) to store Application SSO scripts. To store the Application SSO script, you must extend the AD or the AD LDS schema. After extending the schema, you must assign user rights to these AD or AD LDS objects to allow the AD user created for SSO to update these objects.

- Extending the AD Schema and Assigning User Rights
- Extending the AD LDS Schema and Assigning User Rights

Extending the AD Schema and Assigning User Rights

1. Log in to any server in the domain as a domain administrator.
2. Copy `\Utilities\Schema_Extension_Utility\ADS` folder from the PAM ISO to the server.
3. To extend the AD Schema:
   - **3a** Run the `ADS\adSchema.exe` file.
   - **3b** Select **Extend Active Directory Schema**.
   - **3c** Click **OK**.

   For more information about extending the AD schema, see Extending the Active Directory Schema section in the NetIQ SecureLogin Installation Guide.
4. To assign user rights to the newly added AD objects:
   - **4a** Run the `ADS\adSchema.exe` file.
   - **4b** Select **Assign User Rights** and click **OK**.
   - **4c** (Conditional) If you have configured secure LDAP(LDAPS) for Active Directory, you must select **AES Encryption**.
   - **4d** (Conditional) If you have configured LDAP for Active Directory, you must deselect **AES Encryption**
   - **4e** Specify the AD user that is created for SSO.

     For example, if `ssouser` is the user created for SSO, then you must specify `cn=ssouser, cn=user, dc=machine, dc=com`.
   - **4f** Click **OK**.

     For more information about assigning user rights to AD objects, see Extending the Active Directory Schema section in the NetIQ SecureLogin Installation Guide.

Extending the AD LDS Schema and Assigning User Rights

1. Log into the AD LDS server as a domain administrator.
2. Copy `\Utilities\Schema_Extension_Utility\ADAM` from the PAM ISO to the server.
3. Run the `ADAM\AdamConfig.exe` file and follow the on-screen prompts to extend the AD LDS schema.

   For more information about extending the AD LDS schema, see Extending the Schema by Using ADAM Configuration Wizard section in the NetIQ SecureLogin Installation Guide.

4 Run the `ADAM\SyncAdam.cmd` file to synchronize AD data with AD LDS instance.

For more information about synchronizing AD and AD LDS instances, see Synchronizing Data from Active Directory to an ADAM Instance section in the NetIQ SecureLogin Installation Guide.

Configuring Application SSO

- Create an SSO Credential Vault
- Configuring Installation Attributes
- Installing Application SSO Package
- Configuring the Passphrase
- Configuring Application SSO Scripts
- Configuring the User Preference
- Installing Certificates

Create an SSO Credential Vault

You must create a credential vault for the AD and add the AD user that is created for SSO.

For more information about creating a credential vault and adding credentials, see the Contextual Help of Credential Vault.

Configuring Installation Attributes

You must configure the following installation attributes before installing AppSS0 package:

1 Log in to the PAM administration console.

2 Click **Hosts > Application SSO**.

3 Select the following:

- **Install Mode:**

  Select **Microsoft Active Directory (AD)**, if you are using AD to store Application SSO scripts.

  Select **Microsoft Active Directory Lightweight Directory Services (AD LDS)**, if you are using AD LDS to store Application SSO scripts.

- **Enable SSO to JAVA Applications:** Select this option when you want to enable SSO to Java applications.

  If you are enabling SSO to JAVA applications, ensure that JRE1.7 or later is installed in the Application SSO agent.

- **Account Domain:** Select the appropriate credential vault.
- **Credential:** Select the AD user created for SSO.

4 Click **Finish**.

Installing Application SSO Package

You must install the appsso package on all the servers that are used for Application SSO. The first server on which you install the appsso package becomes the primary Application SSO agent. The primary Application SSO agents contains the SecureLogin Manager component.

NOTE: Installing AppSSO package requires computer reboot at several stages of the installation. You must plan for a downtime before installing AppSSO package.

To install appsso package:

1. Add the appsso package to the package manager.

   For steps to download and add packages to the package manager, see Publishing Packages on the Package Manager.

2. Install appsso on all the Application SSO agents.

   For more information about installing a package on the Application SSO agent, see the Installing Packages on a Host section of the Privileged Account Manager Administration Guide.

Configuring the Passphrase

Passphrases are unique question and answer combinations created to verify and authenticate the identity of a user. Passphrases protect user credentials from unauthorized use. For more information about passphrase, see the Setting Up a PassPhrase section in the NetIQ SecureLogin Installation Guide.

To setup the passphrase:

1. Log into the primary Application SSO agent as a domain administrator.
2. Launch SecureLogin.
3. In the Passphrase Setup dialog box, specify the required details.
4. Click **OK**.

Configuring Application SSO Scripts

Application SSO scripts are used to identify the application authentication fields for SSO. PAM provides sample scripts for a few applications that you can import easily. In addition, you can also create application SSO scripts for any enterprise application using the wizard provided by PAM.

- Importing Application SSO Scripts
- Creating Application SSO Scripts

Importing Application SSO Scripts

PAM provides sample application scripts for a few applications that you can import. After importing these scripts, you must assign these scripts to the AD user created for SSO.

To import application SSO scripts and assign scripts to the AD user created for SSO:

1. Log into the primary Application SSO agent as a domain administrator.

2 Copy the sample SSO scripts `Sample_Scripts\SSO\SSO_Sample_Scripts.xml` from the PAM ISO to the Application SSO agent.

3 Launch SecureLogin.

4 Launch SecureLogin Manager.

5 Expand the domain.

6 Expand the appropriate organizational unit (OU), then select the AD user created for SSO.

7 Select **Distribution > Load > OK**.

8 Select **All Files (*.*)**, then select the appropriate XML file for importing the SSO script.

9 Click **Open**.

10 Click **Yes** in the warning message to upgrade the datastore version.

11 Click **Ok**.

For more information about importing Application SSO scripts, see the Exporting and Importing Predefined Applications and Application Definitions section of the NetIQ SecureLogin Application Definition Guide.

Creating Application SSO Scripts

If you do not have a script for an application, you can create the Application SSO script using the wizard provided by PAM. After creating the script, you must assign the script to the AD user created for SSO.

To create an Application SSO script and assign script to the AD user created for SSO:

1 Log into the primary Application SSO agent as a domain administrator.

2 Launch SecureLogin.

3 **Creating an Application SSO script:**

   3a Launch the application for which you need to create the Application SSO script.

   3b Click the notification that appears in the system tray and select **Yes, I want to single sign enable the screen using the wizard**.

   3c Follow the on screen prompts to create the Application SSO script and click **Apply**.

   For more information about creating an Application SSO script using the wizard, see the Using Application Definition Wizard section of the NetIQ SecureLogin Application Definition Wizard Administration Guide.

   3d Double-click the SecureLogin icon in the notification area.

   3e Click **Applications** and double-click the required application.

   3f Click **Definition > Convert to Application Definition**

   3g Specify `SetRestPlat -method "PAM"` before the command to include credentials. For some applications, such as Remote Desktop Connections, you must provide the host name, port, and then you must provide the login credentials. In such scenario, you must include `SetRestPlat -method "PAM"` command for every dialog box.

   For example,

```
SetRestPlat -method "PAM"
Type #21 $host
Type #22 $port

SetRestPlat -method "PAM"
Type #40 $username
Type #44 $password
```

For more information about editing Application SSO scripts, see the Modifying Predefined Applications and Application Definitions section of the NetIQ SecureLogin Application Definition Guide.

3h Click **OK**.

4 **Assigning the Application SSO scripts to the AD user created for SSO**:

4a Launch SecureLogin Manager.

4b Click **Distribution > Copy.**

4c Specify the AD user object created for SSO in the **Destination Object**. For example, if the AD user is `ssouser`, you must specify the user object as `CN=ssouser,CN=Users,DC=mycompany,DC=com`.

4d Click **OK** and select the application scripts that must be copied.

4e Click **OK**.

Configuring the User Preference

After creating Application SSO scripts, you must modify the following user preferences to improve security.

To modify the user preference:

1 Log in to the primary Application SSO agent as a domain administrator.

2 Launch SecureLogin.

3 Launch SecureLogin Manager.

4 Expand the domain.

5 Expand the appropriate organizational unit (OU), then select the AD user created for SSO.

6 Select **Preferences** and set the value as follows:

- Set **Display splash screen on startup** to **No**.
- Set **Display system tray icon** to **No**.
- Set **Wizard Mode** to **Disabled**.
- Set **Enable passphrase security system** to **Hidden**.

7 Click **OK**.

8 Log out and Log in to the same server as a domain administrator.

9 Launch SecureLogin.

10 Click **Ok** on the SecureLogin message to accept the passphrase preference changes.

Installing Certificates

You must secure the communication between the Application SSO agent and PAM manager by installing the SSL certificates.

You can use one of the following SSL certificates:

- Certificate Authority (CA) Signed Certificates
- Self-Signed Certificate
- Verifying and Installing LDAP Certificate Authority Certificates

Certificate Authority (CA) Signed Certificates

For the CA signed certificate, you can create the certificate signing request from PAM, get it signed from a CA, and install the certificate.

To install CA signed certificate, perform the following:

1. Create a certificate signing request for PAM administrator console.

   If you have multiple PAM administration console, you must create certificate signing request from all the consoles. For steps to create certificate signing request, see Requesting a Certificate for the Framework Manager Console.
2. Get all PAM administration console certificate signed by your CA.
3. Install the CA signed certificate in all PAM administration consoles. For steps to install the CA signed certificates in your administration console, see Installing a Certificate .
4. Install the CA signed certificate as a trusted root CA on all the Application SSO agents.

Self-Signed Certificate

To install the self-signed certificate, perform the following:

1. Launch the PAM administration console.
2. Get the self-signed certificate from the HTTP header of the administration console.
3. Install the self-signed certificate as a trusted root CA on all the Application SSO agents.

   If you have multiple PAM administration console, you must get the self-signed certificate from all the administration console. You must install all the self-signed certificates on all the hosts used for Application SSO.

Verifying and Installing LDAP Certificate Authority Certificates

A check box is added in the user interface to enable or disable certification verification for LDAP Credential vaults. If you enable certification verification, you must perform the following steps.

Linux Manager

1. Place the LDAP CA certificate in the `/etc/ssl/certs/` folder.
2. Enter the command `c_rehash`.
3. Restart Privileged Account Manager service using `/etc/init.d/npum restart` command.

Windows Manager

1 Add the LDAP CA certificate to the Trusted Root List. You can do this by following the below steps:

   1a Right-click on the cert format certificate.

   1b Run Install Certificate and follow the subsequent steps to add it to Computer level trusted root list.

   NOTE: You can also run the certificate management tool **mmc** > **Add the Certificates Snapin** or `Certim.msc`. Import the CA certificate into the trusted tool certificate list.

SLES

Enter `update-ca-certificates` command. The directory of CA certificates trust anchors used by administrators is `/etc/pki/trust/anchors`

RHEL

To add a certificate in PEM or DER file format to the CA trusted list on the system:

1 Add the certificate as a new file to `/etc/pki/ca-trust/source/anchors/` directory.

2 Run `update-ca-trust` extract.

Configuring Application SSO Credential Vault and Rule

After setting up Application SSO, you must configure appropriate Application SSO credential vault and rules in the administration console to grant Application SSO access to any user. For information about configuring Application SSO, see Privileged Single Sign-On in the Privileged Account Manager Administration Guide.

6 Configuring Privileged Account Manager

This chapter provides instructions for configuring Privileged Account Manager.

- "Enabling FIPS Mode" on page 39
- "Disabling CBC Mode" on page 40

Enabling FIPS Mode

PAM offers enhanced protection against security threats and compliance with United States federal government standards by supporting Federal Information Processing Standards (FIPS). PAM leverages the FIPS 140-2 compliant features to meet the security requirements of United States federal agencies and customers with highly secure environments. Enabling FIPS mode in Privileged Account Manager allows the product components such as PAM Manager, PAM Agent, PAM Administration Console, PAM User Console, and target applications to communicate using FIPS 140-2 certified encryption algorithms.

IMPORTANT

- You cannot disable FIPS after you have enabled it.
- When you enable FIPS:
  - FIPS mode is enabled immediately on all the managers that have the **registry** module.
  - The primary registry manager is enabled first, followed by the other registry managers, and then the associated agents. Automatic re-registration of agents happens once in two days. Therefore, it may take up to two days for FIPS to be enabled automatically on all the agents because FIPS is enabled when agents re-register with a manager.
  - For agents in **Offline** state, FIPS will be enabled only after the status changes to **Online** and the agents are re-registered with the manager.

Prerequisites:

- Ensure that all the packages are upgraded to the latest version on all PAM agents and managers.
- Enable FIPS on the operating systems hosting the managers and the agents.

  FIPS mode in PAM can be enabled only on Windows and Linux operating systems, for both managers and agents. FIPS mode in PAM is not supported on Unix operating systems. For a complete list of the supported Windows and Linux operating systems, see Privileged Account Manager 3.7 System Requirements and Sizing Guidelines.

To enable FIPS:

1. Enable FIPS on PAM:
   - **1a** Log in to the PAM Administration Console.
   - **1b** Click **Hosts** > **Host Status** > **Enable**.
   - **1c** (Conditional) To enable FIPS immediately on agents, re-register agents manually. For more information about re-registering agents manually, see the Privileged Account Manager Administration Guide.
2. Enable FIPS on the target machines for the following:
   - (Conditional) RDP relay
   - (Conditional) Credential checkout of applications and databases: Enable FIPS mode on Java that is installed on the system hosting the application.

Disabling CBC Mode

In PAM, Cipher Block Chaining (CBC) mode is enabled by default. Disabling this mode in PAM, ensures CBC mode is not used for communication by product components such as PAM Manager, PAM Agent, PAM Administration Console, PAM User Console, and target applications.

IMPORTANT:

- When you disable CBC Mode:
  - It is disabled immediately on all the managers that have the **registry** module.
  - The primary registry manager is disabled first, followed by the other registry managers, and then the associated agents. Automatic re-registration of agents happens once in two days. Therefore, it may take up to two days for CBC Mode to be disabled automatically on all the agents.
  - For agents in **Offline** state, CBC Mode will be disabled only after the status changes to **Online** and the agents are re-registered with the manager.

Prerequisites:

- Ensure that all the packages are upgraded to the latest version on all PAM agents and managers.

To disable CBC mode:

1. Log in to the PAM Administration Console.
2. Click **Hosts** > **Host Status**, and then click **Disable** next to **CBC Mode**.
3. (Conditional) To disable CBC mode immediately on agents, re-register agents manually. For more information about re-registering agents manually, see the Privileged Account Manager Administration Guide.

7 Upgrading Privileged Account Manager

For instructions to upgrade Privileged Account Manager see Upgrading Privileged Account Manager.