
NetIQ® Privileged Account Manager™ 3.2 Installation Guide

December 2017

Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

© 2017 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>. All third-party trademarks are the property of their respective owners.

Contents

About This book and the Library	5
About NetIQ Corporation	7
1 NetIQ Privileged Account Manager Overview	9
Components	9
2 Installation Requirements	11
System Requirements	11
Hardware Requirements	11
Software Requirements	11
Procedural Overview	14
3 Installing the Framework Manager	15
Installing a Framework Manager	15
AIX Framework Manager Installation	15
HP-UX Framework Manager Installation	16
Linux Framework Manager Installation	16
Solaris Framework Manager Installation	17
Windows Framework Manager Installation	17
Accessing the Framework Console	18
Downloading and Installing NetIQ Privileged Account Manager License	18
Setting Up a Package Manager	19
Stopping and Restarting the Framework	20
AIX	20
HP-UX	20
Linux	20
Solaris	21
Windows	21
Removing the Framework Manager	22
AIX Manager Uninstall	22
HP-UX Manager Uninstall	22
Linux Manager Uninstall	23
Solaris Manager Uninstall	23
Windows Manager Uninstall	24
4 Installing the Agents	25
Agent Installation Overview	25
Creating a Host Name for Each Agent (Optional)	25
Opening Firewall Ports	26
Installing and Registering a Framework Agent	26
AIX Agent Install	26
HP-UX Agent Install	27
Linux Agent Installation	28
Windows Agent Installation	29
Solaris Agent Install	29
Removing the Agent Components	30
AIX Agent Uninstall	30

HP-UX Agent Uninstall	31
Linux Agent Uninstall	31
Solaris Agent Uninstall	32
Windows Agent Uninstall	32

5 Upgrading NetIQ Privileged Account Manager 35

Upgrade Privileged Account Manager	35
Upgrading Through Command Line	35
Upgrading from the Host Console	35
Upgrading Using the Privileged Account Manager Installer	37
Post Upgrade Task	37
Troubleshooting	38
Upgrading to 3.2 Through Command Line Or MSI Does Not Progress And Displays the Status Message Continuously	38
Upgrading from 3.1 to 3.2 in Windows Displays an Error.	38
AIX Agent Upgrade Through UI Fails With An Error Message	38

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

[NetIQ Privileged Account Manager 3.2 Administration Guide](#)

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk is nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ◆ Identity & Access Governance
- ◆ Access Management
- ◆ Security Management
- ◆ Systems & Application Management
- ◆ Workload Management
- ◆ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit <http://community.netiq.com>.

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.

Figure 1-1 Framework Manager



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.

2 Installation Requirements

For information about installation requirements, see the following sections:

- ♦ [“System Requirements” on page 11](#)
- ♦ [“Procedural Overview” on page 14](#)

System Requirements

Hardware Requirements

For the Framework agent:

- ♦ CPU - 2.5 GHz or equivalent
- ♦ Memory - 1 GB additional memory
- ♦ Hard Disk - 512 MB additional storage + additional storage for audit

For the Framework manager:

- ♦ CPU - 2.5 GHz or equivalent
- ♦ Memory - 4 GB
- ♦ Hard Disk - 1 GB additional storage + additional storage for audit

NOTE: Approximate additional storage calculation for audit = (500 KB) X (number of Privileged Account Manager users) X (number of sessions per day (usually 8 sessions)).

For Audit storage, when video capture is enabled, refer the [Performance and Sizing guidelines](#) guide on the [Privileged Account Manager Documentation](#) page.

Software Requirements

- ♦ [“Supported Platforms” on page 11](#)
- ♦ [“Supported Applications” on page 13](#)
- ♦ [“Supported Browsers” on page 13](#)

Supported Platforms

- ♦ [“Supported Platforms for Framework Manager” on page 12](#)
- ♦ [“Supported Platforms for Framework Agent” on page 12](#)

IMPORTANT: Ensure that the operating system is running the vendor's latest maintenance patches.

NOTE: SLES Specific Framework Manager and Framework Agents rpms are not supported on SLES platforms. Linux rpms are supported on SLES platform.

Supported Platforms for Framework Manager

The Framework Manager software has been tested on the following platforms:

- ♦ Windows Server 2016
- ♦ Windows Server 2012 R2 64-bit
- ♦ Windows Server 2012 64-bit GUI version

NOTE: Disable the Network Layer Authentication option. Go to **System Properties** and deselect the **Allow connections only from computers running remote desktop with Network Layer Authentication** option.

- ♦ Windows Server 2008 R2 64-bit
- ♦ Windows Server 2008 (32-bit and 64-bit)
- ♦ SUSE Linux Enterprise Server (SLES) 12 (64-bit)
- ♦ SUSE Linux Enterprise Server (SLES)11 (32-bit and 64-bit)
- ♦ Red Hat 7 (64-bit)
- ♦ Red Hat 6 (32-bit and 64-bit)
- ♦ AIX 7.1 64-bit
- ♦ AIX 6.1 (32-bit and 64-bit)
- ♦ HP-UX (Itanium) 11.31 64-bit
- ♦ HP-UX (Itanium) 11.23 64-bit
- ♦ HP-UX (PA-RISC) 11.23 (32-bit and 64-bit)
- ♦ Sun Solaris (SPARC) (32-bit and 64-bit) on version 10
- ♦ Sun Solaris (Intel) (32-bit and 64-bit) on version 10
- ♦ VMWare ESX/ESXi

Supported Platforms for Framework Agent

The Framework Agent software has been tested on the following platforms:

For Desktop:

- ♦ Windows 10
- ♦ Windows 8.1
- ♦ Windows 7

For Server:

- ♦ Windows Server 2016
- ♦ Windows Server 2012 R2 64-bit
- ♦ Windows Server 2012 64-bit GUI version

NOTE: Disable the Network Layer Authentication option. Go to **System Properties** and deselect the **Allow connections only from computers running remote desktop with Network Layer Authentication** option.

- ◆ Windows Server 2008 R2 64-bit
- ◆ Windows Server 2008 (32-bit and 64-bit)
- ◆ SUSE Linux Enterprise Server (SLES) 12 (64-bit)
- ◆ SUSE Linux Enterprise Server (SLES)11 (32-bit and 64-bit)
- ◆ Red Hat 7 (64-bit)
- ◆ Red Hat 6 (32-bit and 64-bit)
- ◆ AIX 7.1 64-bit
- ◆ AIX 6.1 (32-bit and 64-bit)
- ◆ HP-UX (Itanium) 11.31 64-bit
- ◆ HP-UX (Itanium) 11.23 64-bit
- ◆ HP-UX (PA-RISC) 11.23 (32-bit and 64-bit)
- ◆ Sun Solaris (SPARC) (32-bit and 64-bit) on version 10
- ◆ Sun Solaris (Intel) (32-bit and 64-bit) on version 10
- ◆ VMWare ESX/ESXi

Supported Applications

The Framework Manager software has been tested on the following applications. But you can customize the Privileged account Manager settings on any application that you require, such as Salesforce and so on.

- ◆ System Applications Product (SAP)
- ◆ VMware ESXi
- ◆ Oracle Database versions 11.x and 12.x
- ◆ Lightweight Directory Access Protocol (LDAP)
- ◆ Microsoft SQL Server versions 2008 and 2012
- ◆ OpenStack
- ◆ Amazon Web Services (AWS)

Supported Browsers

NetIQ Privileged Account Manager supports the following browsers:

- ◆ Microsoft Edge
- ◆ Microsoft Internet Explorer versions 10 and 11
- ◆ Mozilla Firefox
- ◆ Google Chrome

NOTE

- ♦ Video playback is supported only in Mozilla Firefox and Google Chrome.
 - ♦ If you are using Internet Explorer, ensure that you select the default document mode (Page Default) from the **F12 Developer Tools** option.
-

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 15](#).
- 2 When the installation has completed, access and log in to the console. See [“Accessing the Framework Console” on page 18](#).
- 3 Install the Privileged Account Manager license. See [“Downloading and Installing NetIQ Privileged Account Manager License” on page 18](#).

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 [“Setting Up a Package Manager” on page 19](#).

NOTE: Ensure that you download the myaccess package first then run an update to update the rdprelay package.

- 5 Install and register a Framework Agent on the computers that you want to manage. See [Chapter 4, “Installing the Agents,” on page 25](#).

When you have installed and registered the Framework agents, you have completed the installation of the Framework.

- 6 For configuration information, see the [NetIQ Privileged Account Manager 3.2 Administration Guide](#).

3 Installing the Framework Manager

- ◆ “Installing a Framework Manager” on page 15
- ◆ “Accessing the Framework Console” on page 18
- ◆ “Downloading and Installing NetIQ Privileged Account Manager License” on page 18
- ◆ “Setting Up a Package Manager” on page 19
- ◆ “Stopping and Restarting the Framework” on page 20
- ◆ “Removing the Framework Manager” on page 22

Installing a Framework Manager

Currently, the Framework Manager is available for installation on the platforms listed below. Refer to [Chapter 2, “Installation Requirements,” on page 11](#) for more information regarding supported versions.

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`.

Download the Privileged Account Manager installation package from [NetIQ Customer Center](#) and follow the below procedure for installing the Framework Manager in different platforms:

- ◆ “AIX Framework Manager Installation” on page 15
- ◆ “HP-UX Framework Manager Installation” on page 16
- ◆ “Linux Framework Manager Installation” on page 16
- ◆ “Solaris Framework Manager Installation” on page 17
- ◆ “Windows Framework Manager Installation” on page 17

AIX Framework Manager Installation

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/npum`. To change this, create a directory in the required part of the file system and create a symbolic link to `/opt/netiq/npum`.

To install the AIX manager:

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

```
gunzip <filename>
```

See the release notes for the actual filename.

- 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 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.
- 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 Framework Console” on page 18](#), and then [“Downloading and Installing NetIQ Privileged Account Manager License” on page 18](#).

HP-UX Framework Manager Installation

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/npum`. To change this, create a directory in the required part of the file system and create a symbolic link to `/opt/netiq/npum`.

To install the HP-UX manager:

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

```
gunzip <filename>
```

See the [NetIQ Privileged Account Manager 3.2 Release Notes](#) for the actual filename.

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


```
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 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 Framework Console” on page 18](#), and then [“Downloading and Installing NetIQ Privileged Account Manager License” on page 18](#).

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`.

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
```

See the [NetIQ Privileged Account Manager 3.2 Release Notes](#) for the actual filename.

- 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 Framework Console” on page 18](#), and then [“Downloading and Installing NetIQ Privileged Account Manager License” on page 18](#).

Solaris Framework Manager Installation

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/npum`. To change this, create a directory in the required part of the file system and create a symbolic link to `/opt/netiq/npum`.

To install the Solaris manager:

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

```
gunzip <filename>
```

See the [NetIQ Privileged Account Manager 3.2 Release Notes](#) for actual filename.

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

```
pkgadd -d /<directory of .pkg file>/<filename>.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 accepted. 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 Framework Console” on page 18](#), and then [“Downloading and Installing NetIQ Privileged Account Manager License” on page 18](#).

Windows Framework Manager Installation

To install the Windows Framework Manager:

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

```
<filename>.exe
```

See the [NetIQ Privileged Account Manager 3.2 Release Notes](#) for the actual filename.

- 2 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.

- 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 Framework Console” on page 18](#), and then [“Downloading and Installing NetIQ Privileged Account Manager License” on page 18](#).

Accessing the Framework 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 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.

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

- 7 Continue with [“Downloading and Installing NetIQ Privileged Account Manager License” on page 18](#).

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:

- ♦ [“Setting Up a Package Manager” on page 19](#)
- ♦ [Chapter 4, “Installing the Agents,” on page 25](#)

Setting Up a Package Manager

The Package Manager allows you to push updates to hosts and to install additional packages on the hosts for load balancing and failover. To use the Novell Update Server as the Package Manager, see [“Configuring the Package Manager”](#) in the *NetIQ Privileged Account Manager 3.2 Administration Guide*.

To use a local host as a Package Manager:

1 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.

2 Copy the `netiq-npam-packages-3.2.tar.gz` from the Package Manager directory on the CD to the machine.

3 Extract the file to the `framework` directory.

For UNIX and Linux platforms, use the following commands:

```
gunzip netiq-npam-packages-3.2.tar.gz
tar -xvf netiq-npam-packages-3.2.tar
```

For Windows platforms, use WinZip to extract the file.

NOTE: To deploy tunnel specific packages, use the following command:

```
gunzip netiq-npam-tunnel-packages-3.2.tar.gz
tar -xvf netiq-npam-tunnel-packages-3.2.tar
```

4 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
```

5 When prompted, enter the password for the admin user.

- 6 (Optional) To view available packages, log in to the Framework Manager, then click **Package Manager**.
- 7 Delete the `framework` directory.

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:

- ♦ [“AIX” on page 20](#)
- ♦ [“HP-UX” on page 20](#)
- ♦ [“Linux” on page 20](#)
- ♦ [“Solaris” on page 21](#)
- ♦ [“Windows” on page 21](#)

AIX

To stop the Framework process:

```
stopsrc -s npum
```

To start the Framework process:

```
startsrc -s npum
```

HP-UX

To stop the Framework process:

```
/sbin/init.d/npum stop
```

To start the Framework process:

```
/sbin/init.d/npum start
```

To check the status:

```
/sbin/init.d/npum status
```

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
```

Solaris

The following instructions apply to all supported 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
```

Solaris 10 also uses the SMF (Service Management facility). Example commands are:

```
svcs | grep npum
```

```
legacy_run Apr_21 lrc:/etc/rc3_d/S99npum
```

```
online Apr_21 svc:/application/security/npum:default
```

Then, to enable the Framework process:

```
svcadm enable npum
```

To disable the Framework process:

```
svcadm disable npum
```

To restart the Framework process:

```
svcadm restart npum
```

To clear the Framework process:

```
svcadm clear npum
```

Please refer to your Solaris documentation for full SMF instructions.

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

- ♦ “AIX Manager Uninstall” on page 22
- ♦ “HP-UX Manager Uninstall” on page 22
- ♦ “Linux Manager Uninstall” on page 23
- ♦ “Solaris Manager Uninstall” on page 23
- ♦ “Windows Manager Uninstall” on page 24

AIX Manager Uninstall

1 Use one of the following methods:

- ♦ The AIX smitty program.
- ♦ The following command:

```
installp -u netiqnpam
```

NOTE

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

```
installp -u novellnpum
```

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

```
installp -u netiqnpum
```

- ♦ 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 3.2 from an earlier version, run the following commands:

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

```
unlink /opt/netiq/npum
```

HP-UX Manager Uninstall

1 Enter the following command:

```
swremove netiq-npam
```

IMPORTANT

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

```
swremove 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:

```
swremove 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 3.2 from an earlier version, run the following commands:

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

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 3.2 from an earlier version, run the following commands:

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

Solaris Manager Uninstall

1 Enter the following command:

```
pkgrm netiq-npam
```

IMPORTANT

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

```
pkgrm 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:

```
pkgrm 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 3.2 from an earlier version, run the following commands:

```
rm -rf /opt/novell/npam
```

```
unlink /opt/netiq/npam
```

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 3.2 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 25
- ♦ “Creating a Host Name for Each Agent (Optional)” on page 25
- ♦ “Opening Firewall Ports” on page 26
- ♦ “Installing and Registering a Framework Agent” on page 26
- ♦ “Removing the Agent Components” on page 30

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 25
- ♦ “Installing and Registering a Framework Agent” on page 26

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 26.](#)

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. Refer to [“Supported Platforms” on page 11](#) for more information regarding supported versions.

Download the Privileged Account Manager installation package from [NetIQ Customer Center](#) and follow the below procedure for installing the Framework Agent in different platforms:

- ♦ [“AIX Agent Install” on page 26](#)
- ♦ [“HP-UX Agent Install” on page 27](#)
- ♦ [“Linux Agent Installation” on page 28](#)
- ♦ [“Windows Agent Installation” on page 29](#)
- ♦ [“Solaris Agent Install” on page 29](#)

NOTE: Agents must be registered with the Framework Manager after installation.

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 <filename>
```

See the [NetIQ Privileged Account Manager 3.2 Release Notes](#) for the actual filename.

- 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 25](#)).

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.

- 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 <filename>
```

See the [NetIQ Privileged Account Manager 3.2 Release Notes](#) for the actual filename.

- 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 25).

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.

- 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`.

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 <filename>.rpm
```

See the [NetIQ Privileged Account Manager 3.2 Release Notes](#) for the actual filename.

- 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 25).

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.

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

Windows Agent Installation

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

`<filename>.exe`

See the [NetIQ Privileged Account Manager 3.2 Release Notes](#) for the actual filename.

- 2 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.

- 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 25).

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.

- 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 Framework Console”](#) on page 18, and then [“Downloading and Installing NetIQ Privileged Account Manager License”](#) on page 18.

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 <filename>
```

See the [NetIQ Privileged Account Manager 3.2 Release Notes](#) for the actual filename.

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

```
pkgadd -d /<directory of .pkg file>/<filename>.pkg
```

See the [NetIQ Privileged Account Manager 3.2 Release Notes](#) for the actual filename.

- 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 25).

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.

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

Removing the Agent Components

- ♦ [“AIX Agent Uninstall”](#) on page 30
- ♦ [“HP-UX Agent Uninstall”](#) on page 31
- ♦ [“Linux Agent Uninstall”](#) on page 31
- ♦ [“Solaris Agent Uninstall”](#) on page 32
- ♦ [“Windows Agent Uninstall”](#) on page 32

AIX Agent Uninstall

- 1 Use one of the following methods:

- ♦ The AIX smitty program
- ♦ The following command:

```
installp -u netiqnpam
```

IMPORTANT

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

```
installp -u novellnpam
```

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

```
installp -u netiqnpum
```

- ◆ 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 3.2 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

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

```
swremove 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:

```
swremove 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 3.2 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

- ◆ 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 3.2 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

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

```
pkgrm 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:

```
pkgrm 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 3.2 from an earlier version, run the following commands:

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

```
unlink /opt/netiq/npum
```

Windows Agent 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 User Manager** and click **Remove**.
- 5 Delete the `C:\Program Files\netiq\npum` folder.

NOTE: If you have upgraded to Privileged Account Manager 3.1 from an earlier version, delete the C:\Program Files\novell\npum folder.

IMPORTANT: This action cannot be undone.

5 Upgrading NetIQ Privileged Account Manager

- ◆ [“Upgrade Privileged Account Manager” on page 35](#)
- ◆ [“Troubleshooting” on page 38](#)

Upgrade Privileged Account Manager

You can upgrade Privileged Account Manager in the following ways:

WARNING: Privileged Account Manager agents and framework managers on Windows reboot automatically after upgrading to 3.2. This happens as some of the Windows components required by Privileged Account Manager are updated in 3.2. Therefore, plan for a system downtime before upgrading to 3.2.

- ◆ [“Upgrading Through Command Line” on page 35](#)
- ◆ [“Upgrading from the Host Console” on page 35](#)
- ◆ [“Upgrading Using the Privileged Account Manager Installer” on page 37](#)
- ◆ [“Post Upgrade Task” on page 37](#)

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](#).

NOTE: To upgrade Privileged Account Manager to version 3.2 from any older version through command line, replace the existing `unifi` file with the `unifi` file from the PAM 3.2 ISO and then execute the upgrade command.

Upgrading from the Host Console

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

To upgrade from the Host Console, perform the following:

- 1 Publish the latest packages to the Package Manager.

There are multiple ways to accomplish this.

- ♦ You can use the Privileged Account Manager CD and set up your Framework Manager machine to be a local Package Manager. For instructions, see [“Setting Up a Package Manager” on page 19](#).
 - ♦ You can configure the Package Manager to use the Novell Update Server through your Novell Customer Care account. For instructions, see [“Configuring the Package Manager”](#) in the *NetIQ Privileged Account Manager 3.2 Administration Guide*.
- 2 (Conditional) If you are using the Novell Update Server, add the packages you need:
 - 2a Click **Package Manager** on the home page of the console, then click **Add Packages**.
 - 2b Configure the **Package Filter** to display the packages you need.

Platform: Select your platforms. Make sure you select **Cross Platform**, which displays the console packages that run on all platforms.

Types: Select at least **Console**, **Module**, and **Patch**.

Components: Select all of them: **Command Control**, **Framework**, and **Miscellaneous**.
 - 2c Select all the packages that are listed. Make sure you select the **Framework Patch**.
 - 2d Click **Next**, then click **Finish** when the packages have been successfully downloaded.
 - 2e To ensure that all packages are up-to-date, click **Check for Updates**.
 - 2f Select any packages that are listed.
 - 2g Click **Next**, then click **Finish** when the packages have been successfully downloaded.
 - 3 To upgrade your Framework Manager:
 - 3a Click **Hosts** on the home page of the console.
 - 3b Select the host that is your Framework Manager.
 - 3c Click **Update Packages** in the task pane.

The Framework Patch should be displayed. This package must be updated to 3.2 before you can update any other packages. If this package does not display, return to [Step 2](#) and add the Framework Patch for your platform.

NOTE: Ensure that you install the **myaccess** console package first then upgrade the **rdprelay** console package.

- 3d Select the package, then click **Next**.
 - 3e When the package is installed, click **Finish**.
 - 3f Click **Update Packages** in the task pane.
 - 3g Select the listed packages, then click **Next**.
 - 3h When the packages have installed, click **Finish**.
 - 3i Verify that all packages display a 3.2 version. If they don't, return to [Step 2](#) and add any missing packages.
- 4 To install new packages available in 3.2 on your Framework Manager:
 - 4a Click **Hosts** on the home page of the console.
 - 4b Select the host that is your Framework Manager, use the arrow to display the packages, then select **Packages**.
 - 4c Click **Install Packages**.
 - 4d Select the **Syslog Emitter**, then click **Next**.
 - 4e When the package has installed, click **Finish**.

- 5 To upgrade your agents:
 - 5a Click **Hosts** on the home page of the console.
 - 5b Select the hosts that are agents or select the domain containing the agents.
 - 5c Click **Update Packages** in the task pane.
 - 5d Select the Framework Patch, then click **Next**.
 - 5e Click **Update Packages** in the task pane.
 - 5f Select the listed packages, then click **Next**.
 - 5g When the packages have installed, click **Finish**.
 - 5h Verify that all packages display 3.2 version.

NOTE: To upgrade the SUSE Linux Enterprise Server (SLES) version of PUM 2.3.3 to the Linux version that Privileged account Manager supports, refer the [TID 7016202](#).

Upgrading Using the Privileged Account Manager Installer

You can upgrade Privileged Account Manager Packages using the Privileged Account Manager Installer. When you execute the installer through command line, it verifies whether Privileged Account Manager is installed in the system and if it is available, the existing packages are upgraded.

NOTE

- ◆ You must have the admin privileges for the `unifi` module to execute this command in the local agent machine.
- ◆ This method is supported only in the Windows system.

-
- 1 Download the Privileged Account Manager installation file from the [NetIQ Downloads website](#).
 - 2 Execute the following command and follow the onscreen prompts to upgrade:

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

Example: `msiexec /i netiq_pam_manager_3.2.0_x64.msi USERNAME="admin"
PASSWORD="novell123" REINSTALL=ALL REINSTALLMODE=VOMUS`

If you have mapped your local account to a Framework Manager user (see [Modify User: Native Maps](#)), you need not specify the user name and password.

Example: `msiexec /i netiq_pam_manager_3.2.0_x64.msi REINSTALL=ALL
REINSTALLMODE=VOMUS`

Post Upgrade Task

After upgrading Privileged Account Manager to 3.2 from lower versions, you must install the console packages:

- ◆ Enterprise Credential Vault (`prvcrdvl1t`)
- ◆ Access Dashboard (`userreqdashboard`)

These console packages are renamed in Privileged Account Manager 3.2. Hence, these packages are not upgraded by default and must be installed manually after upgrade. You can install these packages through the Host Console or the command line options. For information about installing the packages through Host Console, see [Installing Packages on a Host](#) . For information about the commands to install the packages, see [Install and Uninstall Packages](#).

Troubleshooting

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

Upgrading to 3.2 Through Command Line Or MSI Does Not Progress And Displays the Status Message Continuously

Issue: When you upgrade to 3.2 from any lower version through command line or MSI, the message `Attempt to add node with existing siblings` is displayed continuously without progressing to upgrade. This issue occurs when the upgrade through other modes are disabled by setting the value of **Allow Package Management Through Host Console** to **No** in the Host Console.

Workaround: Set the **Allow Package Management Through Host Console** to **Yes** and perform upgrade again.

Upgrading from 3.1 to 3.2 in Windows Displays an Error

Issue: When you upgrade from 3.1 to 3.2 in Windows, Command Control Agent upgrade fails with an error. This issue occurs because the LogonUI.exe or scrcapt.exe is active in the agent machine.

Workaround: To workaround this issue, close all the VMWare console sessions and Agent sessions and perform upgrade again. It is recommended to upgrade to 3.2 during an outage or a downtime.

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.