Privileged Account Manager

Installation Guide

December 2020

Legal Notice

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

Contents

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.
- **Users:** 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.
- **Reports:** 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.
- **Access Control:** The Access Control feature provides a user's controlled access to privileged commands in a secure manner across the enterprise. You can view and manage Users using Assignments, User Roles, Resource Pools, and other Configuration settings.
- **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.
- **Requests:** 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 17.
2. When the installation has completed, access and log in to the console. See “Accessing the Console” on page 18.
3. Install the Privileged Account Manager license. See “Downloading and Installing NetIQ Privileged Account Manager License” on page 19.

   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 Package Manager Permissions.
5. Install and register a Framework Agent on the computers that you want to manage. See Chapter 4, “Installing the Agents,” on page 23.

   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*.

Viewing the Version and the License Details

A framework user who has access to Administration console can verify the version and the license details of the installed Privileged Account Manager from the Administration console. To view the version and license details, the framework user must perform the following on the Administration console:

1. On the Navigation bar, Click ***admin*** **> About**.

   Here, *admin* is the user name of the framework user who is part of default admin group or who has the **admin** role on the unifi module in the Administrator console. For more information about the framework user role, see Configuring Permissions .
2. For License registration, click **Register Framework >** specify the license **> Finish**.
3. Click **Show License Summary** to view the number of each managed system that are being used through Privileged Account Manager, and the total license count.

   For more information about viewing the license summary and generating detailed report see, “License Summary” on page 8.

License Summary

The License Summary page includes the following information:

- The count for each managed end-points
- Total count of the managed end-points
- Time and date when the summary was last updated
- Option to download the detailed license report
- Option to update the license summary to view the latest license summary

For more information about the Privileged Account Manager license, see the Privileged Account Manager EULA in the Privileged Account Manager documentation website.

Managed End Point Type

The license count is based on the following type of managed end-points:

- **Agents:** This displays the number of all the Host servers that are added in the Hosts console and the agents that are registered in the framework.
- **Databases:** This displays the number of databases that are managed or accessed through Privileged Account Manager. This count is inclusive of all the database connectors that are configured for database monitoring and all the resources of type **Database** in **Credential Vault** for credential checkout/ checkin.
- **Applications:** This displays the number of applications that are managed or accessed through Privileged Account Manager for the password checkin/ checkout feature. This count includes all the resources of type **Applications** that are configured in **Credential Vault**.
- **SSH hosts:** This displays the number of SSH servers that are managed though for SSH relay. This count includes the resources of type **SSH** that are configured in **Credential Vault**.

Update License Summary

When you click **Update License Summary**, Privileged Account Manager deletes the previous license summary and updates the latest license summary. If you want to back up the previous license summary, you can download the license report by clicking **Download Detailed Report** before updating the summary.

The date and time when the existing license summary was generated is displayed at the bottom left corner of the License Summary page.

Download Detailed Report

To view and save the detailed report of the managed end-points that are displayed in the license summary page, click **Download Detailed Report**. The detailed report includes the following:

- Type of managed end-points.
- DNS or IP address of the managed end-points.
- Sub-type of the managed end-points.

  The sub-types can be as following:

  - Agent for all Agents
  - Local for SSH
  - The name of the application for Application
  - The name of the database for Database
- Name of hosts or servers associated with each managed end-point.

  The name can be as following:

  - Configured name for Agent

- The configured resource name for SSH and Application
- <*hostname*>:<*port*> for Database

License Acknowledgements

libjpeg-turbo - BSD 3-clause license

This software is based in part on the work of the Independent JPEG Group.

2 Planning Your Privileged Account Manager Installation

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

	Tasks	See
❑	Ensure that the computers on which you want to install Privileged Account Manager components meet the specified requirements.	Privileged Account Manager 4.0 System Requirements and Sizing Guidelines
❑	Install the Framework manager.	Chapter 3, “Installing the Framework Manager,” on page 17
❑	Install the agents.	Chapter 4, “Installing the Agents,” on page 23
❑	Configure Privileged Account Manager.	Chapter 6, “Configuring Privileged Account Manager,” on page 43
❑	Select the Agent and Agent less options as per your environment and requirement.	Agent and Agentless Capabilities in Privileged Account Manager - Tabular Overview

High Availability

The high availability or failover feature works by using a hierarchical view of the hosts associated with the Framework.

The hierarchy of hosts is created by using the Hosts console to group hosts into domains and subdomains, which are representative of your enterprise network structure. This effectively gives them a chain of command, where they always address requests to managers in their immediate subdomain before moving along a branch to another subdomain or parent domain.

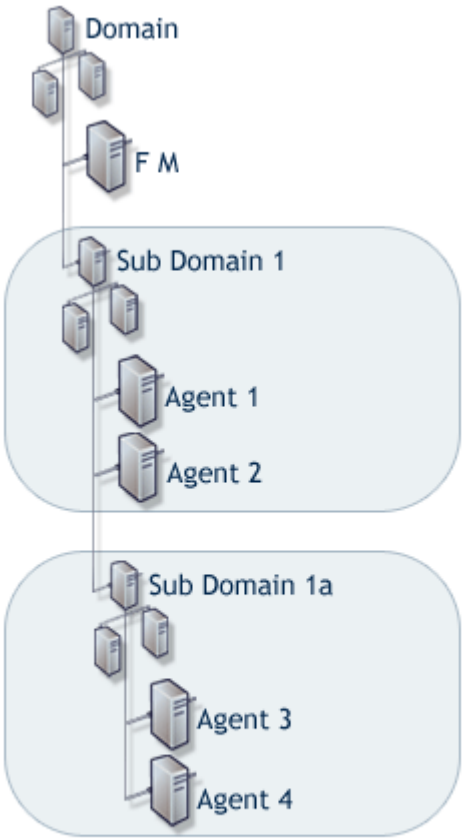
To achieve an effective failover environment, at least two Framework Manager packages must be deployed across the same Framework. The licensing model is not based on how many managers or agents are deployed, but how many hosts the Framework is deployed on. This means that there are no restrictions on how many Framework Manager packages you can deploy.

The Registry Manager controls a database that records the location and status of each package deployed on each of the hosts within the Framework. A copy of this information is held at each host by the Registry Agent package that is included as part of the agent installation. The distributed information is used to calculate the route to the appropriate manager for requests from any agent registered on the Framework. The structure of the registry data enables each host to determine

which Framework Manager on the Framework should be the target of requests, and which Framework Manager to use if there is a failure or withdrawal of the initially selected Framework Manager.

The failover feature automatically and transparently redirects requests from a failed or withdrawn Framework Manager to the next available manager of the same type. The agent automatically connects to a manager that is next in line in accordance with your defined hierarchy.

Table 2-1 *Creating a Failover Environment*



This diagram shows an example of a typical way to create an effective failover environment.

Deployment: Deploy the Command Control Manager package on the Framework Manager, Agent 1, and Agent 3 hosts.

Who authenticates to whom: By default, each agent contacts the following host for Command Control authorization:

Agent 1 and 2 contact Agent 1.
Agent 3 and 4 contact Agent 3.

Examples:

1. Agent 3 is downed for maintenance. Agent 4 seeks authorization from Agent 1.
2. Agent 1 is also downed because of a broken network card. Agents 2, 3, and 4 seek authorization from the Framework Manager.
3. The Command Control Manager package is removed from the Framework Manager and the Agent 1 is still broken. Agents 2, 3, and 4 seek authorization from Agent 3, considering Agent 3 is up and Agent 1 is still broken.

IMPORTANT: If an additional subdomain is added, agents under Subdomain 1 and 1a then seek authorization from the new Subdomain if no other Command Control Manager is available.

Configuring High Availability

To configure high availability, you must do the following:

- Install and register the agents to the manager.
- Define the domain.
- (Conditional) Promote the backup manager when primary fails. To write configuration changes, you must first try to get the primary up again. If you are unable to get the primary up again, you can promote the backup manager.

To configure high availability:

1. Install and register the PAM managers:
   - **1a** Install a PAM manager.

     The first manager you install is defined as the primary manager by default, and its packages are defined as primary. Manager packages on all other manager hosts act as backups.
   - **1b** Install another Privileged Account Manager manager.

     For more information about installing Privileged Account Manager managers, see Installing the Framework Manager in the Privileged Account Manager Installation Guide.
   - **1c** Register the second PAM manager you installed to the Privileged Account Manager instance you installed first. After you register, the second PAM manager acts as a backup manager.
2. To define the domain:
   - **2a** Login to Privileged Account Manager administrator console.
   - **2b** On the home page of the console, click **Hosts** > **Add Domain**.
   - **2c** Specify a domain name.
   - **2d** Click **Add**.
   - **2e** To add managers and agents to the domain, drag and drop the managers and agents from the list to the domain.

     You can have multiple domains in Privileged Account Manager. If you have multiple domains, you can add a backup manager in every domain. So, any request from the agent can be processed by the manager in their domain.
3. (Conditional) To promote a backup when the primary fails:
   - **3a** Select a host from **Hosts**.
   - **3b** Click **Packages**.

     The **Status** column indicates whether the status of a module is primary or backup.
   - **3c** To promote a backup manager:
     - **3c1** Ensure that the registry manager package is promoted to primary.
     - **3c2** Select the required backup packages and click **Promote Manager**.

Load Balancing

The load balancing feature work by using a hierarchical view of the hosts associated with the Framework.

The hierarchy of hosts is created by using the Hosts console to group hosts into domains and subdomains, which are representative of your enterprise network structure. This effectively gives them a chain of command, where they always address requests to managers in their immediate subdomain before moving along a branch to another subdomain or parent domain.

To achieve an effective load balancing environment, at least two Framework Manager packages must be deployed across the same Framework. The licensing model is not based on how many managers or agents are deployed, but how many hosts the Framework is deployed on. This means that there are no restrictions on how many Framework Manager packages you can deploy.

The Registry Manager controls a database that records the location and status of each package deployed on each of the hosts within the Framework. A copy of this information is held at each host by the Registry Agent package that is included as part of the agent installation. The distributed information is used to calculate the route to the appropriate manager for requests from any agent registered on the Framework. The structure of the registry data enables each host to determine which Framework Manager on the Framework should be the target of requests, and which Framework Manager to use if there is a failure or withdrawal of the initially selected Framework Manager.

Load balancing means the ability to evenly distribute processing and communications activity across the Framework so that no single Framework Manager is overwhelmed by agent requests.

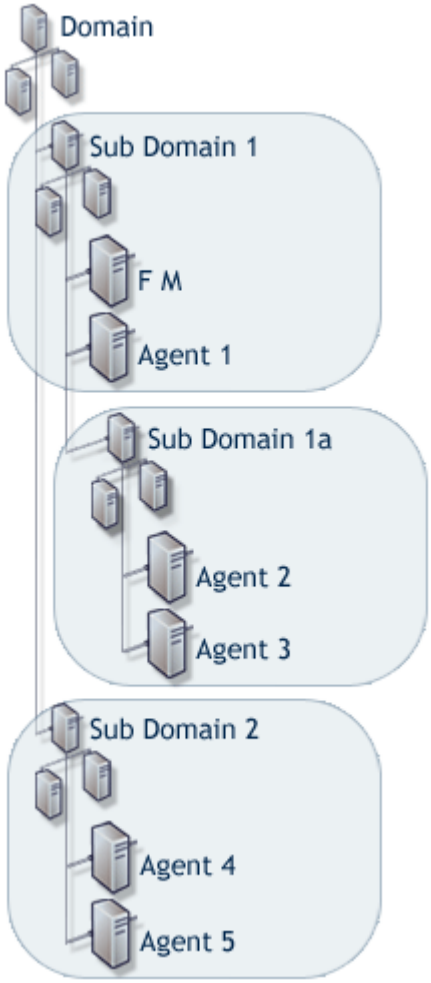
Load balancing is particularly important in situations where it is difficult to predict the number of requests that are directed to a specific category of manager.

The Framework automatically replicates data from the defined primary manager to each additional manager that is deployed in the Framework. Replication takes place automatically when the manager is initially deployed and then again at any stage when the data on the primary manager is modified.

The following packages can be load balanced:

- **Registry Manager:** Maintains a database of all hosts and modules and provides certificate-based registration features for the hosts.
- **Package Manager:** Manages a repository for packages.
- **Administration Agent:** Provides the functionality for the Web-based user interface. Consoles can be installed on the Administration Agent and used to control product features.
- **Access Manager:** Maintains a list of Framework user accounts and provides authentication services for the Framework. This package must be installed with a local Registry Manager in order to create a secure user authentication token.
- **Command Control Manager:** Maintains a database of all defined command control rules, commands, and scripts.

Table 2-2 *Creating a Load Balancing Environment*



This diagram is an example of a typical way to create an effective load-balanced environment.

Deployment: Deploy the Command Control Manager package on the Framework Manager, Agent 2, and Agent 4.

Who authenticates to whom: By default, each agent contacts the following host for Command Control authorization:

Agent 1 contacts the Framework Manager.

Agents 2 and 3 contact Agent 2.

Agents 4 and 5 contact Agent 4.

Example of load balancing working with failover:

1. Agent 2 is downed for maintenance. Agent 3 seeks authorization from the Framework Manager.
2. Agent 4 is down because of a broken network card. Agents 5 seeks authorization from the Framework Manager.

3 Installing the Framework Manager

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 Privileged Account Manager 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

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 18, and then "Downloading and Installing NetIQ Privileged Account Manager License" on page 19.

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 18, and then "Downloading and Installing NetIQ Privileged Account Manager License" on page 19.

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 19.

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 Permissions
- Chapter 4, “Installing the Agents,” on page 23

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 20
- “Windows” on page 20

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 21
- “Windows Manager Uninstall” on page 21

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

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 23
- "Installing and Registering a Framework Agent" on page 24

NOTE: For information about Agent and Agent-less capabilities, see

---

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 24.

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 Privileged Account Manager Documentation website.

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

- "AIX Agent Install" on page 24
- "HP-UX Agent Install" on page 25
- "Linux Agent Installation" on page 26
- "Windows Agent Installation" on page 27
- "Solaris Agent Install" on page 28

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 23).

   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 23).

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 Privileged Account Manager 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 23).

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 23).

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 18, and then "Downloading and Installing NetIQ Privileged Account Manager License" on page 19.

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 23).

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

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 Privileged Account Manager 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:

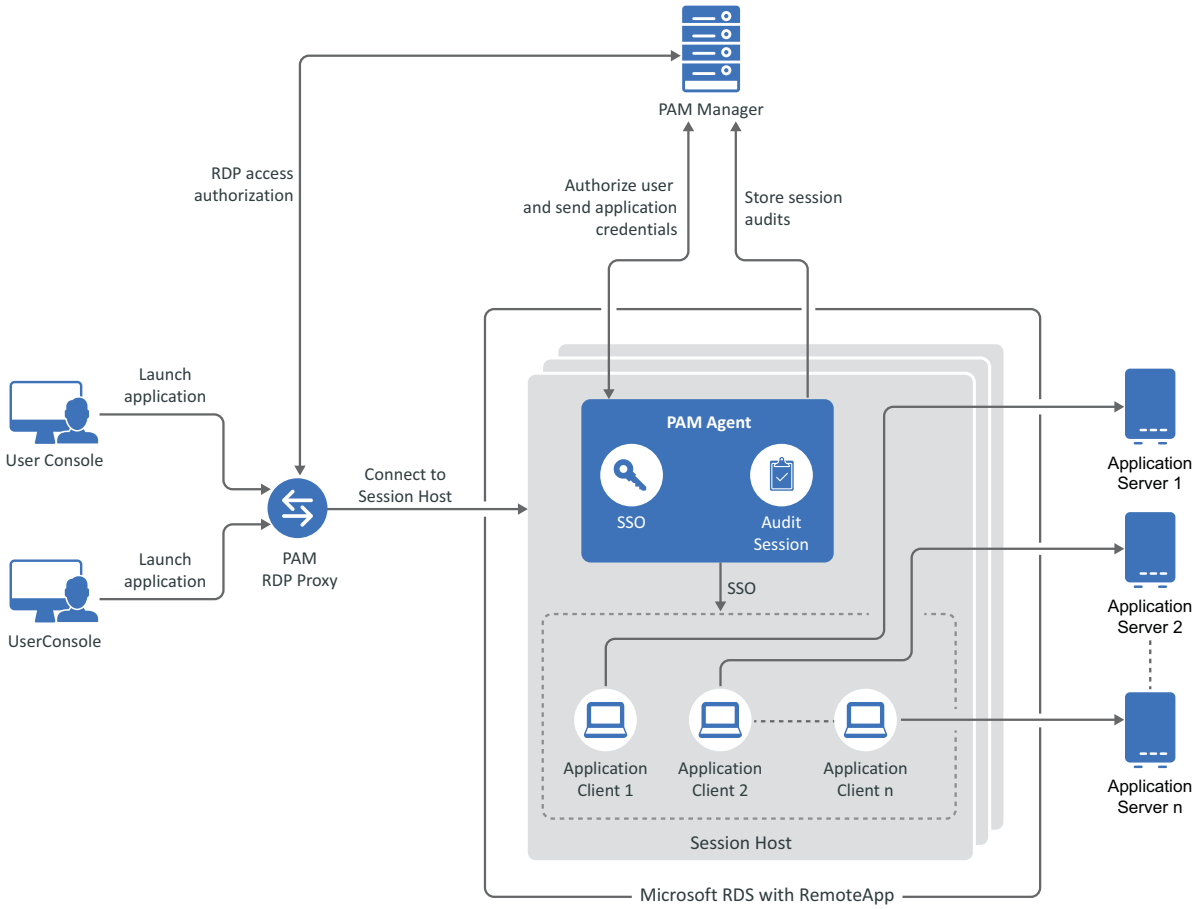
- RemoteApp Mode
- Direct Access Mode

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 Privileged Account Manager web portal (user console) and Privileged Account ManagerPrivileged Account Manager 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:

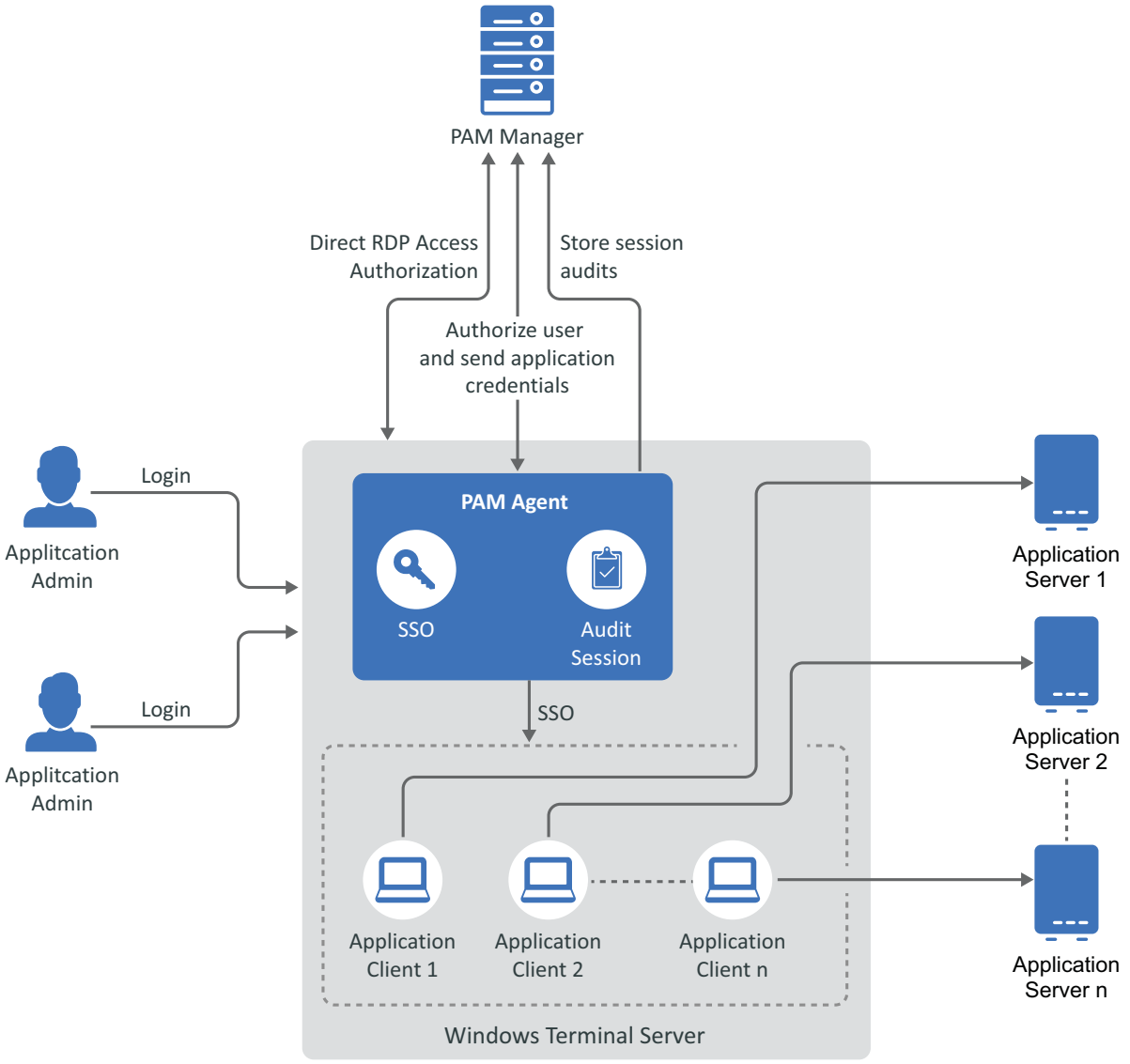


Direct Access Mode

In this mode, the application is installed on a remote server. The user can launch the application directly and Privileged Account Manager 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
- 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 Privileged Account Manager. 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 Privileged Account Manager Documentation website.

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 Privileged Account Manager agent on all the session hosts that will be used for Application SSO and register the agent with Privileged Account Manager. 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 Privileged Account Manager agent on all the remote Windows servers that will be used for Application SSO and register the agent with Privileged Account Manager. 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

Privileged Account Manager 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 Privileged Account Manager 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 Privileged Account Manager 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 Privileged Account Manager 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 AppSS0 package requires computer reboot at several stages of the installation. You must plan for a downtime before installing AppSS0 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 Package Manager Permissions.

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. Privileged Account Manager 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 Privileged Account Manager.

- Importing Application SSO Scripts
- Creating Application SSO Scripts

Importing Application SSO Scripts

Privileged Account Manager 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 Privileged Account Manager 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 Privileged Account Manager. 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

Certificate Authority (CA) Signed Certificates

For the CA signed certificate, you can create the certificate signing request from Privileged Account Manager, 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 Privileged Account Manager administrator console.

If you have multiple Privileged Account Manager 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 Privileged Account Manager administration console certificate signed by your CA.

3 Install the CA signed certificate in all Privileged Account Manager 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 Privileged Account Manager 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 Privileged Account Manager 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.

NOTE: 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.

---

6 Configuring Privileged Account Manager

This chapter provides instructions for configuring Privileged Account Manager.

Enabling FIPS Mode

Privileged Account Manager offers enhanced protection against security threats and compliance with United States federal government standards by supporting Federal Information Processing Standards (FIPS). Privileged Account Manager 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, Privileged Account Manager Agent, Privileged Account Manager Administration Console, Privileged Account Manager 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 Privileged Account Manager agents and managers.
- Enable FIPS on the operating systems hosting the managers and the agents.

  FIPS mode in Privileged Account Manager can be enabled only on Windows and Linux operating systems, for both managers and agents. FIPS mode in Privileged Account Manager is not supported on Unix operating systems. For a complete list of the supported Windows and Linux operating systems, see Privileged Account Manager 4.0 System Requirements and Sizing Guidelines.

To enable FIPS:

1. Enable FIPS on Privileged Account Manager:
   - **1a** Log in to the Privileged Account Manager 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 Privileged Account Manager, Cipher Block Chaining (CBC) mode is enabled by default. Disabling this mode in Privileged Account Manager, ensures CBC mode is not used for communication by product components such as PAM Manager, Privileged Account Manager Agent, Privileged Account Manager Administration Console, Privileged Account Manager 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 Privileged Account Manager agents and managers.

To disable CBC mode:

1. Log in to the Privileged Account Manager 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 Virtualization Implementation

You can access the target desktop using the Citrix Virtual Desktop Infrastructure (Citrix VDI). Privileged Account Manager supports Privileged Account Manager agent on target desktop and PAM manager on the Cirtix VDI server.

The users can have remote access to the hosted desktop machines within an organization by using a Virtual Desktop Infrastructure (VDI) environment. You can also monitor the user sessions and define roles for different users by using Citrix VDI environment and installing Privileged Account Manager agent on the target desktop.

You can create rules on PAM Manager for different users for their access and roles. When a user logs in to the target desktop using Citrix VDI server, the defined rules are used for his access and monitoring of the session. The following two different methods demonstrates to access the target desktop:

Using Citrix's Access Control

1. Install Privileged Account Manager agent on the target desktop.
2. Install PAM manager on the Citrix VDI server or any other machine. Register the Privileged Account Manager agent to the installed PAM manager.
3. Install the Citrix Receiver on the user's machine to access the target desktop.
4. Configure the rules for different users to access the target desktop by using Direct RDP in the PAM manager. These rules will be used to decide the login and the privileges of the user.

   For more information about configuring rules for Direct RDP.
5. The user can access the target desktop using the Citrix receiver.

Using Privileged Account Manager's Access Control

1. Install Privileged Account Manager agent on the target desktop.
2. Install PAM manager on the Citrix VDI server or any other machine. Register the Privileged Account Manager agent to the installed PAM manager.
3. Add the target desktop to the machine catalog of the Citrix VDI server.
4. Configure the rules for different users in PAM manager. You can defines rules for access and role. These rules will be used to decide the login and the privileges of the user.
5. The user can access the target desktop using RDP Relay, Credential Provider, or Direct RDP.

8 Upgrading Privileged Account Manager

This chapter provides instructions for upgrading Privileged Account Manager.

Privileged Account Manager Upgrade Checklist

Upgrade your Privileged Account Manager installation using the following checklist:

	Tasks	See
❑	1. Review the Privileged Account Manager Release Notes to see the new functionality and understand the known issues.	Privileged Account Manager Documentation website
❑	2. Ensure that the computers on which you want to upgrade Privileged Account Manager components meet the specified requirements.	System Requirements in Privileged Account Manager Documentation website.
❑	3. (Conditional) Configure the location from where the Package Manager must download the latest packages. By default, the package manager downloads packages from the Novell update server.	Configuring the Package Manager
❑	4. Download and publish the latest packages on the package manager.	Publishing Packages on the Package Manager
❑	5. Upgrade Privileged Account Manager.	Upgrading Privileged Account Manager
❑	6. (Conditional) Enabling Privileged Account Manager to run in FIPS 140-2 Mode.	Enabling FIPS Mode

Configuring the Package Manager

Package Manager acts as a repository that contains the latest packages, which can be installed on the required host. By configuring the Package Manager, you define the location from where the Package Manager must download the latest packages.

You can download packages to a Package Manager in the following ways:

- Manually download packages from the Downloads Website. To publish the downloaded packages, see Publishing Packages from the Downloads Website.
- Download packages directly from the Novell Update Server (Recommended).

  The Novell Update Sever contains all the packages of the last two major Privileged Account Manager releases and also the maintenance release (hot fix and service pack) packages of the second last release. For example, if the latest release of Privileged Account Manager is 3.2, the Novell Update Server contains the packages of the releases, such as 3.2.0.0, 3.1.0.0, 3.1.1.0, 3.1.1.1, 3.0.1.2, and so forth. You can differentiate the packages with the help of version numbering.
- Download packages from another Privileged Account Manager server, which contains the latest packages, that were downloaded using one of the two methods mentioned above.

To configure a Package Manager to download packages from Novell Update Server or another Privileged Account Manager server:

1. Click **Package Manager** on the home page of the console.
2. Click **Settings** in the task pane.
3. (Conditional) **To use the Novell Update server:**
   - **3a** Select **Novell Update Server**.
   - **3b** Specify the User Name and Password (These are the Mirrored Credentials obtained from the Novell Customer Center account for Privileged Account Manager).
   - **3c** To view the update server information, select **Advanced Settings**.
     - Select the **Packages** checkbox, the following URL is configured:

       `https://nu.novell.com:443/PUM/packages`
4. (Conditional) **To use another Privileged Account Manager server:**
   - **4a** Select **Local Package Manager**.
   - **4b** Fill in the following fields:

     Host name: Specify the DNS name of the host.

     Port: Specify the communication port. The default is 29120.

     The Local Package Manager is a Framework host that has been configured to store the packages.
5. Click **Finish**.
6. Continue with Publishing Packages from Novell Update Server or another Privileged Account Manager Server.

NOTE: By default, Package Manager connects to **Novell Update Server** for updates.

Publishing Packages on the Package Manager

You can publish the packages on the package manager in the following ways:

- Download packages from downloads website and publish the packages using command-line options. See Publishing Packages from the Downloads Website.
- If you have configured the system to download packages from the NetIQ Customer Center (NCC) or another Privileged Account Manager server, you can download and publish the packages from the console. See Publishing Packages from Novell Update Server or another Privileged Account Manager Server.

Publishing Packages from the Downloads Website

1. Download packages from the Downloads Website.
2. Create a directory such as `framework` on the Framework Manager in the `/tmp` directory.

   This directory is called `framework` in the rest of these instructions.
3. Copy the `netiq-npam-packages-4.0.tar.gz` from the Package Manager directory on the CD to the machine.
4. Extract the file to the `framework` directory.

   For UNIX and Linux platforms, use the following commands:

   ```
   gunzip netiq-npam-packages-4.0.tar.gz
   ```

   ```
   tar -xvf netiq-npam-packages-4.0.tar
   ```

   For Windows platforms, use WinZip to extract the file.
5. Use the following command to publish the packages to the Package Manager.

   Replace *<admin>* with the name of your admin user.

   For Linux and UNIX platforms:

   ```
   /opt/netiq/npum/sbin/unifi -u <admin> distrib publish -d /tmp/framework
   ```

   For Windows platforms:

   ```
   c:\Program Files\netiq\npum\bin\unifi -u <admin> distrib publish -d
   c:\tmp\framework
   ```

   For more information about the command to publish packages to the package manager, see Package Distribution Options section of the Privileged Account Manager Administration Guide.
6. When prompted, enter the password of the admin user.
7. (Optional) To view available packages, log in to the Framework Manager, then click **Package Manager**.
8. Delete the `framework` directory.
9. Continue with Upgrading Privileged Account Manager.

Publishing Packages from Novell Update Server or another Privileged Account Manager Server

Publishing Packages of Major Releases

To download and publish packages of the major Privileged Account Manager releases, such as 3.1, 3.2, 4.0, to the Package Manager, perform the following:

1. Ensure that you have configured the appropriate server for downloading packages. For more information, see Configuring the Package Manager.
2. Click **Package Manager** on the home page of the console.
3. Click **Add Packages** in the task pane.
4. Set the **Package Filter** options:

   Platforms: Select the operating system, then use the arrow to display and select the platforms.

   Types: Select the type of package you want to add (Console, Module, Interface, Patch).

   Components: Select the component (Command Control, Framework, Miscellaneous).
5. Select the required packages from the list of packages.

   To select multiple packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of packages. To select all the packages, select **Select all the packages** checkbox.
6. Click **Add** to start downloading.
7. Click **Finish**.
8. To ensure that all packages are up-to-date, continue with Publishing Packages of Service Packs, Patch Updates, and Hotfixes.

Publishing Packages of Service Packs, Patch Updates, and Hotfixes

After adding the appropriate major release packages to the Package Manager, check for any updates (hot fix, patch updates or service pack) on the major releases, such as 3.1.1.1, 3.0.1.2 and publish the updated packages to the Package Manager.

To download and publish packages, perform the following:

1. Ensure that you have configured the appropriate server for downloading packages. For more information, see Configuring the Package Manager.
2. Click **Package Manager** on the home page of the console.
3. Click **Check for Updates** in the task pane.

   If updates are available, the navigation pane displays the updated packages that are available for download. Else, an Alert dialog box is displayed stating **No package updates are available**.
4. Select the packages from the list of available packages.

To select multiple packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of packages. To select all the packages, select **Select all the packages** checkbox.

5 Click **Update** to start downloading.

6 Click **Finish**.

7 Continue with Upgrading Privileged Account Manager.

Upgrading Privileged Account Manager

Prerequisites

- Disconnect all Privileged Account Manager sessions to the host on which you are installing the package.
- Ensure that latest packages are available in the Package Manager. For publishing packages on the Package Manager, see Publishing Packages on the Package Manager.

NOTE: When you launch the dashboard for the first time after upgrade, the dashboard widgets may take a few minutes to load depending on the size of your database.

You must upgrade all Privileged Account Manager manager and agent components. You can upgrade all hosts or selected hosts in the following ways:

- "Upgrading Through Command Line" on page 51
- "Upgrading Through Console" on page 51
- "Upgrading Using the Privileged Account Manager Installer" on page 53

Upgrading Through Command Line

You can upgrade Privileged Account Manager by executing certain commands in the agent or the framework manager. To use these upgrade commands, you must have the `unifi` file in your machine at the location `/netiq/npum/bin/`. This file is available as part of the Privileged Account Manager ISO. For information about the upgrade commands and its usage, refer Upgrade and Rollback Packages.

Upgrading Through Console

You can upgrade Privileged Account Manager from the console, only if the **Enable Package Management Through Host Console** is set to **Yes** in the **Package Manager > Settings > Agent Package Management**.

WARNING: An Application SSO package update, triggers an automatic restart of the computer it is installed on.

To upgrade from the console, perform the following:

1 Upgrade your Framework Manager:

1a Click **Hosts**.

1b Select the host that is your Framework Manager.

1c Click **Update Packages** in the task pane.

The Framework Patch is displayed. This must be the latest version of the package before you can update any other packages. If the Framework Patch package is not displayed, follow the steps in Publishing Packages of Major Releases and add the Framework Patch for your platform.

1d Select the package, then click **Next**.

Ensure that the Credential Vault package (`prvcrdvlt`) is selected. If you do not update Credential Vault package (`prvcrdvlt`), you will not be able to manage privileged credentials.

1e When the package is installed, click **Finish**.

1f Click **Update Packages** in the task pane.

1g (Conditional) If Application SSO is enabled, update Administration Manager (admin) and Agent Console (servers) packages first, manually log out of the application, clear browser cache and log in again before you update any other packages.

1h Select all required packages, then click **Next**.

1i When the packages are installed, click **Finish**.

1j Verify that all packages display latest version. If they don't, return to Publishing Packages on the Package Manager and download any missing package.

2 (Conditional) If there are any new packages introduced in 4.0, you must install those packages on your Framework Manager:

New package introduced in 3.6 is Task Manager (`taskmanager`). Task Manager package is required only if you want to rotate resource password using Privileged Account Manager. Before installing the Task Manager package, review the Prerequisite in the Privileged Account Manager Administration Guide.

2a Click **Hosts**.

2b Select the host that is your Framework Manager, use the arrow to display the packages, then select **Packages**.

2c Click **Install Packages**.

2d Select packages newly added in 4.0 and then click **Next**.

2e Click **Finish**.

3 Upgrade your agents:

WARNING: An Application SSO package update, triggers an automatic restart of the computer it is installed on.

3a Click **Hosts** on the home page of the console.

3b Select the hosts that are agents or select the domain containing the agents.

3c Click **Update Packages** in the task pane.

3d Select the Framework Patch, then click **Next**.

3e Click **Update Packages** in the task pane.

3f Select the listed packages, then click **Next**.

3g When the packages have installed, click **Finish**.

3h Verify that all packages display 4.0 version.

Upgrading Using the Privileged Account Manager Installer

You can upgrade Privileged Account Manager Packages using the Privileged Account Manager Installer.

Prerequisites

- You must have the administrator privilege for the `unifi` module to execute this command in the local agent machine.
- This method is supported only in Windows computer.

To upgrade Privileged Account Manager:

1. Download the Privileged Account Manager installation file from the NetIQ Downloads website.
2. (Conditional) For interactive upgrade, run the following installer file and follow the onscreen prompts:

   `<filename>.msi`
3. (Conditional) For silent upgrade, use the following command:

   Syntax: `msiexec /i <Installer Filename> /passive USERNAME=<"username"> PASSWORD=<"password"> REINSTALL=ALL REINSTALLMODE=VOMUS`

   Example: `msiexec /i netiq_pam_manager_4.0.0_x64.msi /passive USERNAME="admin" PASSWORD="novell123" REINSTALL=ALL REINSTALLMODE=VOMUS`

   If you have mapped your local account to a Framework Manager user, you need not specify the user name and password.

   Example: `msiexec /i netiq_pam_manager_4.0.0_x64.msi /passive REINSTALL=ALL REINSTALLMODE=VOMUS`

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

Troubleshooting

This section contains potential problems and error codes that you may encounter when upgrading Privileged Account Manager.

AIX Agent Upgrade Through UI Fails With An Error Message

Issue: When you upgrade Framework package (`spf`) of the AIX agent through UI, the upgrade fails with the error message **Failed to receive response from the module**.

Workaround: To workaround this issue, you must perform hard restart of the AIX agent from the Host Console and try upgrading again.