

CA SiteMinder®

Policy Server and Web Agent Option Pack Guide

r6.0 SP6/r6.x QMR6



This documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2011 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Product References

This document references the following CA Technologies products:

- CA SiteMinder®
- CA SiteMinder® SAML Affiliate Agent

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA Technologies products. At <http://ca.com/support>, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA Technologies product documentation, complete our short customer survey, which is available on the CA Support website at <http://ca.com/docs>.

Contents

Chapter 1: SiteMinder Option Packs	7
Overview of the Option Packs	7
Federation Security Services and its Components	8
eTelligent Rules	8
Web Service Variables	8
C Sample Program smpolicyapi	9
Chapter 2: System Requirements	11
System Requirements	11
Chapter 3: Installation Considerations	13
Version Compatibility	13
Components Required for Federation Security Services	13
Components Required for eTelligent Rules	13
Installation Requirements for the Policy Server Option Pack	14
Installation Requirements for the Web Agent Option Pack	14
ServletExec CLASSPATH for the Web Agent Option Pack (Windows)	14
Environment Variables Added by the Policy Server Option Pack	15
Environment Variables Added by the Web Agent Option Pack	15
Chapter 4: Policy Server Option Pack Installation and Uninstallation	17
Installation Modes	17
Policy Server Option Pack GUI and Console Mode Installation	17
Solaris 10 Setup Requirement for the Policy Server Option Pack	19
Import Federation Data After Installation (Optional)	20
Policy Server Option Pack Uninstallation	21
Chapter 5: Policy Server Option Pack Unattended Installation	23
Unattended Installation Overview	23
Prepare an Unattended Installation for the Policy Server Option Pack	23
Run the Unattended Installation (Policy Server Option Pack)	25
Stop an Unattended Installation in Progress	26

Chapter 6: Web Agent Option Pack Installation	27
Installation Modes	27
Web Agent Option Pack GUI and Console Mode Installation	27
Chapter 7: Web Agent Option Pack Unattended Mode Installation	31
Unattended Installation Overview	31
Prepare an Unattended Installation for the Web Agent Option Pack	31
Run an Unattended Installation (Web Agent Option Pack)	32
Stop an Unattended Installation in Progress	33
Chapter 8: Web Agent Option Pack Uninstallation	35
Uninstall the Web Agent Option Pack from Windows Systems	35
Uninstall the Web Agent Option Pack from UNIX Systems	35
Chapter 9: Upgrade the Option Packs	37
Policy Server Option Pack Upgrade	37
Version Compatibility for Upgrades	37
Preserve the smkeydatabase.properties File Before an Upgrade	37
Upgrade the Policy Server Option Pack	38
Web Agent Option Pack Upgrade	38

Chapter 1: SiteMinder Option Packs

This section contains the following topics:

[Overview of the Option Packs](#) (see page 7)

[Federation Security Services and its Components](#) (see page 8)

[eTelligent Rules](#) (see page 8)

[Web Service Variables](#) (see page 8)

[C Sample Program smpolicyapi](#) (see page 9)

Overview of the Option Packs

The Policy Server Option Pack and the Web Agent Option Pack are stand-alone products. The Policy Server Option Pack is installed on the same system you install the SiteMinder Policy Server. The Web Agent Option Pack can be installed on an application server or Web server.

The Option Packs enable you to use the following features:

- Federation Security Services
- eTelligent Rules
- Web Service Variables
- C sample program smpolicyapi

These features are described in the sections that follow.

Federation Security Services and its Components

Federation Security Services lets business partners exchange user identity information in a secure fashion. This exchange enables single sign-on across partner Web sites in multiple domains.

Federation Security Services is separately-licensed from SiteMinder and supports the following features:

SAML 1.0, 1.1, 2.0 and WS-Federation

SAML and WS-Federation are standards that define the exchange of authentication and authorization information between entities in a network using assertions. The Policy Server Option Pack provides the ability to generate SAML assertions. The Web Agent Option Pack supports the consumption of SAML assertions.

Federation Web Services (FWS)

Federation Web Services is an application that enables the consumption of SAML assertions. FWS is installed by the Web Agent Option Pack on a server that is connected to the Policy Server.

SAML Affiliate Agent

The SAML Affiliate Agent is a stand-alone component that provides authentication and session management for a consumer site or affiliate that does not have a SiteMinder Policy Server and Web Agent to protect its resources. The Web Agent Option Pack installs Federation Web Services, which allows the SAML Affiliate Agent to communicate with the Policy Server.

For more information about Federation Security Services, see the *Federation Security Services Guide*.

eTelligent Rules

eTelligent Rules variables enables a SiteMinder administrator to define fine-grained access-control policy expressions and can include operators and customer-defined variables that are evaluated at runtime when a user actually needs to access a protected resource on a Web site. For more information, see *SiteMinder Policy Design*.

You can use eTelligent Rules by installing only the Policy Server Option Pack. To use POST variables, you must also install the Web Agent Option Pack.

Web Service Variables

Web service variables let you add variables to SiteMinder policies to make authorization decisions. They are resolved through web services calls to local or remote data sources. This feature is supported by the Policy Server Option Pack.

C Sample Program smpolicyapi

The C sample program, smpolicyapi, can be run after you install the Policy Server Option Pack. It supports the manipulation of policy store data related to affiliates and affiliate domains.

For more information, see the *Developer's Guide for C*.

Chapter 2: System Requirements

This section contains the following topics:

[System Requirements](#) (see page 11)

System Requirements

For a list of supported platforms:

1. Log in to the [Technical Support](#) site.
2. Search for SiteMinder 6.0 Platform Support Matrix.

Some platforms supported in previous releases may no longer be supported.

Chapter 3: Installation Considerations

This section contains the following topics:

[Version Compatibility](#) (see page 13)

[Components Required for Federation Security Services](#) (see page 13)

[Components Required for eTelligent Rules](#) (see page 13)

[Installation Requirements for the Policy Server Option Pack](#) (see page 14)

[Installation Requirements for the Web Agent Option Pack](#) (see page 14)

[Environment Variables Added by the Policy Server Option Pack](#) (see page 15)

[Environment Variables Added by the Web Agent Option Pack](#) (see page 15)

Version Compatibility

The Policy Server and Web Agent Option Packs are compatible only with each other. Also, the Option Packs run only on the corresponding version of the Policy Server and Web Agent. For example, the Policy Server 6.0 SP6 Option Pack can only run on the 6.0 SP6 Policy Server.

For details on using the Option Packs in a mixed mode environment, that is, an environment with SiteMinder 5.x and 6.x systems, see the *SiteMinder Upgrade Guide*.

Components Required for Federation Security Services

The following components are required for Federation Security Services:

- Policy Server and Policy Server Option Pack
- Web Agent and Web Agent Option Pack
- Web Server or Application Web Server for the Federation Web Services application installed by the Web Agent Option Pack

Components Required for eTelligent Rules

The following components are required for eTelligent Rules:

- Policy Server and Policy Server Option Pack
- Web Agent and Web Agent Option Pack

Installation Requirements for the Policy Server Option Pack

The following are requirements to install the Policy Server Option Pack:

- Option Pack License
This is a site license; you need one license for each Policy Server. Contact your CA account manager to obtain a license.
- Policy Server v6.0 SP 6
This Policy Server must have a JRE, which is used by the Option Pack. For the specific JRE version, see the SiteMinder 6.0 Platform Matrix on the [Technical Support](#) site.
- Session Server
To use the Policy Server Option Pack, upgrade the session server. For upgrade instructions, see the *SiteMinder Upgrade Guide*.

Installation Requirements for the Web Agent Option Pack

The following are requirements to install the Policy Server Option Pack:

- ServletExec or supported application server
For supported platforms, see the SiteMinder 6.0 Platform Matrix at the [Technical Support](#) site.
Note: Be sure to apply the most current hot fixes for ServletExec. Without the hot fixes, Federation Web Services will not work with ServletExec. To obtain the hot fixes, go to the [New Atlanta Communications](#) web site.
- Java Development Kit (JDK)
For supported JDKs, see the SiteMinder 6.0 Platform Matrix at the [Technical Support](#) site.
A JDK is required even if you are using an application server that ships with a JDK or JRE.
The Web Agent is not required to install the Web Agent Option Pack; however, the Web Agent must be installed at run time to use Federation Security Services.

ServletExec CLASSPATH for the Web Agent Option Pack (Windows)

If you install the Web Agent Option Pack on a Windows system with ServletExec ISAPI and get an error message, such as **Class not found** when you access an existing servlet or .jsp, verify that the ServletExec classpath is correct.

If your classpath is correct and you still get the error, you may need to repair your classpath.pref file.

To repair the classpath.pref file

1. Access the ServletExec Admin Web page by entering the following in a browser:
http://myserver.myorg.org/servlet/admin
2. Under the Virtual Machine menu, select classpath to open the Classpath page.
3. Click Submit.
4. Restart the Sun ONE Web server or IIS Admin services. This forces ServletExec to write the classpath.pref.

If you are using Windows 2000, stop the IIS Admin services, then start the World Wide Web Publishing service without manually starting the IIS Admin service.

On Windows 2000, if this procedure does not fix the classpath do the following:

1. Open the classpath.pref in a text editor.
2. Collapse all entries to one line separated by a semi-colon(;).
3. Save the file.
4. Restart the Web server.

Environment Variables Added by the Policy Server Option Pack

The installation of the Policy Server Option Pack adds and modifies the following environment variables:

- NETE_PS_OPACK = "INSTALLED"
- NETE_JAVA_PATH =
%NETE_JRE_ROOT%\$/bin;%NETE_JRE_ROOT%\$/bin\$/server

Environment Variables Added by the Web Agent Option Pack

The installation of the Web Agent Option Pack sets the following environment variables:

- NETE_WA_OPACK = "INSTALLED"
- NETE_WA_PATH =
\$NETE_WA_ROOT\$/bin;\$NETE_WA_ROOT\$/bin\$/thirdparty;
\$NETE_JRE_ROOT\$/bin;\$NETE_JRE_ROOT\$/bin\$/server
- NETE_WA_CLASSPATH = \$NETE_WA_ROOT\$/java\$/smconapi.jar

Chapter 4: Policy Server Option Pack Installation and Uninstallation

This section contains the following topics:

[Installation Modes](#) (see page 17)

[Policy Server Option Pack GUI and Console Mode Installation](#) (see page 17)

[Solaris 10 Setup Requirement for the Policy Server Option Pack](#) (see page 19)

[Import Federation Data After Installation \(Optional\)](#) (see page 20)

[Policy Server Option Pack Uninstallation](#) (see page 21)

Installation Modes

The Policy Server Option Pack can be installed using one of the following modes:

GUI mode

Installation using the graphical user interface

Console mode

Installation by executing the Option Pack binary file

Unattended mode

After an initial installation, you can run unattended installations using the `nete-ps-opack-installer.properties` file

Installation instructions can be found in the following sections:

- [GUI and Console Mode Installation](#) (see page 17)
- [Unattended Mode Installation](#) (see page 23)

Policy Server Option Pack GUI and Console Mode Installation

The installation instructions that follow reflect the GUI mode prompts. For UNIX systems, you can install the Policy Server Option Pack using Console mode by executing the Option Pack binary file with the `-i` console command argument. The command line installation prompts are similar to the GUI mode prompts.

Before you install the Policy Server Option Pack, be sure of the following:

- The Policy Server is installed locally.
- The Policy Server is using a JRE, which the Policy Server Option Pack also uses.

To locate installation kits on the Support site

1. Click Technical Support.
2. Log into CA Support Online.
3. Click Download Center.
4. Search the Download Center for the installation kit you need.

To install the Policy Server Option Pack

1. Stop the Web or application server and exit any applications that are running.
2. Run the installation program according to your platform.

Windows

Double-click the executable nete-ps-opack-6.0-sp6-win32.exe.

Important! If you are running this wizard on Windows Server 2008, run the executable file with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

UNIX

At the command prompt, type one of the following commands:

■ **GUI Mode**

./binary_filename

■ **Console Mode**

./binary_filename -i console

There is a binary file for each supported operating system.

Example: To run the installation in GUI mode on a Solaris platform, enter the following command:

./nete-ps-opack-6.0-sp6-sol.bin

Note: If needed, use the chmod command to add execute permissions to the installation file, for example:

chmod +x nete-ps-opack-6.0-sp6-sol.bin

3. Follow the installation dialogs and prompts to complete the installation, noting the following:
 - In the Import Affiliate Data dialog box, do one of the following:

- For new installations, accept the default option, Import affiliate data during install. If you clear the check box, you will have to import this data later using the `smobjimport` command. For details, see [Importing Federation Services Data After Option Pack Installation](#).
- For an upgrade, clear this checkbox if you have made any changes or additions to the Federation Web Services policy store objects. Importing affiliate data overwrites policy store objects for Federation Web Services.
- In the SM Admin Username and SM Admin Password fields, specify the SiteMinder administrator username and password that you used during the installation of the Policy Server. Re-confirm the password in the Re-enter password field, then click Next.
- In the SM Key Database dialog, accept the default to create an `smkeydatabase` and enter a password to encrypt keys and certificate data in the `smkeydatabase`. Click Next.
- In the second SM Key Database dialog, accept the default if you want to import the default CA certificates, then click Install.

The program installs the Option Pack files then displays the Install Complete dialog box.

4. Choose whether to reboot your system immediate or later on your own, then click Done.

To reinstall the Policy Server Option Pack, repeat this procedure.

Solaris 10 Setup Requirement for the Policy Server Option Pack

A setup requirement exists for a Policy Server Option Pack running on a Solaris 10 system. If the default PKCS11 security provider is listed before the Sun security provider in the `java.security` properties file, the Policy Server Option Pack cannot execute encryption and decryption properly.

To solve this problem, list the Sun provider (`sun.security.provider.Sun`) before the PKCS11 provider (`sun.security.pkcs11.SunPKCS11`) in the `java.security` properties file. The properties file is located in the `lib/security` directory of the JDK installation.

Modify the java.security file as follows:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.pkcs11.SunPKCS11
${java.home}/lib/security/sunpkcs11-solaris.cfg
security.provider.3=sun.security.rsa.SunRsaSign
security.provider.4=com.sun.net.ssl.internal.ssl.Provider
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=sun.security.jgss.SunProvider
security.provider.7=com.sun.security.sasl.Provider
```

Import Federation Data After Installation (Optional)

During the installation of the Policy Server Option Pack you are prompted to import the ampolicy.smdif file. This file enables you to see the Option Pack policy objects in the Policy Server User Interface. If you did not import the file during installation, you can import the file after the installation using the smobjimport command.

Important! Whether during or after installation, you must import the ampolicy.smdif file.

The smobjimport command uses the following command arguments:

Argument	Meaning
siteminder_home	Installed location of the Policy Server
admin_name	SiteMinder administrator's user name
admin_pw	SiteMinder administrator's password
-f	Overrides duplicate objects.
-v	Enables verbose mode.
-l	Creates a log file.
-c	Indicates that the smdif input file contains unencrypted data.

Windows Systems Example for Importing ampolicy.smdif

```
smobjimport -isiteminder_home\db\smdif\ampolicy.smdif -dadmin_name
-wadmin_password -f -v -l -c
```

On Windows systems, if an argument contains spaces, use double quotes around the entire argument.

Example

```
smobjimport -i"C:\Program Files\netegrity\siteminder\db\smdif\ampolicy.smdif"  
-dsiteminder -wmypassword -f -v -l -c
```

UNIX Systems Example for Importing ampolicy.smdif

```
smobjimport -isiteminder_home/db/smdif/ampolicy.smdif -dadmin_name  
-wadmin_pw -f -v -l -c
```

Example

```
smobjimport -i/export/smuser/siteminder/db/smdif/ampolicy.smdif -dsiteminder  
-wmypassword -f -v -l -c
```

Policy Server Option Pack Uninstallation

To uninstall the Policy Server Option Pack, you simply uninstall the Policy Server, which automatically removes the Policy Server Option Pack.

To uninstall the Policy Server, see the *Policy Server Installation Guide*.

Chapter 5: Policy Server Option Pack Unattended Installation

This section contains the following topics:

[Unattended Installation Overview](#) (see page 23)

[Prepare an Unattended Installation for the Policy Server Option Pack](#) (see page 23)

[Run the Unattended Installation \(Policy Server Option Pack\)](#) (see page 25)

[Stop an Unattended Installation in Progress](#) (see page 26)

Unattended Installation Overview

After you have installed the Policy Server Option Pack on one system, you can automate other installations using the Policy Server Option Pack's unattended installation feature. An unattended installation lets you install or uninstall the Policy Server Option Pack without any user interaction.

Prepare an Unattended Installation for the Policy Server Option Pack

An unattended installation uses the `nete-ps-opack-installer.properties` file to propagate the Policy Server Option Pack installation setup across all Policy Servers in your network. In this properties file, you define a set of installation parameters, then copy the file and the Policy Server Option Pack executable file to any web server in your network. After you copy the files to the web server, run an unattended installation.

The `nete-ps-opack-installer.properties` file is installed in the following location:

`siteminder_home/install_config_info/nete-ps-opack-installer.properties`

The default parameter values reflect the information you entered during the initial Option Pack installation.

Note: The `nete-ps-opack-installer.properties` file is case-sensitive. The parameter names must be all upper-case and their values are case-sensitive.

The following table lists parameters in the `nete-ps-opack-installer.properties` file.

Parameter	Meaning
DEFAULT_IMPORT_CHOICE	Indicates whether affiliate policy objects are imported automatically during installation or imported manually after installation. Select true to allow an automatic import or false to do a manual import. The value must be entered in lower-case text.
DEFAULT_ADMIN_USER	Identifies the SiteMinder administrator defined at the Policy Server. Enter a user name in lower-case text
DEFAULT_ADMIN_PW	Identifies the SiteMinder administrator's password in clear text. To modify the password, uncomment this line and enter the password in clear text. It cannot be encrypted. You cannot modify the encrypted password in the ENCRYPTED_ADMIN_PW parameter
ENCRYPTED_ADMIN_PW	Encrypted SiteMinder administrator's password entered during the initial installation of the Option Pack.
DEFAULT_SMKEYDB_CHOICE	Indicates whether an smkeydatabase is created during installation or after installation. Select true to allow an automatic creation. Select false not to create the database. The value must be entered in lower-case text.
DEFAULT_SMKEYDB_PW	Identifies the smkeydatabase password in clear text. To modify the password, uncomment this line and enter the password in clear text. It cannot be encrypted. You cannot modify the encrypted password in the ENCRYPTED SMKEYDB_PW parameter
ENCRYPTED SMKEYDB_PW	Encrypted password for the smkeydatabase entered during the initial installation of the Option Pack.
DEFAULT_SMKEYDB_IMPORT_CHOICE	Indicates whether the CA default certificates are imported into the database during installation. Select true to allow the certificates to be imported. Select false not to import the certificates. The value must be entered in lower-case text.

To install the `nete-ps-opack-installer.properties` file

1. Install the Policy Server Option Pack in [GUI or Console mode](#) (see page 17).
2. Open the `nete-ps-opack-installer.properties` file and if needed, modify it.
3. Save the file.

Run the Unattended Installation (Policy Server Option Pack)

You should have completed an initial Policy Server Option Pack installation and, if necessary, modified the `nete-ps-opack-installer.properties` file. Now you can use the file to run subsequent Policy Server Option Pack installations.

To run an unattended installation

1. From a system where the Policy Server is already installed, copy the following files to a local directory.
 - `nete-ps-opack-6.0-sp6-win32.exe` (Windows) or the binary `nete-ps-opack-6.0-sp6-operating_system.bin` (UNIX)
 - `nete-ps-opack-installer.properties` file from `policy_server_home/install_config_info`

2. Place these files onto your local system.
3. Open a console window and navigate to the directory where you copied the two files.
4. Run the Policy Server Option Pack executable with the `-f` and `-i silent` options, as follows:

```
siteminder_executable -f properties_file -i silent
```

Assuming that you run the installation from the directory where the executable and properties file are located, the command is:

Windows:

```
nete-ps-opack-6.0-sp6-win32.exe -f nete-ps-opack-installer.properties -i silent
```

Important! Before running a SiteMinder utility or executable on Windows Server 2008, open the command line window with Administrator permissions. Open the command line window this way, even if your account has Administrator privileges. For more information, see the release notes for your SiteMinder component.

Note: If you are not running the command from the location where the files reside, specify the complete path to these files. If there are spaces in the path to the directory, enclose the entire path between quotation marks.

UNIX (Solaris example):

```
./nete-ps-opack-6.0-sp6-sol.bin -f nete-ps-opack-installer.properties -i silent
```

The status dialog opens and shows the unattended installation in process.

5. Check if the installation completed successfully by looking at the `CA_SiteMinder_Option_Pack_v6.0_SP6_for_Policy_Server_InstallLog.log` file, located in the `policy_server_home/install_config_info` directory. This log file contains the results of the installation.

Stop an Unattended Installation in Progress

You can stop an unattended installation while it is in progress.

To stop the installation, follow the instructions for your platform

Windows

Open the Windows Task Manager and stop the nete-ps-opack-6.0-sp6-win32.exe and ps_install.exe processes.

UNIX

Type Ctrl+C

Chapter 6: Web Agent Option Pack Installation

This section contains the following topics:

[Installation Modes](#) (see page 27)

[Web Agent Option Pack GUI and Console Mode Installation](#) (see page 27)

Installation Modes

The Web Agent Option Pack can be installed on a Web server running ServletExec or an application server (WebLogic, WebSphere, or JBoss).

There are several installation modes:

GUI mode

Installation using the graphical user interface.

Console mode

Installation by executing the Option Pack binary file.

Unattended mode

After an initial installation, you can run unattended installations using the nete-wa-opack-installer.properties file.

Installation instructions can be found in the following sections:

- [GUI and Console Mode Installation](#) (see page 27)
- [Unattended Mode Installation](#) (see page 31)

Web Agent Option Pack GUI and Console Mode Installation

The installation instructions that follow reflect the GUI mode installation prompts. For UNIX systems, you can install the Web Agent Option Pack using console mode by executing the Option Pack binary file with the -i console command argument. The command line installation prompts are similar to the GUI mode prompts.

Important! If you are installing the Web Agent Option Pack on a Windows system immediately after installing the Web Agent, reboot your machine first.

Install the Web Agent Option Pack using the method for your platform.

Windows systems

Install in GUI mode.

Important! If you are installing the Web Agent Option Pack on a Windows system immediately after installing the Web Agent, reboot your machine first.

UNIX systems

Install in GUI or console mode.

To install in console mode, you execute the Option Pack binary with the `-i console` command argument.

To locate installation kits on the Support site

1. Click Technical Support.
2. Log into CA Support Online.
3. Click Download Center.
4. Search the Download Center for the installation kit you need.

To install the Web Agent Option Pack

1. Stop the Web or application server and exit any applications that are running.
2. Run the installation program according to your platform.

Windows

Double-click the executable `nete-wa-opack-6qmr6-win32.exe`

UNIX

At the command prompt, type one of the following commands:

- **GUI Mode**

`./binary_filename`

- **Console Mode**

`./binary_filename -i console`

There is a binary file for each supported operating system.

Example: To run the installation in GUI mode on a Solaris platform, enter the following command:

`./nete-wa-opack-6qmr6-sol.bin`

Note: If needed, use the `chmod` command to add execute permissions to the installation file, for example:

`chmod +x nete-wa-opack-6qmr6-sol.bin`

3. Follow the installation dialogs and prompts to complete the installation.
4. When the installation is complete, choose whether to reboot your system now or later; then click Done.

To reinstall the Option Pack, re-run the executable.

Chapter 7: Web Agent Option Pack Unattended Mode Installation

This section contains the following topics:

[Unattended Installation Overview](#) (see page 31)

[Prepare an Unattended Installation for the Web Agent Option Pack](#) (see page 31)

[Run an Unattended Installation \(Web Agent Option Pack\)](#) (see page 32)

[Stop an Unattended Installation in Progress](#) (see page 33)

Unattended Installation Overview

After you have installed the Web Agent Option Pack on one system, you can automate installations on other web or application servers using the Web Agent Option Pack's unattended installation feature. An unattended installation lets you install or uninstall the Web Agent Option Pack without any user interaction.

Prepare an Unattended Installation for the Web Agent Option Pack

An unattended installation uses the `nete-wa-opack-installer.properties` file to propagate the Option Pack installation set-up across all servers in your network. In the properties file, you define installation parameters, then copy the properties file and the Web Agent Option Pack executable file to any applicable server in your network. After the files are copied, you can run an unattended installation.

The `nete-wa-opack-installer.properties` file is in the directory `web_agent_opack_home/install_config_info`. The default parameter and path in the file reflect the information you entered during the initial Option Pack installation.

To install the `nete-wa-opack-installer.properties` file

1. Run an initial installation of the Web Agent Option Pack. For instructions, see [Web Agent Option Pack GUI and Console Mode Installation](#) (see page 27).
2. Open the `nete-wa-opack-installer.properties` file and if needed, modify the following settings:
 - `USER_INSTALL_DIR`--specifies the location where you want to install the Web Agent Option Pack.
 - `USER_REQUESTED_RESTART`--restarts the server after installation.
3. Save the file.

Run an Unattended Installation (Web Agent Option Pack)

Prior to running an unattended installation, you should have:

- completed an initial Web Agent Option Pack installation
- modified the `nete-wa-opack-installer.properties` file, if necessary

You can now use the `nete-wa-opack-installer.properties` file to run subsequent Web Agent Option Pack installations.

Note: You can run an unattended installation to reinstall the Web Agent on the same system where you initially performed an installation in GUI or console mode.

To run an unattended installation

1. From a system where the Web Agent Option Pack is already installed, copy the following files to a local directory on your system.

- Executable file

Windows: `nete-wa-opack-6qmr6-win32.exe`

UNIX: `nete-wa-opack-6qmr6-operating_system.bin`

- Properties file

`nete-wa-opack-installer.properties` file from
`web_agent_opack_home/install_config_info`

Important! If you are running this wizard on Windows Server 2008, run the executable file with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Open a console window and navigate to the location where you copied the files.
3. Run the Agent executable using the **-f** and **-i silent** options, as follows:

```
agent_executable -f properties_file -i silent
```

Assuming that you run the installation from the directory where the executable and properties file are located, the command syntax is shown in the following examples:

Windows example:

```
nete-wa-opack-6qmr6-win32.exe -f nete-wa-opack-installer.properties -i silent
```

Note: If you are not at the location where the executable and properties file reside, specify the full path to these files. If there are spaces in the directory paths, enclose the entire path with quotation marks.

Solaris example:

```
./nete-wa-opack-6qmr6-sol.bin -f nete-wa-opack-installer.properties -i silent
```

The status dialog box displays, which shows the unattended installation in process.

When the installation is complete, you return to the command prompt.

4. Check to see if the installation completed successfully by looking in the `CA_SiteMinder_Option_Pack_v6qmr6_for_Web_Agent_InstallLog.log` file, located in the `web_agent_opack_home/install_config_info` directory. This log file contains the results of the installation.

Stop an Unattended Installation in Progress

You can stop an unattended installation while it is in progress.

To stop the installation, follow the instructions for your platform

Windows

Open the Windows Task Manager and stop the `nete-wa-opack-6qmr6-win32.exe` and `wa_option_pack.exe` processes.

UNIX

Type Ctrl+C

Chapter 8: Web Agent Option Pack Uninstallation

This section contains the following topics:

[Uninstall the Web Agent Option Pack from Windows Systems](#) (see page 35)

[Uninstall the Web Agent Option Pack from UNIX Systems](#) (see page 35)

Uninstall the Web Agent Option Pack from Windows Systems

To uninstall the Web Agent Option Pack

1. Stop the Web server and exit applications that are running.
2. Open up the Windows Control Panel.
3. Double-click on Add/Remove Programs.
The control panel opens.
4. Select CA SiteMinder Option Pack v6QMR6 for Web Agent then click Change/Remove.
The program displays a dialog box confirming the uninstallation.
5. Click Uninstall.
The Option Pack is removed.
6. Stop and restart the Web server.

Uninstall the Web Agent Option Pack from UNIX Systems

The uninstallation instructions that follow reflect the GUI mode prompts. For UNIX systems, you can uninstall the Option Pack using Console mode by executing the Option Pack binary file with the **-i console** command argument. The command line installation prompts are similar to GUI mode prompts.

To uninstall the Web Agent Option Pack

1. Stop the Web server and exit any applications that are running.
2. Open a console window.
3. Add the location of the JDK to the PATH environment variable to uninstall the Option Pack as follows:

```
PATH=/jdk_home/bin:${PATH}
```

```
export PATH
```

where *jdk_home* is the location of the JDK

This avoids an error message that the Java virtual machine could not be found.

4. Navigate to the installed location of the Web Agent.
5. At the prompt, enter one of the following:

GUI mode

```
./nete-wa-opack-uninstall.sh
```

Console mode

```
./nete-wa-opack-uninstall.sh -i console
```

6. Review the dialog that confirms the removal of the Option Pack, then click Uninstall.

The Web Agent Option Pack is now removed from your system.

Chapter 9: Upgrade the Option Packs

This section contains the following topics:

[Policy Server Option Pack Upgrade](#) (see page 37)

[Web Agent Option Pack Upgrade](#) (see page 38)

Policy Server Option Pack Upgrade

Different features require different versions of the Policy Server and its Option Pack, as follows:

SAML 1.1 POST profile

Requires that the Policy Server be at version 6.0 SP 2 or higher.

SAML 2.0 features

Requires that the Policy Server be at version 6.0 SP 3 or higher.

WS-Federation

Requires that the Policy Server be at version 6.0 SP 5 or higher.

Version Compatibility for Upgrades

The Policy Server Option Pack 6.0 SP6 is compatible only with Policy Server v6.0 SP6. You can upgrade the Option Pack from a previous version, but you must also upgrade the Policy Server.

Important! When you upgrade, the upgrade program automatically creates back-up configuration files and overwrites the existing configuration files.

Preserve the smkeydatabase.properties File Before an Upgrade

When reinstalling the Policy Server Option Pack as part of an upgrade, the smkeydatabase.properties file gets replaced with a new properties file that has some revised settings from the existing file. Also, the EncryptedPassword from the existing file is not preserved.

To ensure the smkeydatabase.properties file uses the correct EncryptedPassword value, the value from the old file needs to be placed into the new file.

To ensure the smkeydatabase.properties file is upgraded properly

1. Back up the existing smkeydatabase and the smkeydatabase.properties file.
2. Upgrade the Policy Server and the Policy Server Option Pack by installing the new versions.
3. Edit the smkeydatabase.properties file and insert the EncryptedPassword value from the back-up copy of the file. The file is located in the directory `policy_server_home/config/properties/`.

Upgrade the Policy Server Option Pack

To upgrade the Policy Server Option Pack to v6.0 SP 6

1. Stop the Policy Server.
2. Upgrade the Policy Server to v6.0 SP 6.
For instructions, see the *Policy Server Installation Guide*.
3. Upgrade the Policy Server Option Pack to v6.0 SP 6.

The installation program also runs as an upgrade. For instructions, go to the [installation chapter](#) (see page 17) in this guide.

Web Agent Option Pack Upgrade

The Web Agent v6.x QMR 6 Option Pack is compatible only with Web Agent v6.x QMR 6. You can upgrade from any previous version of the Web Agent Option Pack to v6.x QMR 6, but you must also upgrade the Web Agent.

Important! When you upgrade, the upgrade program automatically creates back-up configuration files and overwrites the existing configuration files.

To upgrade the Web Agent Option Pack to v6.x QMR 6

1. Uninstall the current Option Pack. For instructions, go to the [uninstallation chapter](#) (see page 35).
2. Upgrade the Web Agent to v6.x QMR 6.
For instructions, see the *Web Agent Installation Guide*.
3. Upgrade the Web Agent Option Pack to v6.x QMR 6.

The installation program also runs as upgrade. For instructions, go to the [installation chapter](#) (see page 27) in this guide.