CA SiteMinder®

Policy Server Installation Guide

r6.0 SP6

Second Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA SiteMinder®

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: Installing the Policy Server on Windows

This section contains the following topics:

Quick Installation Overview

Policy Server

1. **Install the Policy Server**
   See *Policy Server Installation Guide*
2. **Set up Agent Objects in Policy Server User Interface:**
   - SiteMinder Administrator with rights to register trusted hosts
   - Host Configuration Object
   - Agent Configuration Ojbect

   See *Policy Design Guide*
3. **Set up policies in Policy Server User Interface:**
   See *Policy Design Guide*

Web Agent

4. **Install Web Agent**
   See *Web Agent Installation Guide*
5. **Register Trusted Host**
   (part of Agent installation and configuration process)
   See *Web Agent Installation Guide*
6. **Run the Agent Configuration Wizard (Windows) or Script (UNIX)**
   See *Web Agent Installation Guide*
7. **Enable the Web Agent**
   See *Web Agent Installation Guide*

Windows Installation Overview

This chapter describes how to install the Policy Server on a Windows system, which includes running a setup program and configuring the web server. When you install the Policy Server on a Windows system, you can use the Policy Server installer to configure the SiteMinder policy store automatically in one of the following:

- Sun™ Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet)
- Microsoft Active Directory® Application Mode (ADAM)
- Microsoft Active Directory® Lightweight Directory Services (AD LDS)

For other supported LDAP and relational database vendors, you configure the policy store manually after installing the Policy Server. These manual steps are outlined in this guide.

Audit logs can be stored in either an ODBC database (SQL Server or Oracle) or a text file. After you install the Policy Server, audit logging is set to a text file and not to ODBC by default.

System Requirements

The Policy Server on Windows requires an Intel Pentium III or better.

Before you install the Policy Server, make sure you are using a supported operating system and third-party software. For a list of supported operating systems, Web Servers, databases, Web browsers, LDAP Directory Servers, and servlet engines, go to the Technical Support site and search for the SiteMinder Platform Matrix for 6.0.

Note: For Internet Explorer 5.5, make sure you have SP2 since SP1 cannot post data greater than 4072 bytes.

In addition, make sure you have the following components installed on your computer:

- Memory: 512 MB system RAM (minimum).
- Hard disk space: 270 MB free disk space in the install location and 180 MB of free space in the system's temporary file location. These requirements are based on a medium size policy database (about 1,000 policies).

- Screen resolution: 800 x 600 or higher resolution with 256 colors or better to properly view the Policy Server User Interface.
- JRE: Make sure you have the required JRE version. For the required version, search for the SiteMinder Platform Matrix for 6.0 on the Technical Support site. You can download the latest version at the Sun Developer Network (SDN).

Note: To run the OneView Monitor user interface, make sure you have the required Java SDK and Servlet Exec/ISAPI for Windows. For the required versions, search for the SiteMinder Platform Matrix for 6.0 on the Technical Support site. You also need ServletExec for JSP Password and Registration Services.

Before You Begin

Be aware of the following before installing the Policy Server:

- To install the Policy Server, you must log into a Windows account with local administrator privileges.
- (Windows 2008) If you are installing a Policy Server on a system running the Windows 2008 operating environment, update the Windows firewall settings to allow inbound connections on the following ports:
  - 44441
  - 44442
  - 44443

  These ports are the default Policy Server accounting, authentication, and authorization ports. If you change these ports after installing the Policy Server, be sure to allow inbound connections to the respective ports.

  Note: For more information, see the Microsoft documentation.
- (IBM Directory Server) If you are using IBM Directory Servers in your SiteMinder environment, edit the V3.matchingrules file by adding the following line:

  ```
  MatchingRules=(2.5.13.15 NAME 'integerOrderingMatch' SYNTAX
  1.3.6.1.4.1.1466.115.121.1.27
  ```

  If the V3.matchingrules file does not contain the change, the directory store is not be configured correctly and the necessary SiteMinder objects are not created
- Install the documentation.
- System Path Length—If the system path length exceeds 1024 characters, including or excluding the SiteMinder added directories, the Policy Server installation fails We recommend trimming the pre–SiteMinder system path to approximately 700 characters.

- The 6.x Policy Server does not configure Microsoft Access as the default policy store as with previous SiteMinder releases. Access is not supported as a policy store.
- Be sure that the Sun Java System or IIS web server instance is stopped to let the Policy Server installer configure the Policy Server User Interface.
- To avoid possible policy store corruption, be sure that the server on which the policy store is to reside is configured to store objects in UTF-8 form. For more information about configuring your server to store objects in UTF-8 form, see the vendor–specific documentation.
- The Policy Server and Documentation installations each modify environment variables.

More Information:

Modified Windows Environment Variables (see page 239)

Install the SiteMinder Documentation

You install the documentation separately using nete-sm-doc-6.0-sp6-win32.exe because it is not installed by default with the Policy Server. We recommend that you install the documentation before the Policy Server.

To install the SiteMinder documentation

1. Exit all applications that are running.
2. Download the installation kit from the Technical Support site and extract it to a temporary location.
3. Double–click nete-sm-doc-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.
4. In the Introduction dialog, read the welcome message and click Next.
5. Read the Software License Agreement, accept the terms if you agree and click Next.
6. Read the Installation Notes and click Next.
7. In the Choose Install Folder dialog, select the location where you want the documentation installed. The default is C:\Program Files\Netegrity\netegrity_documents.

8. In the Choose Shortcut Folder dialog, select one of the following to create product icons.

   In a new Program Group

   The install program configures a SiteMinder program group in the Start, Programs menu.

   In an existing Program Group

   The install program configures a SiteMinder program group in an existing group.

   Example: Start, Programs, Accessories.

   In the Start Menu

   The install program configures a program icon in the Windows Start menu.

   On the Desktop

   The install program configures a SiteMinder program icon on the Windows desktop.

   In the Quick Launch Bar

   The install program configures a SiteMinder program icon in the Quick Launch bar.

   Other

   The install program configures a SiteMinder installation directory in the specified directory.

   Don't create icons

   The install program does not configure SiteMinder icons.

9. Review the settings in the Pre-Installation Summary dialog and click Install.

   The installation program begins copying files to your system.

10. After the installation is complete, click Done.

If you have installed the documentation after installing the Policy Server, create the netegrity_docs virtual directory on the web server. This directory lets you view the documentation using the Policy Server User Interface. You can run the Policy Server Configuration Wizard to create the directory or you can manually create it for IIS 5.0/6.0.

More Information

Run the Policy Server Configuration Wizard (see page 25)
Manually Create the netegrity_docs Virtual Directory on IIS 6.0 (see page 213)

Install the Policy Server

The Policy Server installer extracts the Policy Server files and installs them on your computer. The Policy Server is installed, by default, in the C:\Program Files\Netegrity\siteminder directory.

Run the Policy Server Installer

Run the Policy Server installer to install the Policy Server.

To run the Policy Server installer

1. Exit all applications that are running.

   After installation, you can find the installation log files in *siteminder_home*\install_config_info:

   - CA_SiteMinder_Policy_Server_v6.0_SP6_InstallLog.log
   - nete-ps-details.log

     If you use the Policy Server installer to configure the policy store automatically, the nete-ps-details.log file lets you determine the status of the policy store after it has been configured.

   siteminder_home

   Specifies the Policy Server installation path.

2. Download the Policy Server installation kit from the Technical Support site and extract the installation media to a temporary location.

3. Navigate to the installation media and double–click nete–ps–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.

   Setup verifies the following prerequisites:

   - You are logged into an account with local administrator privileges.
   - You have the appropriate operating system and web server listed on the SiteMinder Platform Matrix for 6.0. To access this matrix, go to the Technical Support site and search for the SiteMinder Platform Matrix for 6.0.
   - The computer has necessary free disk space and the required JDK or JRE installed. For the required versions, search for the SiteMinder Platform Matrix for 6.0 on the Technical Support site.

4. In the first Introduction dialog, be sure that the system has the prerequisites listed and click Next. If it does not, stop the installation and install the required prerequisites.

5. If the installer cannot locate the JRE, it prompts you for the location. Enter the appropriate location and click Next.
6. Read the Software License Agreement, accept the terms if you agree, and click Next.
7. Read the Installation Notes, then click Next.
8. Enter your name and company name and click Next.
9. Accept the default Policy Server installation location or select a different one and click Next. If necessary, click Choose to browse to the appropriate location.

   Note: If you cut and paste a path, the Next button is disabled. Type a character to enable the Next button.
10. Decide where you would like to create product icons in Windows for the Policy Server by selecting one of the following:

    In a new Program Group

    The install program configures a SiteMinder program group in the Start, Programs menu.

    In an existing Program Group

    The install program configures a SiteMinder program group in an existing group.

    Example: Start, Programs, Accessories.

    In the Start Menu

    The install program configures a program icon in the Windows Start menu.

    On the Desktop

    The install program configures a SiteMinder program icon on the Windows desktop.

    In the Quick Launch Bar

    The install program configures a SiteMinder program icon in the Quick Launch bar.

    Other

    The install program configures a SiteMinder installation directory in the specified directory.

    Don’t create icons

    The install program does not configure SiteMinder icons.

11. In the Encryption Key dialog, complete the following:
    a. Enter a case–sensitive, alphanumeric encryption key. The encryption key is a key that secures data sent between the Policy Server and the policy store. The key can be from 6 to 24 characters in length. All Policy Servers that share a SiteMinder policy store (a database containing policy information) must be configured using the same encryption key. For stronger protection, define a long encryption key.
    b. Re–enter the key to confirm the entry.
    c. Take note of this key for future reference and click Next.
12. In the Choose Features dialog, select the Policy Server features you want to configure:

    OneView Monitor GUI

    The install program configures the OneView Monitor GUI to work on the web server you specify later in this procedure.

    Note: A supported version of a Java SDK and ServletExec are required to use the OneView Monitor GUI. For supported versions, see the SiteMinder Platform Support Matrix for 6.0 on the Technical Support site.

    Web Server(s)

    The install program configures the Policy Server User Interface and the OneView Monitor (if you specified it previously) to work on this web server.

    SNMP

    The install program configures the SNMP to work with the Policy Server.

    Note: Be sure that you have an SNMP Service (Master OS Agent) installed with your Windows operating system. For instructions on installing the SNMP service, see to the Windows online help system.

    Policy Store

    The install program can automatically configure an LDAP directory server as a policy store. You can automatically configure the policy store in an instance of Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet), Active Directory Application Mode (ADAM), or Active Directory Lightweight Directory Services (AD LDS). For other supported LDAP or relational database vendors, you configure the policy store manually after installing the Policy Server.

    Note: If there is a problem with configuring the policy store, you can run the Policy Server Configuration Wizard (located in C:\Program Files\Netegrity\siteminder\install_config_info\nete-ps-config.exe) to fix the issue.

13. In the Web Server dialog, select the web server to configure with the Policy Server and click Next.

    Note: Consider the following:

    - Be sure that the web server instance is stopped.
    - If you have multiple web servers, only select one. We recommend configuring one web server at a time. Use the Policy Server Configuration Wizard to configure additional web servers after installing the Policy Server.
    - If you are installing the Policy Server before the documentation, you are prompted to run the Policy Server Configuration Wizard to create the netegrity_docs virtual directory on the web server. This virtual directory lets you view the documentation using the Policy Server User Interface.
    - If you plan on configuring the Policy Server User Interface on multiple web servers, the URL of the Policy Server User Interface shortcut is configured to the port number of the first web server you configure. For example, if the first web server in the list is IIS at port 80 and the second is Sun ONE at port 81, the Policy Server User Interface shortcut is configured for port 80. If you want to run the Policy Server User Interface on the second web server, edit the URL in the shortcut or the Policy Server User Interface does not appear.

14. (Optional) Use the Policy Server installer to configure an instance of ADAM, AD LDS, or Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) as a policy store.

Note: For other supported LDAP or relational database vendors, configure the policy store manually after installing the Policy Server.

More Information:

Configure an LDAP Policy Store (see page 20)
Run the Policy Server Configuration Wizard (see page 25)
LDAP Directory Servers as a Policy or Key Store (see page 81)
Relational Databases as a Policy or Key Store (see page 111)

Configure an LDAP Policy Store

The following procedures assume that you are running the Policy Server installer to configure a policy store automatically.

For a list of supported LDAP directory servers, see the SiteMinder Platform Support Matrix. To access this matrix, go to the Technical Support site and search for the SiteMinder Platform Support Matrix for 6.0.

To configure the LDAP directory server, you are required to supply the following:

- The IP address and port of the LDAP server
- The root DN under which the SiteMinder schema is placed
- The administrator information for the LDAP directory

Note: This installation cannot be completed using an SSL connection.

If the Policy Server installer automatically configures the policy store, the installer does not configure ODBC data sources. If you migrate your policy store to an ODBC database, you are required to create the ODBC data sources manually.

Configure ADAM/AD LDS as a Policy Store

To use the Policy Server installer to configure ADAM or AD LDS as a policy store

1. Be sure that you have met the prerequisites for configuring ADAM/AD LDS as a policy store (see page 98).
2. When prompted by the installer to configure the policy store, enter the following information and click Next:

   IP address

   Specifies the IP Address of the directory server host system.

   Port number

   Specifies the port on which the directory server instance is listening.

   Root DN

   Specifies the root DN location of the application partition in the directory server where the policy store schema must be installed.

   Example: dc=netegrity,dc=com

Admin DN

Specifies the full domain name, including the guid value, of the directory server administrator.

Example: CN=user1,CN=People,CN=Configuration,CN={guid}

Admin password

Specifies the password of the directory server administrator.

3. In the next Policy Store dialog, specify if a different LDAP user account is to administer the policy store.

   By default, SiteMinder uses the LDAP administrator account to administer the policy store. You have the option to have the policy store administered through a different LDAP user account. The complete DN for the user is required to configure SiteMinder this way.

   Note: This user must have all the necessary privileges to modify attributes and change passwords.

   - If you do not want to use a different LDAP account, click Next.
   - If you want to use a different LDAP account, do the following:
     a. Select Use different LDAP user.
     b. Enter the DN of the LDAP user.
     c. Enter and confirm the password for the specified account.
     d. Click Next.

     Example: uid=SMAdmin, ou=people, o=security.com.

4. In the next Policy Store dialog, select Initialize LDAP instance only if you are initializing a new LDAP instance and click Next.
5. For the SiteMinder super user password, complete the following:
   a. Enter a password for the SiteMinder super user account. The pre–defined SiteMinder super user account has maximum SiteMinder privileges. The password can be from 6 to 24 characters in length.

      Note: The password is case–insensitive, except when the password is stored in an Oracle policy store.

b. Re–enter the password.

Important! Take note of the password. You use this password to log into the Policy Server User Interface for the first–time. You can change the password using the Policy Server Management Console.

Note: We recommend that you do not use this account for day–to–day operations. Instead, use this account to access the Policy Server User Interface for the first–time to create another SiteMinder administrator with system–wide privileges. For more information about the Policy Server Management Console, see the *Policy Server Management Guide*.

c. Click Next.

6. Review the settings in the Pre–Configuration Summary and click Install.

   The installation program begins copying files to your system. The installation can take a few minutes.

7. Click Done to complete the installation and reboot the system.

   If there were problems during the installation, you can find the installation log files in *siteminder_home*\install_config_info.

   siteminder_home

   Specifies the Policy Server installation path.

   The file names are:

   - CA_SiteMinder_Policy_Server_v6.0_SP6_InstallLog.log
   - nete-ps-details.log

     The nete-ps-details.log file lets you determine the status of the policy store.

8. (Optional) Access the Policy Server User Interface.

More Information:

Access the Policy Server User Interface (see page 30)

Configure Sun Java System Directory Server Enterprise Edition as a Policy Store

To configure Sun Java System Directory Server Enterprise Edition as a policy store

1. In Policy Store dialog for the LDAP server:
   a. Enter the IP address of the LDAP directory host system.
   b. Enter the port on which the directory server instance is listening.

c. Enter the root DN. Specify the root DN as the following:

o=*root_DN*

root_DN

Specifies the root DN.

d. Click Next.

2. In the next Policy Store dialog:

a. Enter the user name (Bind DN) for the LDAP administrator account.

Example: cn=Directory Manager

b. Enter the password for the administrator DN account.

c. Confirm the password.

d. Click Next.

3. In the next Policy Store dialog, specify if a different LDAP user account is to administer the policy store.

By default, SiteMinder uses the LDAP administrator account to administer the policy store. You have the option to have the policy store administered through a different LDAP user account. The complete DN for the user is required to configure SiteMinder this way.

- If you do not want to use a different LDAP account, click Next.
- If you want to use a different LDAP account, do the following:

a. Select Use different LDAP user.

b. Enter the DN of the LDAP user.

Example: uid=SMAdmin,ou=people,o=security.com.

c. Enter and confirm the password for the specified account.

d. Click Next.

4. In the next Policy Store dialog, select Initialize LDAP instance only if you are initializing a new LDAP instance and click Next.

5. For the SiteMinder super user password, complete the following:

a. Enter a password for the SiteMinder super user account. The pre–defined SiteMinder super user account has maximum SiteMinder privileges. The password can be from 6 to 24 characters in length.

Note: The password is not case–sensitive, except when the password is stored in an Oracle policy store.

b. Re–enter the password.

Important! Take note of the password. You use this password to log into the Policy Server User Interface for the first–time. You can change the password using the Policy Server Management Console.

Note: We recommend that you do not use this account for day–to–day operations. Instead, use this account to access the Policy Server User Interface for the first–time to create another SiteMinder administrator with system–wide privileges. For more information about the Policy Server Management Console, see the *Policy Server Management Guide*.

c. Click Next.

6. Review the settings in the Pre–Configuration Summary and click Install.

   The installation program begins copying files to your system. The installation can take a few minutes.

7. Click Done to complete the installation and reboot your system.

   If there were problems during the installation, you can find the installation log files in *siteminder_home*\install_config_info.

   The file names are:

   - CA_SiteMinder_Policy_Server_v6.0_SP6_InstallLog.log
   - nete-ps-details.log

     The nete-ps-details.log file lets you determine the status of the policy store.

8. (Optional) Access the Policy Server User Interface.

More Information:

Access the Policy Server User Interface (see page 30)

Additional SNMP Step

After the installation is complete, if you chose to have SNMP configured, the installer prompts you to configure SNMP event trapping.

Note: Before running this step, you must have an SNMP Service installed with your Windows operating system.

Configure SNMP Event Trapping

To enable SNMP event trapping

1. Launch the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. Click the Advanced tab.
3. In the Event Handlers field at the bottom, enter the full path to the eventsnmp.dll.
4. Click OK.

After enabling SNMP event trapping, configure the snmptrap.config file.

More Information:

Configure the SNMP Agent on Windows (see page 198)

Run the Policy Server Configuration Wizard

The Policy Server Configuration Wizard (nete-ps-config.exe) lets you configure the following:

- The OneView Monitor GUI
- The Policy Server User Interface
- The netegrity_docs virtual directory on a web server
- SNMP support
- A policy store

When configuring a policy store on Windows, the wizard can automatically configure Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet), ADAM, or AD LDS as a policy store. If another supported LDAP directory server or relational database is to function as the policy store, you configure the policy store manually.

If you install the documentation after installing the Policy Server, run the Policy Server Configuration Wizard to create the netegrity_docs virtual directory on the web server. This virtual directory lets you view the documentation using the Policy Server User Interface.

To run the Policy Server Configuration Wizard

1. Close all programs.
2. Navigate to *siteminder_home*\install_config_info.

   siteminder_home

   Specifies the Policy Server installation path.

3. Double–click nete-ps-config.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.

   The wizard verifies the following prerequisites:

   - You are logged into an account with local administrator privileges.
   - You have the appropriate Policy Server environment variables set.

4. In the Choose Features dialog, select the Policy Server features you want to configure. The OneView Monitor GUI, Web Server(s), and Policy Store are selected by default:

   OneView Monitor GUI

   The install program configures the OneView Monitor GUI to work on the web server you selected before completing this procedure.

   Note: To use the OneView Monitor, you must have the required Java SDK and ServletExec ISAPI for Windows/IIS installed. For the required versions, see the SiteMinder Platform Matrix for 6.0 on the Technical Support site.

   Web Server(s)

   The install program configures the Policy Server User Interface and the OneView Monitor (if you specified it previously) to work on this web server.

   SNMP

   The install program configures SNMP to work with the Policy Server.

   Note: Be sure that you have an SNMP Service (Master OS Agent) installed with your Windows operating system. For more information about installing the SNMP service, see the Windows online help system.

   Policy Store

   The install program configures an LDAP directory server as a policy store.

5. In the Web Server dialog, select the web server to configure for the Policy Server and click Next.

   Note: Consider the following:

   - Be sure that the web server instance is stopped.
   - If you have multiple web servers, only select one. We recommend configuring one web server at a time. Use the Policy Server Configuration Wizard to configure additional web servers after installing the Policy Server.
   - If you are installing the Policy Server before the documentation, you are prompted to run the Policy Server Configuration Wizard to create the netegrity_docs virtual directory on the web server. This virtual directory lets you view the documentation using the Policy Server User Interface.
   - If you plan on configuring the Policy Server User Interface on multiple web servers, the URL of the Policy Server User Interface shortcut is configured to the port number of the first web server you configure. For example, if the first web server in the list is IIS at port 80 and the second is Sun ONE at port 81, the Policy Server User Interface shortcut is configured for port 80. If you want to run the Policy Server User Interface on the second web server, edit the URL in the shortcut or the Policy Server User Interface does not appear.

6. In the first Policy Store dialog, select whether you want to configure a new policy store or update an existing one.
7. (Optional) In the next Policy Store dialog, click Next to configure ADAM, AD LDS, or Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) as a policy store.

More Information:

Configure an LDAP Policy Store (see page 20)
LDAP Directory Servers as a Policy or Key Store (see page 81)
Import Policy Data Using smobjimport (see page 150)
Relational Databases as a Policy or Key Store (see page 111)

Run the Unattended Policy Server Installer

After you have installed the Policy Server on one system, you can reinstall it or install it on another system using an unattended installation mode. An unattended installation lets you install or uninstall the Policy Server without user interaction.

The installer provides a properties template (nete–ps–installer.properties) file that lets you pre–define installation variables. The default parameters, passwords, and paths in this file reflect the information you entered during the initial Policy Server installation.

In this file, you can either store encrypted or plain text passwords. If you are using encrypted passwords, for example, a shared secret or SiteMinder super user password, use the same values entered during the initial Policy Server installation. These passwords are encrypted in the file and cannot be modified. However, you can use plain text passwords by modifying the file.

The nete-ps-installer properties file is located in the *siteminder_home*\install_config_info directory.

siteminder_home

Specifies the Policy Server installation path.

To run the installer in the unattended installation mode

1. Modify the nete-ps-installer properties file with the settings you want.
2. From a Policy Server host system, copy nete-ps-6.0-sp6-win32.exe and the nete-ps-installer properties file to a temporary location.

   Note: To reinstall the Policy Server on the same system, copy these files to C:\Temp. To install the Policy Server on another system, copy these files to C:\Temp on that system.
3. From the C:\Temp directory, run the following command:

   ```
   nete-ps-6.0-sp6-win32.exe -f nete-ps-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.

   If the nete-ps-installer properties file is not in the same directory as the installation program, enclose the argument with double–quotes if the argument contains spaces.

   Example: nete-ps-6.0-sp6-win32.exe -f "C:\Program Files\Netegrity\siteminder\install_config_info\nete-ps-installer.properties" -i silent

   -i silent

   Specifies that the installer run in the unattended installation mode.

   The unattended installation begins. When installing the Policy Server, the installer uses the parameters specified in the nete-ps-installer properties file.

To stop the installation manually, use the Windows Task Manager and stop the nete-ps-6.0-sp6-win.exe and ps_install.exe processes.

To verify if the unattended installation completed successfully, see the CA_SiteMinder_Policy_Server_v6.0_SP6_InstallLog.log file in the *siteminder_home*\install_config_info directory. This log file contains the results of the installation.

More Information:

Configure Installation for Unattended Mode (see page 224)

Scripting Interface for Perl

The Scripting Interface let you write Perl scripts to configure and manage policy stores. Using the Scripting Interface, you can write Perl scripts to import and export particular objects rather than all the Policy Store objects. The installation program installs a full version of Perl and puts the interface files in the *siteminder_home*\CLI directory.

siteminder_home

Specifies the Policy Server installation path.

To use the Scripting Interface, be sure that the following directory is in your system's Path environment variable before any other Perl bin directories on your machine:
C:\Program Files\Netegrity\siteminder\CLI\bin

Note: For more information on this interface, see the *Scripting Guide for Perl*.

Reports Server

In 6.x, the Reports Server (Crystal Reports) is not installed with the Policy Server, as with previous SiteMinder releases. However, SiteMinder 6.x provides reports files (.rpt) that are compatible with Crystal Reports 9.0. After integrating these files into you existing Crystal Reports 9.0 environment, you can run SiteMinder reports.

More Information:

Crystal Reports in a Policy Server Environment (see page 179)

Next Steps

Now that you have installed the Policy Server on Windows, complete the following:

1. Set up an LDAP directory or relational database as a policy store to store your policy–related information. All Policy Servers in a SiteMinder installation must share the same policy store.

   Note: If you used the Policy Server installer or Policy Server Configuration wizard to configure the policy store automatically, you can skip this step.

2. Access the Policy Server User Interface to verify that your browser supports it and the required Java version.

3. Prepare the Policy Server for the Web Agent Installation.
4. Install a Web Agent

   Note: For more information about installing a Web Agent, see the *Web Agent Installation Guide*.

More Information:

LDAP Directory Servers as a Policy or Key Store (see page 81)
Relational Databases as a Policy or Key Store (see page 111)
Access the Policy Server User Interface (see page 30)
How to Prepare for the Web Agent Installation (see page 34)
Crystal Reports in a Policy Server Environment (see page 179)

Access the Policy Server User Interface

Once you have installed the Policy Server, access it through a browser. Verify that the browser supports the Policy Server User Interface and the required Java version by entering the following URL: http://www.netegrity.com/UItest6.0

Note: The URL for the browser test is case–sensitive.

To access the Policy Server User Interface using Internet Explorer, access the Policy Server User Interface from Internet Explorer (see page 32) *before* completing the following procedure.

To reduce the time it takes to load the Policy Server User Interface, you can access it locally from your system.

To access the Policy Server User Interface

1. On the Status tab of the Policy Server Management Console, be sure that the Policy Server is running.

   Note: For more information about the Policy Server Management Console, see the *Policy Server Management Guide*.

2. Do one of the following:

   - Open your browser and enter the following URL:
     http://*hostname*:port/siteminder

     hostname

     Specifies the name of the Policy Server host system. The port is the port number of the web server. If you are using the default port (80) for HTTP requests, you do not need to enter a port.

     Example: http://www.myorg.org:80/siteminder

- From the Start menu, select Programs, SiteMinder, SiteMinder Policy Server User Interface.

  The system opens your browser and displays the SiteMinder Administrator login page.

  Note: For a list of supported web browsers, go to the Technical Support site and search for the SiteMinder Platform Matrix for 6.0.

3. Click Administer Policy Server.

   Once the Administration applet has downloaded, the SiteMinder Administration window appears.

4. Grant permission for your browser to load files from CA.

5. In the User Name field, enter SiteMinder.

   This user name is the default super user for which you entered a password during the installation.

6. In the Password field, enter the password you defined when configuring the policy store.

7. If you have trouble logging into the Policy Server User Interface, reset the SiteMinder super user password by completing the following steps:

   a. Copy the smreg utility (smreg.exe) from the Policy Server installation kit to *siteminder_home*\bin.

      siteminder_home

      Specifies the Policy Server installation path.

   b. Run the following command:

      `smreg -su super_user_password`

      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.

      super_user_password

      Specifies the password for the SiteMinder super user account.

      Note: Be sure that there is a space between -su and the password.

   c. Delete smreg.exe.

      Deleting smreg.exe prevents anyone from changing the super user password.

More Information:

Access the User Interface Locally (see page 32)

Run the User Interface from a Non-default Port

When launching the Policy Server User Interface for Windows, the URL assumes that you are running the Web server at the default port 80. If you are running on a different port, or if you change the port of your Web server, modify the Policy Server User Interface shortcut in the Start menu.

To modify the Internet shortcut

1. Go to the C:\Documents and Settings\All Users\Start Menu\Programs\SiteMinder directory.
2. Right click on the Policy Server User Interface shortcut and select Properties.
3. From the Internet Shortcut tab, edit the Target URL field to reflect the correct machine name and port.

Access the User Interface Locally

Accessing the Policy Server User Interface locally reduces the time it takes to load.

If you access the Policy Server User Interface from Internet Explorer, the Policy Server User Interface files, which are stored in sm_admin.cab are automatically stored in the cache of Internet Explorer.

Access the User Interface from Internet Explorer

If you are using Internet Explorer, you must add your domain as a trusted site before accessing the Policy Server User Interface.

To access the Policy Server User Interface from Internet Explorer

1. Open Internet Explorer and select Internet Options from the Tools menu.
2. Select the Security tab to bring it to the front.
3. Click the Trusted Sites icon to select it, then click the Sites button.

   The Trusted sites dialog box is displayed. The Require sever verification (https) for all sites in this zone is enabled by default.
4. (Optional) If you are not accessing the Policy Server using a secured connection (https), deselect the Require server verification (https) for all sites in this zone check box.

5. In the Add this Web site to the zone field, enter the full name of your server including the domain, then click Add:

   Example: http://<*servername*>.<*domain-name*>

   Example: http://security.myorg.org

   Note: If you are connecting to the Policy Server User Interface using a secured connection (https), you must include https when specifying the domain.

   Example: https://security.myorg.org

6. Click OK to save the changes and return to the Internet Options dialog box.
7. Click OK to exit the Internet Options dialog box.
8. Exit Internet Explorer, then restart the browser for the settings to take effect.

Troubleshoot the User Interface

The following section detail how you can troubleshoot the User Interface.

Policy Server User Interface Fails to Start in Internet Explorer

Symptom:

When I attempt to start the Policy Server User Interface in Internet Explorer it fails.

Solution:

Make sure that the Java Plug-in is set as the default Java Runtime in the browser by doing the following:

1. From the Control Panel, select Java Plug-In.
2. On the Browser tab, make sure that Microsoft Internet Explorer is checked and click Apply.
   - If the plug-in is not set, the Policy Server User Interface stalls indefinitely at the Downloading Administration dialog box.
   - If you are still have difficulty getting the Policy Server User Interface to display, run the Policy Server User Interface Browser Compatibility Test at the following URL: http://www.netegrity.com/uitest6.0
   - If the panel is a solid box, click Details for more troubleshooting information.

Policy Server UI Fails to Start on a Sun Java System Web Server

Symptom:

When I attempt to start the Policy Server User Interface that is configured for a Sun Java System Web server, it fails to start.

Solution:

Disable the Java Enabled Globally option by doing the following:

1. Open the Sun Java System Enterprise Administration Server home page by entering the following URL in a browser: http://<*yourserver.com*>:<*webserverport*>

   yourserver.com

   Specifies the domain name of the Enterprise Administration Server.

   webserverport

   Specifies the port number.

2. In the Select a Server drop-down menu, select a server, and then click Manage.
3. Select the Java tab.
4. Deselect Enable Java for class defaultclass and Enable Java Globally and click OK.
5. Turn on the Web server.

How to Prepare for the Web Agent Installation

Before you install the Web Agent, the Policy Server must be installed and be able to communicate with the system where you plan to install the Web Agent.

To centrally manage Agents, you configure the following using the Policy Server User Interface:

- A SiteMinder Administrator that has the right to register trusted hosts.

  A trusted host is a client computer where one or more SiteMinder Web Agents are installed. The term trusted host refers to the physical system. There must be an administrator with the privilege to register trusted hosts.

  Note: To configure an administrator, see the Administrators chapter of the *Policy Design* guide.

- Agent identity

  An Agent identity establishes a mapping between the name and the IP address of the web server instance hosting a Web Agent. You define an Agent identity from the Agents object in the Policy Server User interface. You assign it a name and specify the Agent type as a Web Agent.

  The name you assign for the Agent is the same name you specify in the DefaultAgentName parameter for the Agent Configuration Object that you must also define to centrally manage an Agent.

- Host Configuration Object

  This object defines the communication between the trusted host and the Policy Server after the initial connection between the two is made.

  A *trusted host* is a client computer where one or more SiteMinder Web Agents can be installed. The term trusted host refers to the physical system.

  Do not confuse this object with the trusted host's configuration file, SmHost.conf, which is installed at the trusted host after a successful host registration. The settings in the SmHost.conf file enable the host to connect to a Policy Server for the first connection only. Subsequent connections are governed by the Host Configuration Object.

  Note: More information on the host configuration object exists in the *Policy Design* guide.

- Agent Configuration Object

  This object includes the parameters that define the Web Agent configuration. There are a few required parameters you must set for basic operation described below.

  Note: To read more about this object, see the Agents and Agent Groups chapter of *Policy Design* guide.

  - **For all Agents**

    The Agent Configuration Object must include a value for the DefaultAgentName. This entry should match an entry you defined in the Agents object.

    The DefaultAgentName identifies the Agent identity that the Web Agent uses when it detects an IP address on its Web server that does not have an Agent identity assigned to it.

- **For Domino Web Agents**

  The Agent Configuration Object must include values for the following parameters:

  DominoDefaultUser-If the user is not in the Domino Directory, and they have been authenticated by SiteMinder against another user directory, this is the name by which the Domino Web Agent identifies that user to the Domino server. This value can be encrypted.

  DominoSuperUser-Ensures that all users successfully logged into SiteMinder will be logged into Domino as the Domino SuperUser. This value can be encrypted.

- **For IIS Web Agents**

  The Agent Configuration Object must include values for the DefaultUserName and DefaultPassword parameters.

  The DefaultUserName and DefaultPassword identify an existing NT user account that has sufficient privileges to access resources on an IIS Web server protected by SiteMinder. When users want to access resources on an IIS Web server protected by SiteMinder, they may not have the necessary server access privileges. The Web Agent must use this NT user account, which is assigned by an NT administrator, to act as a proxy user account for users granted access by SiteMinder.

  If you plan to use the NTLM authentication scheme, or enable the Windows User Security Context feature, do not specify values for these IIS Web Agent parameters.

Note: For instructions about configuring Agents at the Policy Server, see *the Policy Design* guide. For Agent parameter descriptions, see the *Web Agent Guide*.

How to Reinstall the Policy Server

Installing the Policy Server over an existing Policy Server of the same version lets you restore lost application files or to restore the Policy Server's default installation settings.

To reinstall the Policy Server

1. Using the Policy Server Management Console's Status tab, stop and restart the Policy Server.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. Close the Policy Server Management Console.

3. Install the Policy Server.
4. Configure an LDAP directory or relational database as a policy store.

More Information:

Install the Policy Server (see page 16)
Configure an LDAP Policy Store (see page 20)
LDAP Directory Servers as a Policy or Key Store (see page 81)
Relational Databases as a Policy or Key Store (see page 111)

How to Uninstall the Policy Server and Documentation

To uninstall the Policy Server and documentation, you must log into the account from which the Policy Server was installed originally and:

1. Set the JRE Path variable (see page 37).
2. Uninstall the Policy Server (see page 38), including leftover files.
3. Uninstall the documentation (see page 39).

Note: Running the uninstallation deletes all Policy Server files and all Policy Server settings. The Policy Server Option Pack is also removed if present.

Set JRE in PATH Variable Before Uninstalling Any SiteMinder Component

When you are uninstalling the Policy Server, Web Agent, Policy Server Option Pack, Web Agent Option Pack, SDK, SAML Affiliate Agent, make sure the JRE is in the PATH variable or the uninstallation program stops and issues one of the following error messages:

- “Could not find a valid Java virtual machine to load. You need to reinstall a supported Java virtual machine.”
- "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program."

To Set the JRE in the PATH variable

1. Go to the Control Panel.
2. Double-click System.
3. In the Environment Variables dialog, add the location of the JRE to the Path system variable.

Uninstall the Policy Server

To uninstall the Policy Server

1. Shut down all instances of the Policy Server Management Console.
2. Verify that no Web Agents are configured to use the Policy Server you are uninstalling:
   a. Navigate to a*gent_install_directory*\config

      agent_install_directory

      Specifies the Web Agent installation directory.

   b. Open the SmHost.conf file in a text editor.
   c. Remove the Policy Server from the SmHost.conf file by deleting the entire line that begins "policyserver=" and contains the IP Address and port numbers for the Policy Server you are uninstalling.
   d. Save SmHost.conf.

   Note: For information about modifying the SMHost.conf file, see the *Web Agent Guide* and the *Web Agent Installation Guide*.
3. From the Control Panel, double-click Add/Remove Programs.
4. Select CA SiteMinder Policy Server v6.0 and click Add/Remove.
5. Complete the uninstall by following the instructions on the screen.

   Note: If the system displays a "Remove Shared File?" message, click No to All.
6. When the uninstall is finished, reboot your system (if requested).

Remove Files Left by Uninstallation

There may be files and registry keys that are left on the system by the Policy Server uninstallation. Be aware of the following:

- The following directories and file may be left on the system after you uninstall the Policy Server:
  - *siteminder_home*\bin
  - *siteminder_home*\install_config_info
  - C:\Program Files\ZeroG Registry\com.zerog.registry.xml

  Remove these manually before reinstalling the Policy Server.
- Registry entries for AdventNet software are also left in the system registry under:

  HKEY_LOCAL_MACHINE\SOFTWARE\Advent, Inc.

  Important! Delete this key only if AdventNet software was not on the system before installing the Policy Server.

- The SNMP Agent is also not removed by the uninstall.

  To uninstall the service, run the following:

  ```
  c:\WINDOWS\javaservice.exe -uninstall
  ```

  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.

- The SiteMinder virtual directories in IIS may not be removed by the uninstall. Delete the following virtual directories using the IIS Microsoft Management Console:
  - 'SiteMinder'
  - SiteMinderCgi'
  - 'SiteMinderMonitor'
  - 'netegrity_docs'

After uninstalling the Policy Server and rebooting the machine, the following services may not be removed:

- SiteMinder Health Monitor Service
- SiteMinder Policy Server
- SNMP Agent

The registry key names for the latter services are SMServMon, SMPolicySrv, and Agent Service, respectively.

To remove services that remained after uninstalling the Policy Server

1. Stop each service.
2. Remove the following Windows registry key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\`*`registry_key_name`*

Uninstall the Documentation

To uninstall SiteMinder documentation

1. From the Control Panel, double-click Add/Remove Programs.
2. Select CA SiteMinder v 6.0 Documentation and click Remove.
3. Remove the documentation by following the instructions on the screen.

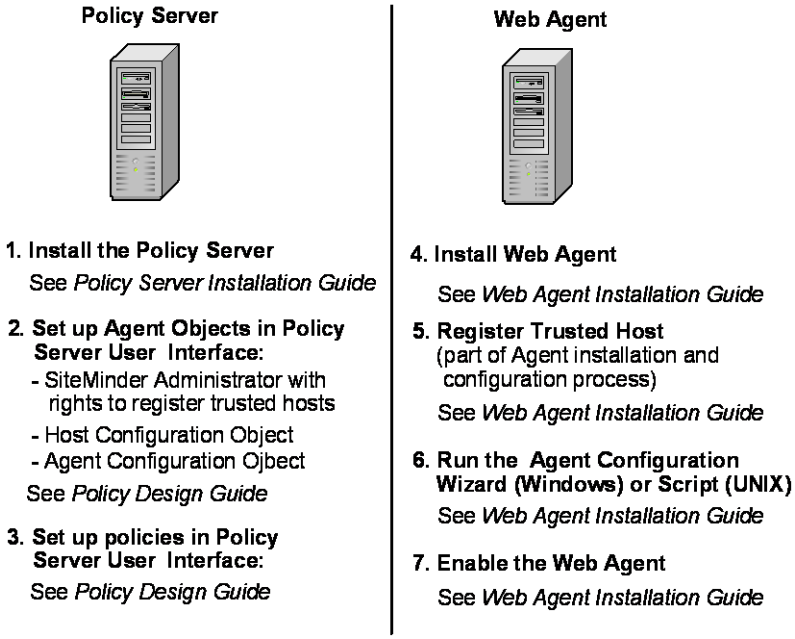
   Note: If the system displays a "Remove Shared File?" message, click Yes to All.
4. When the uninstall is finished, click Done.

   The SiteMinder documentation is removed.

Chapter 2: Installing the Policy Server on UNIX Systems

This section contains the following topics:

Quick Installation Overview



UNIX Installation Overview

This chapter describes how to install the Policy Server on a UNIX system, which includes running a setup program and configuring the web server. When you install the Policy Server on a UNIX system, you can use the Policy Server installer to configure the SiteMinder policy store automatically in one of the following:

- Sun™ Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet)
- Microsoft Active Directory® Application Mode (ADAM)
- Microsoft Active Directory™ Lightweight Directory Services (AD LDS)

For other supported LDAP and relational database vendors, you configure the policy store manually after installing the Policy Server. These manual steps are outlined in this guide.

Audit logs can be stored in either an ODBC database (SQL Server or Oracle) or a text file. After you install the Policy Server, audit logging is set to a text file and not to ODBC by default.

System Requirements

Before you install the Policy Server, make sure you are using a supported operating system and third-party software. For a list of supported operating systems, Web Servers, databases, Web browsers, LDAP Directory Servers, and servlet engines, go to the Technical Support site and search for the SiteMinder Platform Matrix for 6.0.

Make sure you have the following components installed on your machine:

- Memory: 512 MB RAM
- Free disk space: 300 MB free disk space and 200 MB free disk space in /tmp.

  Note: Typically, 10 MB or less free disk space in /tmp is required for the daily operation of the Policy Server. The Policy Server creates files and named pipes under /tmp. The path to which these files and pipes are created cannot be changed.
- Screen resolution: 800 x 600 or higher resolution with 256 colors or better to properly view the Policy Server User Interface. Web browsers running on a display with less than 256 colors cannot properly display the Policy Server User Interface.
- JRE: Make sure you have the required JRE version installed. For the required version, search for the SiteMinder Platform Matrix for 6.0 on the Technical Support site. You can download the latest JRE version at the Sun Developer Network (SDN).

Note: To run the OneView Monitor user interface, you need the required version of Java SDK and ServletExec/AS for UNIX installed. For the required versions, search for the SiteMinder Platform Matrix for 6.0 on the Technical Support site. You also need ServletExec for Password and Registration Services.

Solaris 10 Zone Support

A SiteMinder Policy Server is supported in:

- Global zones
- Sparse-root zones
- Whole-root zones

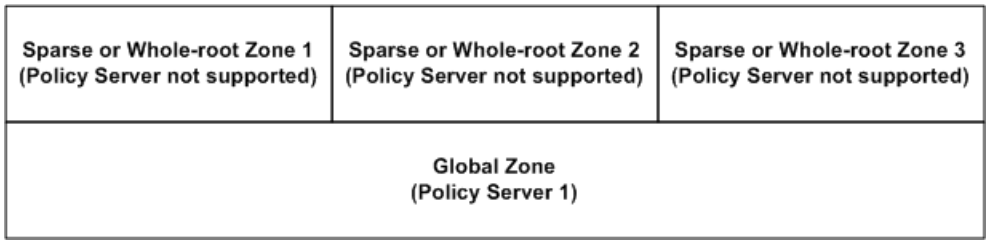
Consider the following scenarios when planning to run one or more Policy Servers in a Solaris 10 environment.

Global Zone Support

A global zone configuration limits the implementation to a single Policy Server instance across all zones. Specifically:

- Only a single Policy Server instance is supported on the global zone.
- A Policy Server instance is not supported on a sparse-root zone if there is another Policy Server instance on the global zone.
- A Policy Server instance is not supported on a whole-root zone if there is another Policy Server instance on the global zone.

Example: Global zone support



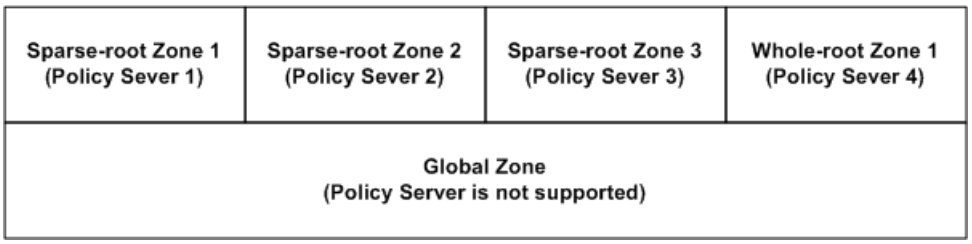
Note: Web Agents, however, may run concurrently in any zone.

Sparse-root Zone Support

A sparse-root zone configuration supports multiple Policy Server instances running on multiple sparse-root zones. Specifically:

- Only one Policy Server instance is supported on each sparse-root zone.
- Concurrent Policy Server instances are supported on sparse-root zones and whole-root zones, so long as there is only one Policy Server instance on each sparse-root or whole-root zone.
- Policy Server instances are not supported running concurrently on the global zone and on sparse-root zones.

Example: Sparse-root zone support



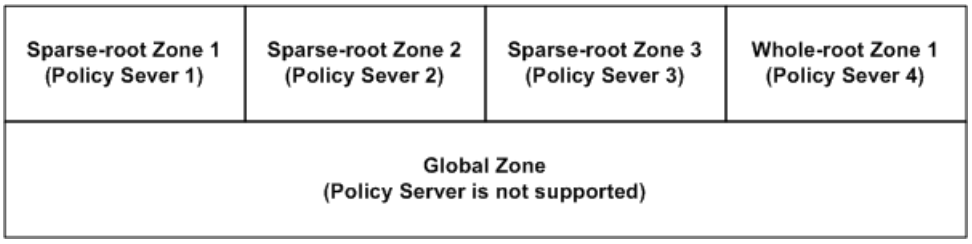
Note: Web Agents, however, may run concurrently in any zone.

Whole-root Zone Support

A whole-root zone configuration supports multiple Policy Server instances running on multiple whole-root zones. Specifically:

- Only one Policy Server instance is supported on each whole-root zone.
- Concurrent Policy Server instances are supported on whole-root zones and sparse-root zones, so long as there is only one Policy Server instance on each whole-root zone or sparse-root zone.
- Policy Server instances are not supported running concurrently on the global zone and on whole-root zones.

Example: Whole-root zone support



Note: Web Agents, however, may run concurrently in any zone.

Solaris and HP-UX Patches

For a list of required and recommended Solaris and HP–UX patches, see the *Policy Server Release Notes*.

Before You Begin

Before you install the Policy Server, complete the following procedures, if applicable:

- Create a new UNIX account (see page 45).
- Modify the UNIX system parameters (see page 46), if necessary.

- Unset the localization variables (see page 46), if necessary.
- Install the documentation (see page 47).
- (Linux) Be sure that the required Linux libraries are installed to the Policy Server host system. For more information, see Required Linux Libraries.
- (**IBM Directory Server**) If you are using IBM Directory Servers in your SiteMinder environment, edit the V3.matchingrules file by adding the following line:

  ```
  MatchingRules=(2.5.13.15 NAME 'integerOrderingMatch' SYNTAX
  1.3.6.1.4.1.1466.115.121.1.27
  ```

  The Directory store will not be configured correctly and the necessary SiteMinder objects will not be created if the V3.matchingrules file does not contain the change.
- Stop the web server instance to allow the installation program to configure the Policy Server User Interface.
- Trim the pre–SiteMinder system path to approximately 700 characters. The Policy Server installation fails if the system path length exceeds 1024 characters, including or excluding the directories SiteMinder adds.

Note: The Policy Server and Documentation installations each modify environment variables.

More information:

Modified UNIX Environment Variables (see page 240)

Create a New UNIX Account

Create a new UNIX account named smuser with the default shell as ksh. You may also need to modify the profile for the smuser account, as indicated later in this chapter.

Important! You should install the Policy Server using the smuser UNIX account, but do not configure the Sun Java System or Apache on Linux Web Server for the Policy Server User Interface or the OneView Monitor GUI because the installer modifies the Web server's configuration files and smuser does not have the appropriate root privileges. Thus, when you run the Policy Server installer, do not select Web Server(s) or OneView Monitor when prompted to choose components.

After the Policy Server installation is complete, run the Policy Server Configuration Wizard (located in *siteminder_installation*\install_config_info\nete-ps-config.bin) as root to configure the Policy Server User Interface or the OneView Monitor GUI.

UNIX System Parameters

When the Policy Server is placed under load, it opens a large number of sockets and files. This can become a problem if the default limit parameters are not appropriate for the load.

To view the default limit parameters, type ulimit -a. The system displays a message similar to the following:

```
$ ulimit -a
time(seconds)                   unlimited
file(blocks)                    unlimited
data(kbytes                     2097148
stack(kbytes)                   8192
coredump(blocks)                unlimited
nofiles(descriptors)            256
vmemory(kbytes)                 unlimited
```

The nofiles parameter is set to 256 in this example. This is the total number of files (sockets + files descriptors) that this shell and its descendants have been allocated. If this parameter is not set high enough, the Policy Server returns numerous socket errors. The most common socket error is 10024, or too many open files. You must increase this parameter value for proper Policy Server operation under load. You can change this value by running the ulimit -n command. For example, to set nofiles to 1024, place the ulimit -n 1024 command in the .profile or smprofile.ksh of the smuser account. The Policy Server is bound by the nofiles parameter within smuser's ulimit for the number of connections to it.

Note: On HP-UX systems, prior to the Policy Server installation, check your .profile file for a set +u option. If it has a set -u option, do a set +u to nullify it. A setting of set -u will cause a problem when the installation sets a SHLIB_PATH for smuser.

Localization Requirement

Use of the LC_* environment variables for localization is not permitted.

If the LC_* variables are set by default, they must be unset in the .profile or smprofile.ksh files of the smuser account.

The LANG environment variable should also be unset. To unset the variable, add the unset LANG command to the smprofile.ksh file.

Required Linux Libraries

If you are installing or upgrading a Linux version of this component, the following is required on the host system:

`compat–libstdc++–33.3.2.3–patch_version.i386.rpm`

Install this rpm to be sure that you have the appropriate 32-bit C run–time library for your operating system.

Install the SiteMinder Documentation

For 6.x, you install the documentation separately using the documentation installation program. The documentation is not installed by default with the Policy Server. We recommend that you install the documentation before the Policy Server.

To install the SiteMinder documentation

1. Log in as smuser or as the user who installed the Policy Server.

   Note: This user must have sufficient privileges to modify the web server and ServletExec configuration files. The installer modifies these files to configure the Policy Server User Interface and the OneView Monitor.

2. Download the documentation kit from the Technical Support site and save one of the following installation executables to a temporary location:

   - nete-sm-doc-6.0-sp6-sol.bin
   - nete-sm-doc-6.0-sp6-aix.bin
   - nete-sm-doc-6.0-sp6-rhel30.bin
   - nete-sm-doc-6.0-sp6-hp.bin

   Depending on your permissions, you may need to add executable permissions to the install file by running the following command:

   chmod +x nete-sm-doc-6.0-sp6-*os*.bin

To use the GUI mode

1. Open a command window and navigate to where the install program is located.
2. Enter the following command:

   `sh ./nete-sm-doc-6.0-sp6-os.bin`

   os

   Specifies sol, aix, linux, or hp.

To use the console mode

1. Open a command window and navigate to where the install program is located.
2. Enter the following command:

   ```
   sh ./nete-sm-doc-6.0-sp6-os.bin -i console
   ```

   os

   Specify sol, aix, linux, or hp.

   Solaris example: sh ./nete-sm-doc-6.0-sp6-sol.bin -i console

   Note: The -i console part of the command lets you run the installation in a console instead of a GUI.
3. To view the Introduction/License Agreement, press ENTER when prompted.

   The installation script displays the License Agreement.
4. Enter **y** to agree with the terms and continue the installation.
5. Read the Installation/Release Notes and press ENTER.
6. Enter the installation directory.
7. Review the Pre–Installation Summary and press ENTER to install the documentation.

   The installation program installs the documentation in the directory you specified.
8. Press ENTER to exit the installer.

If you have installed the documentation after installing the Policy Server, create the netegrity_docs virtual directory on the web server. This directory lets you view the documentation using the Policy Server User Interface. You can run the Policy Server Configuration Wizard to create the directory or you can manually create it for IIS 5.0/6.0.

More Information:

Run the Configuration Wizard Using a GUI or Console Window (see page 66)
Manually Edit the netegrity_docs Virtual Directory (see page 71)

Run the Policy Server Setup

The following sections detail how to run the Policy Server setup.

Important Considerations Before Installation

Be aware of the following:

- The Policy Server install requires 200 MB of free space in /tmp.
- If you are installing the Policy Server using telnet or other terminal emulation software, complete the installation using a console window, as described in Run the Installation Script Using a UNIX Console Window (see page 58). If you do not, the installer throws an Java exception and exits if you try to run a GUI through a telnet window.
- Running the Policy Server installer or Policy Server Configuration Wizard using an Exceed X-windows application can cause text in the dialog box to truncate due to unavailable fonts using Exceed. This limitation has no affect on the Policy Server installation or configuration.
- Be sure that you use the correct installation program on Red Hat Advanced Server (AS) for Linux. For Red Hat AS 3.0, use nete-ps-6.0-sp6-rhel30.bin.
- To avoid possible policy store corruption, be sure that the server on which the policy store will reside is configured to store objects in UTF-8 form. For more information on configuring your server to store objects in UTF-8 form, see the documentation for that server.

Run the Installer Using a Graphical User Interface

To install the Policy Server using a GUI

1. Exit all applications that are running.

   After installation, you can find the installation log files in *siteminder_home*/install_config_info. The file names are:

   - CA_SiteMinder_Policy_Server_v6.0_SP6_InstallLog.log
   - nete-ps-details.log

     If you use the Policy Server installer to configure the policy store automatically, the nete-ps-details.log file lets you determine the status of the policy store after it has been configured.

2. Download the Policy Server installation kit from the Technical Support site and save one of the following installation executables to a temporary location:

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

- nete-ps-6.0-sp6-rhel30.bin.
- nete-ps-6.0-sp6-hp.bin.

Depending on your permissions, you may need to add executable permissions to the install file by running the following command:

```
chmod +x nete-ps-6.0-sp6-os.bin
```

Important! The Policy Server installer can crash when executed across different subnets. Install the Policy Server directly on the host system to prevent this problem.

3. Open a command window, navigate to the installation executable, and enter:

   ```
   sh ./nete-ps-6.0-sp6-os.bin
   ```

   os

   Specifies sol, rhel30, or hp.

   Setup verifies the following prerequisites:

   - You are logged into an account with local administrator privileges.
   - You have the appropriate operating system and web server listed on the SiteMinder Platform Support Matrix. To access this matrix, go to the Technical Support site and search for the SiteMinder Platform Support Matrix.
   - The computer has necessary free disk space and the required JDK or JRE versions installed. For the required versions, search for the SiteMinder Platform Support Matrix on the Technical Support site.

4. In the first Introduction dialog, be sure that the system has the prerequisites listed and click Next. If not, stop the installation and install the required prerequisites.

   Note: The installer runs smpatchcheck to confirm that you have the required/recommended patches installed on the operating system. For a list of these patches, see the *Policy Server Release Notes*.

5. (Optional) If the installer cannot locate the JRE, it prompts you for the location. Enter the appropriate location.

6. Read the Software License Agreement, accept the terms if you agree, and click Next.

7. Read the Release Notes, then click Next.

8. Enter your name and company name and click Next.

9. Accept the default Policy Server installation location or select a different one and click Next. If necessary, click Choose to browse to the appropriate location.

   Note: If you cut and paste a path, the Next button is disabled. Type a character to enable the Next button.

10. Enter the full path to the web browser on this system, including the executable, and click Next.

    Note: The installer uses this information to make the SiteMinder documentation available from Policy Server User Interface.

11. Select Yes or No to add the smprofile.ksh to the .profile file and click Next.

12. In the Encryption Key dialog, complete the following:

    a. Enter a case–sensitive, alphanumeric encryption key. The encryption key is a key that secures data sent between the Policy Server and the policy store. The key can be from 6 to 24 characters in length. All policy servers that share a SiteMinder policy store must be configured using the same encryption key. For stronger protection, define a long encryption key.

    b. Re–enter the key to confirm the entry.

    c. Take note of this key for future reference and click Next.

13. In the Choose Features dialog, select which Policy Server features you want and click Next.

    OneView Monitor GUI

    The install program configures the OneView Monitor GUI to work on the web server you specify later in this procedure.

    Note: To use the OneView Monitor, you must have the required version of Java SDK and ServletExec/AS installed. For the required versions, search for the SiteMinder Platform Matrix for 6.0 on the Technical Support site.

    Web Server(s)

    The install program configures the Policy Server User Interface and, if selected, the OneView Monitor to work on this web server.

    SNMP

    The install program configures SNMP to work with the Policy Server.

    Note: The password of the root user and a native SunSolstice Master Agent are required to enable SNMP support.

    Policy Store

    The install program configures an LDAP directory server as a policy store.

Additional Considerations

- You are installing the Policy Server using the smuser UNIX account. Do not configure the Sun Java System or Apache on Linux web server for the Policy Server User Interface or the OneView Monitor GUI. The installer modifies the web server configuration files and smuser does not have the appropriate root privileges. After the Policy Server installation is complete, run the Policy Server Configuration Wizard, which is located in *siteminder_home*/install_config_info/nete-ps-config.bin, as root to configure the Policy Server User Interface or the OneView Monitor GUI.
- The installer can automatically configure an LDAP directory server as a policy store. You can automatically configure the policy store in an instance of Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet), ADAM, or AD LDS. For other supported LDAP or relational database vendors, you configure the policy store manually after installing the Policy Server.

Note: If there is a problem with configuring the policy store, you can run the Policy Server Configuration Wizard, which is located in *siteminder_home/*install_config_info/nete-ps-config.bin, to fix the issue.

14. (Optional) If you specified that the installer configure the OneView Monitor GUI, specify the following ServletExec information:
    a. Enter the ServletExec installation directory.

       Example: /usr/local/NewAtlanta/ServletExecAS

    b. Enter the port number for the ServletExec instance.
    c. (Optional) If you have multiple ServletExec instances, select the se-*hostname*-server you want to configure for the OneView Monitor GUI
    d. Click Next.
15. Enter the path to the root folder of a supported web server and click Next.
16. Select the web server you want to configure with the Policy Server and click Next.

    Note: Consider the following:

    - Be sure that the web server instance is stopped.
    - If you have multiple web servers, only select one. We recommend configuring one web server at a time. Use the Policy Server Configuration Wizard to configure additional web servers after installing the Policy Server. See Configure Additional Web Server Instances for the Policy Server for more information.
    - If you are installing the Policy Server before the documentation, you are prompted to run the Policy Server Configuration Wizard to create the netegrity_docs virtual directory on the web server. This virtual directory lets you view the documentation using the Policy Server User Interface.

17. In the first Policy Store dialog, select whether you want to configure a new policy store or update an existing one.
18. In the second Policy Store dialog for the LDAP Server, click Next, and configure ADAM, AD LDS, or Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) as a policy store (see page 53).

    Note: For other supported LDAP or relational database vendors, configure the policy store manually after installing the Policy Server.

More Information:

LDAP Directory Servers as a Policy or Key Store (see page 81)
Relational Databases as a Policy or Key Store (see page 111)
Run the Configuration Wizard Using a GUI or Console Window (see page 66)

Configure an LDAP Policy Store During the GUI Installation

The following procedures assume that you are running the Policy Server installer to configure a policy store automatically.

For a list of supported LDAP directory servers, see the SiteMinder Platform Support Matrix. To access this matrix, go to the Technical Support site and search for the SiteMinder Platform Support Matrix for 6.0.

To configure the LDAP directory server, you are required to supply the following:

- The IP address and port of the LDAP server
- The root DN under which the SiteMinder schema is placed
- The administrator information for the LDAP directory

Note: This installation cannot be completed using an SSL connection.

If the Policy Server installer automatically configures the policy store, the installer does not configure ODBC data sources. If you migrate your policy store to an ODBC database, you are required to create the ODBC data sources manually

Configure ADAM/AD LDS as a Policy Store

To configure ADAM/AD LDS as a policy store

1. Be sure that you have met the prerequisites for configuring ADAM/AD LDS as a policy store (see page 98).
2. When prompted by the installer to configure the policy store, enter the following information:

   IP address

   Specifies the IP Address of the directory server host system.

   Port number

   Specifies the port on which the directory server instance is listening.

   Root DN

   Specifies the root DN location of the application partition in the directory server where the policy store schema must be installed.

   Example: dc=netegrity,dc=com.

   Admin DN

   Specifies the full domain name, including the guid value, of the directory server administrator.

   Example: CN=user1,CN=People,CN=Configuration,CN={guid}

   Admin password

   Specifies the password of the directory server administrator.
3. In the next Policy Store dialog, specify if a different LDAP user account is to administer the policy store.

   By default, SiteMinder uses the LDAP administrator account to administer the policy store. You have the option to have the policy store administered through a different LDAP user account. The complete DN for the user is required to configure SiteMinder this way.

   Note: This user must have all the necessary privileges to modify attributes and change passwords.

   - If you do not want to use a different LDAP account, click Next.
   - If you want to use a different LDAP account, do the following:

     a. Select Use different LDAP user.

     b. Enter the DN of the LDAP user.

c. Enter the password for the specified account.

d. Confirm the password for the specified account.

e. Click Next.

Example: uid=SMAdmin,ou=people,o=security.com

4. In the next Policy Store dialog, select Initialize LDAP instance only if you are initializing a new LDAP instance and click Next.

5. For the SiteMinder super user password, complete the following:

   a. Enter a password for the SiteMinder super user account. The pre–defined SiteMinder super user account has maximum SiteMinder privileges. The password can be from 6 to 24 characters in length.

      Note: The password is case–insensitive, except in cases where the password is stored in an Oracle policy store.

   b. Re–enter the password.

      Important! Take note of the password. You use this password to log into the Policy Server User Interface for the first–time. You can change the password using the Policy Server Management Console.

      Note: We recommend that you do not use this account for day–to–day operations. Instead, use this account to access the Policy Server User Interface for the first–time to create another SiteMinder administrator with system–wide privileges. For more information about the Policy Server Management Console, see the *Policy Server Management Guide*.

6. Review the settings in the Pre–Configuration Summary dialog and click Install.

   The installation program begins copying files to your system. The installation can take a few minutes.

7. Click Done to complete the installation and reboot your system.

   If there were problems during the installation, see the Policy Server installation log file (CA_SiteMinder_Policy_Server_v6.0_SP6_InstallLog.log), which is located in *siteminder_home/*install_config_info.

8. (Optional) Access the Policy Server User Interface.

More Information:

Access the Policy Server User Interface (see page 72)

Configure a Sun Java System Directory Server Enterprise Edition as a Policy Store

To configure Sun Java System Directory Server Enterprise Edition as a policy store

1. In Policy Store dialog for the LDAP server:
   a. Enter the IP address of the LDAP directory host system.
   b. Enter the port on which the directory server instance is listening.
   c. Enter the root DN. Specify the root DN as the following:

      o=*root_DN*

      root_DN

      Specifies the root DN.
   d. Click Next.
2. In the next Policy Store dialog:
   a. Enter the user name (Bind DN) for the LDAP administrator account.

      Example: cn=Directory Manager
   b. Enter the password for the administrator DN account.
   c. Confirm the password.
   d. Click Next.
3. In the next Policy Store dialog, specify if a different LDAP user account is to administer the policy store.

   By default, SiteMinder uses the LDAP administrator account to administer the policy store. You have the option to have the policy store administered through a different LDAP user account. The complete DN for the user is required to configure SiteMinder this way.

   - If you do not want to use a different LDAP account, click Next.
   - If you want to use a different LDAP account, do the following:
     a. Select Use different LDAP user.
     b. Enter the DN of the LDAP user.

        Example: uid=SMAdmin,ou=people,o=security.com.
     c. Enter and confirm the password for the specified account.
     d. Click Next.
4. In the next Policy Store dialog, select Initialize LDAP instance only if you are initializing a new LDAP instance and click Next.

5. For the SiteMinder super user password, complete the following:

   a. Enter a password for the SiteMinder super user account. The pre–defined SiteMinder super user account has maximum SiteMinder privileges. The password can be from 6 to 24 characters in length.

      Note: The password is not case–sensitive, except when the password is stored in an Oracle policy store.

   b. Re–enter the password.

      Important! Take note of the password. You use this password to log into the Policy Server User Interface for the first–time. You can change the password using the Policy Server Management Console.

      Note: We recommend that you do not use this account for day–to–day operations. Instead, use this account to access the Policy Server User Interface for the first–time to create another SiteMinder administrator with system–wide privileges. For more information about the Policy Server Management Console, see the *Policy Server Management Guide*.

   c. Click Next.

6. Review the settings in the Pre–Configuration Summary and click Install.

   The installation program begins copying files to your system. The installation can take a few minutes.

7. Click Done to complete the installation and reboot your system.

   If there were problems during the installation, you can find the installation log files in *siteminder_home/*install_config_info.

   The file names are:

   - CA_SiteMinder_Policy_Server_v6.0_SP6_InstallLog.log
   - nete-ps-details.log

     The nete-ps-details.log file lets you determine the status of the policy store.

8. (Optional) Access the Policy Server User Interface.

More Information:

Access the Policy Server User Interface (see page 72)

Run the Installation Script Using a UNIX Console Window

You can run the installation script using a UNIX console window.

Important! The Policy Server installer can crash when executed across different subnets. Install the Policy Server directly on the host system to prevent this problem.

To run the installation script with a console window

1. Close all programs.

   Note: Be sure that you install the Policy Server as the same UNIX user you used for installing the documentation.

2. Download the Policy Server installation kit from the Technical Support site and save one of the following installation executables to a temporary location:

   - nete-ps-6.0-sp6-sol.bin
   - nete-ps-6.0-sp6-rhel30.bin
   - nete-ps-6.0-sp6-hp.bin

   Note: Depending on your permissions, you may need to add executable permissions to the install file.

   Example: chmod +x nete-ps-6.0-sp6-sol.bin

3. In a UNIX shell, enter the following command:

   ```
   sh ./nete-ps-6.0-sp6-os.bin -i console
   ```

   os

   Specifies sol, rhel, or hp

   Solaris example: sh ./nete-ps-6.0-sp6-sol.bin -i console

   Setup verifies the following prerequisites:

   - You have the appropriate UNIX system permissions to install the Policy Server for the location you specify during installation and can modify web server configuration files.
   - You have the appropriate operating system and web server listed on the SiteMinder Platform Support Matrix for 6.0. To access this matrix, go to the Technical Support site and search for the SiteMinder Platform Support Matrix for 6.0.
   - The computer has necessary free disk space and the required JDK or JRE version installed. For the required versions, search for the SiteMinder Platform Support Matrix for 6.0 on the Technical Support site.
   - The system has the required/recommended patches installed.

After installation, you can find the installation log file in *siteminder_home*/install_config_info.

The file name is CA_SiteMinder_Policy_Server_v6.0_SP6_InstallLog.log.

4. Read the introduction and press Enter.

   The installation program runs smpatchcheck to verify that you have the required/recommended UNIX operating system patches are installed. If the patches are not installed, the installer aborts and tells you which patches are needed.

5. Enter the JRE directory.

6. The installer displays the License Agreement. Press Enter to read the complete agreement.

7. If you agree with License Agreement terms, enter y to continue the installation.

8. Read the Installation Notes for important information about installing SiteMinder and press Enter to continue.

9. Enter your name and press Enter.

10. Enter your company name and press Enter.

11. Specify a directory path under which the SiteMinder installation directory must be created or press Enter to use the default location.

    The installation script creates a siteminder directory in the specified location. For example, if you specify /opt, then this product is installed in /opt/siteminder. If the siteminder installation directory exists, be sure that the installation user account has proper file permissions to create a subdirectory.

12. Enter **Y** to confirm Policy Server installation location.

13. Enter the full path to the web browser on this system, including the executable. The installation program needs this information for the Policy Server User Interface online help system.

14. Enter **1** if you want the smprofile.ksh added to the .profile file.

15. Enter the Encryption Key:

    - If you are installing the first Policy Server in a multiple Policy Server deployment, specify a random, case–sensitive string from 6 through 24 characters long.
    - If you have already installed a Policy Server and this Policy Server is part of the same site, enter the Encryption Key you specified during that installation.

    The encryption key is a key that secures data sent between the Policy Server and the policy store. All Policy Servers that share a SiteMinder policy store must be configured using the same encryption key. For stronger protection, define a long encryption key.

16. In the Choose Features section, enter the numbers (separated by commas) of the Policy Server features you want. The OneView Monitor GUI, Web Server(s), and LDAP Policy Store are selected by default.

    Note: To select none of the features, enter a "," (comma).

    OneView Monitor GUI

    The install program configures the OneView Monitor GUI to work on the web server you specify later in this procedure.

    Note: To use the OneView Monitor, you must have the required Java SDK and ServletExec AS for UNIX/Sun Java System installed. For the required versions, search for the SiteMinder Platform Matrix for 6.0 on the Technical Support site.

    Web Server(s)

    The install program configures the Policy Server User Interface and, if specified, the OneView Monitor to work on this web server.

    SNMP

    The install program configures SNMP to work with the Policy Server.

    Note: The password of the root user and a native SunSolstice Master Agent are required to enable SNMP support**.**

    Policy Store

    The install program configures an LDAP directory server as a policy store.

    Additional Considerations:

    - You are installing the Policy Server using the smuser UNIX account. Do not configure the Sun Java System or Apache on Linux web server for the Policy Server User Interface or the OneView Monitor GUI. The installer modifies the web server configuration files and smuser does not have the appropriate root privileges. After the Policy Server installation is complete, run the Policy Server Configuration Wizard, which is located in *siteminder_home*/install_config_info/nete-ps-config.bin, as root to configure the Policy Server User Interface or the OneView Monitor GUI.
    - The installer can automatically configure an LDAP directory server as a policy store. You can automatically configure the policy store in an instance of Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet), ADAM, or AD LDS. For other supported LDAP or relational database vendors, you configure the policy store manually after installing the Policy Server.

    Note: If there is a problem with configuring the policy store, you can run the Policy Server Configuration Wizard, which is located in *siteminder_home/*install_config_info/nete-ps-config.bin, to fix the issue.

17. (Optional) If you chose to have the OneView Monitor GUI configured, enter the JDK directory.

18. (Optional) If you chose to have the OneView Monitor GUI configured, enter the ServletExec installation directory for the OneView Monitor GUI.

    Example: /usr/local/NewAtlanta/ServletExecAS

    a. Enter a free port number.

    b. If you have multiple ServletExec instances, select the se-*hostname*-server you want to configure for the Monitor GUI and press Enter.

19. Enter the path to the root folder of a supported web server and press Enter.

20. Specify the web server you want to configure with the Policy Server and press Enter.

    Note: Consider the following:

    - Be sure that the web server instance is stopped.
    - If you have multiple web servers, only select one. We recommend configuring one web server at a time. Use the Policy Server Configuration Wizard to configure additional web servers after installing the Policy Server. See Configure Additional Web Server Instances for the Policy Server for more information.
    - If you are installing the Policy Server before the documentation, you are prompted to run the Policy Server Configuration Wizard to create the netegrity_docs virtual directory on the web server. This virtual directory lets you view the documentation using the Policy Server User Interface.

21. At the Policy Store - LDAP server prompt configure ADAM, AD LDS, or Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) as a policy store (see page 62).

Note: For other supported LDAP or relational database vendors, configure the policy store manually after installing the Policy Server.

More Information:

LDAP Directory Servers as a Policy or Key Store (see page 81)
Relational Databases as a Policy or Key Store (see page 111)
Run the Configuration Wizard Using a GUI or Console Window (see page 66)

Configure an LDAP Policy Store During the Console Installation

The following instructions assume you have completed the Policy Server setup procedure by running the installation script using a UNIX console window.

For a list of supported LDAP directory servers, see the SiteMinder Platform Support Matrix. To access this matrix, go to the Technical Support site and search for the SiteMinder Platform Support Matrix for 6.0.

To configure the LDAP directory server, you are required to supply the following:

- The IP address and port of the LDAP server
- The root DN under which the SiteMinder schema is placed
- The administrator information for the LDAP directory

Note: This installation cannot be completed using an SSL connection.

If the Policy Server installer automatically configures the policy store, the installer does not configure ODBC data sources. If you migrate your policy store to an ODBC database, you are required to create the ODBC data sources manually.

Configure ADAM/AD LDS as a Policy Store

To configure ADAM/AD LDS as a policy store

1. Be sure that you have met the prerequisites for configuring ADAM/AD LDS as a policy store (see page 98).
2. When prompted by the installer to configure the policy store, enter the following information:

   IP address

   Specifies the IP Address of the directory server host system.

   Port number

   Specifies the port on which the directory server instance is listening.

   Root DN

   Specifies the root DN location of the application partition in the directory server where the policy store schema must be installed.

   Example: dc=netegrity,dc=com.

Admin DN

Specifies the full domain name, including the guid value, of the directory server administrator.

Example: CN=user1,CN=People,CN=Configuration,CN={guid}

Admin password

Specifies the password of the directory server administrator.

3. Specify if a different LDAP user account is to administer the policy store.

   To select no user, enter a "," (comma).

   By default, SiteMinder uses the LDAP administrator account to administer the policy store. You have the option to have the policy store administered through a different LDAP user account. The complete DN for the user is required to configure SiteMinder this way.

   Note: This user must have all the necessary privileges to modify attributes and change passwords.

   - If you accept the default go to the next step.
   - If you enter a number do the following:

     a. When prompted, Enter the DN of the LDAP user.

     b. Enter the password for the specified account.

     c. Confirm the password for the specified account.

     Example: uid=SMAdmin,ou=people,o=security.com

4. Enter **1** to initialize a new 6.x policy store.

   Note: If you do not want to initialize a new policy store, enter a "," (comma).

5. For the SiteMinder super user password, complete the following:

   a. Enter a password for the SiteMinder super user account. The pre–defined SiteMinder super user account has maximum SiteMinder privileges. The password can be from 6 to 24 characters in length.

      Note: The password is not case–sensitive, except in cases where the password is stored in an Oracle policy store.

   b. Take note of the password. You use this password to log into the Policy Server User Interface for the first–time. You can change the password using the Policy Server Management Console.

      Note: For more information about the Policy Server Management Console, see the *Policy Server Management Guide*.

6. In the Pre–Configuration Summary, be sure that all settings are accurate and press Enter.

   The installation program begins copying files to your system. The installation can take a few minutes.

7. After the installation is complete, press Enter to exit the installer.

   Note: If you configured SNMP, restart the SNMP daemon by entering sh S76snmpdx stop and sh S76snmpdx start in /etc/rc3.d.

8. (Optional) Access the Policy Server User Interface.

More Information:

Access the Policy Server User Interface (see page 72)
LDAP Directory Servers as a Policy or Key Store (see page 81)
Relational Databases as a Policy or Key Store (see page 111)

Configure a Sun Java System Directory Server Enterprise Edition as a Policy Store

To configure a Sun Java System Directory Server Enterprise Edition as a policy store

1. For the LDAP server:
   - Enter the IP address of the LDAP directory host system.
   - Enter the port on which the directory server instance is listening.
   - Enter the root DN. Specify the root DN as the following:

     o=*root_DN*

     root_DN

     Specifies the root DN.

2. For the LDAP administrator:
   - Enter the user name (Bind DN) for the LDAP administrator account.

     Example: cn=*Directory Manager*

     Directory Manager

     Specifies the Bind DN SiteMinder uses to bind to the LDAP server.
   - Enter the password for the administrator DN account.
   - Confirm the password.

3. Specify if a different LDAP user account is to administer the policy store.

   Note: To select no user, enter a "," (comma).

   By default, SiteMinder uses the LDAP administrator account to administer the policy store. You have the option to have the policy store administered through a different LDAP user account. The complete DN for the user is required to configure SiteMinder this way.
   - If you accept the default go to the next step.

- If you enter a number do the following:
  a. When prompted, Enter the DN of the LDAP user.
  b. Enter the password for the specified account.
  c. Confirm the password for the specified account.

  Example: uid=SMAdmin,ou=people,o=security.com.

4. Enter **1** to initialize a new 6.x policy store.

   Note: If you do not want to initialize a new policy store, enter a "," (comma).

5. For the SiteMinder super user password, complete the following:
   a. Enter a password for the SiteMinder super user account. The pre–defined SiteMinder super user account has maximum SiteMinder privileges. The password can be from 6 to 24 characters in length.

      Note: The password is not case–sensitive, except in cases where the password is stored in an Oracle policy store.

   b. Take note of the password. You use this password to log into the Policy Server User Interface for the first–time. You can change the password using the Policy Server Management Console.

      Note: For more information about the Policy Server Management Console, see the *Policy Server Management Guide*.

6. In the Pre–Configuration Summary, be sure that all settings are accurate and press Enter.

   The installation program begins copying files to your system. The installation can take a few minutes.

7. After the installation is complete, press Enter to exit the installer.

   Note: If you configured SNMP, restart the SNMP daemon by entering sh S76snmpdx stop and sh S76snmpdx start in /etc/rc3.d.

8. (Optional) Access the Policy Server User Interface.

More Information:

Access the Policy Server User Interface (see page 72)
LDAP Directory Servers as a Policy or Key Store (see page 81)
Relational Databases as a Policy or Key Store (see page 111)

Run the Configuration Wizard Using a GUI or Console Window

The Policy Server Configuration Wizard lets you configure the following:

- The OneView Monitor GUI
- The Policy Server User Interface
- The netegrity_docs virtual directory on a web server
- SNMP support
- A policy store

The wizards gives you the option of using either a GUI or a console window.

When configuring a policy store, the wizard can automatically configure Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet), ADAM, or AD LDS as a policy store. If another supported LDAP directory server or relational database is to function as the policy store, you configure the policy store manually.

Note: For more information about configuring other LDAP versions, see LDAP Directory Servers as a Policy Store or Key Store (see page 81).

Note: The Policy Server Configuration Wizard requires 150 MB of free space in /tmp.

To run the configuration wizard

1. Close all programs.

   Be sure that you run the wizard as the UNIX user that has sufficient privileges to modify the web server configuration files. The wizard modifies these files to configure the Policy Server User Interface.

2. Start the Policy Server Configuration Wizard by running one of the following commands:

   (GUI Mode)

   ```
   sh ./nete-ps-config.bin
   ```

   (Console Mode)

   ```
   sh ./nete-ps-config.bin -i console
   ```

Setup verifies the following prerequisites:

- You are logged into an account with local administrator privileges.
- You have the appropriate Policy Server environment variables set. The system has the required/recommended patches installed.

If you get a "Required variables not found" error, run the following script using a ksh shell from the SiteMinder installation directory, and then rerun the wizard:

```
. ./nete_ps_env.ksh
```

Note: Be sure that there is a space between the two periods (. .) when running the script.

3. In the Choose Features section:
   - For the GUI mode, select which Policy Server features you want. The OneView Monitor GUI, Web Server(s), and Policy Store are selected by default.
   - For the console mode, enter the numbers (separated by commas) of the Policy Server features you want. The OneView Monitor GUI, Web Server(s), and Policy Store are selected by default. To select none of the features, enter a "," (comma).

   OneView Monitor GUI

   The install program configures the OneView Monitor GUI to work on the web server you specify later in this procedure.

   Note: To use the OneView Monitor, you require a supported Java SDK and ServletExec AS for UNIX/Sun Java System. For the required versions, search for the SiteMinder Platform Matrix for 6.0 on the Technical Support site.

   Web Server(s)

   The install program configures the Policy Server User Interface and, if specified, the OneView Monitor to work on this web server.

   SNMP

   The install program configures SNMP to work with the Policy Server.

   Note: The root user password and a native SunSolstice Master Agent are required to enable SNMP support.

   Policy Store

   The install program configures an LDAP directory server as a policy store.

4. (Optional) If you are configuring the OneView Monitor:
   a. Enter the ServletExec installation directory.

      Example: /usr/local/NewAtlanta/ServletExecAS

   b. Enter the port number for the ServletExec instance.
   c. (Optional) If you have multiple ServletExec instances, select the se–*hostname*–server to configure with the OneView Monitor GUI and press Enter.
5. Enter the path to the root folder of a supported web server.
6. Specify the web server you want to configure with the Policy Server.

   Note: Consider the following:

   - Be sure that the web server instance is stopped.
   - If you have multiple web servers, only select one. We recommend configuring one web server at a time. Use the Policy Server Configuration Wizard to configure additional web servers after installing the Policy Server. See Configure Additional Web Server Instances for the Policy Server for more information.
   - If you are installing the Policy Server before the documentation, you are prompted to run the Policy Server Configuration Wizard to create the netegrity_docs virtual directory on the web server. This virtual directory lets you view the documentation using the Policy Server User Interface.
7. (GUI mode only) For the first policy store prompt, select whether you want to configure a new policy store or update an existing one.
8. At the next policy store prompt, configure your policy store using either the GUI or console window.

More Information:

Configure an LDAP Policy Store During the Console Installation (see page 62)
Configure an LDAP Policy Store During the GUI Installation (see page 53)
Import Policy Data Using smobjimport (see page 150)
LDAP Directory Servers as a Policy or Key Store (see page 81)
Relational Databases as a Policy or Key Store (see page 111)

Configure Additional Web Server Instances for the Policy Server

If you have a Sun Java System web server instance configured for the Policy Server User Interface, OneView Monitor GUI, or SNMP support, do not configure new instances using the Policy Server Configuration Wizard.

If you run the wizard again, the existing web server configured for the Policy Server can fail. If you have run the wizard again and the web server instance fails, see backup versions of the obj.conf and magnus.conf files. These backup files let you return to the web server configuration that existed before running the Policy Server Configuration Wizard or installation program.

Backup Versions of Obj.conf and Magnus.conf Files

Each time you run the Policy Server Configuration Wizard, it creates backup versions of the obj.conf and magnus.conf files. These files allow you to return to the original Web server configuration you had before running the Policy Server Configuration Wizard or installation program. These backup versions are in the following format in the Web server's configuration directory:

obj.conf.*<year>-<month>-<date>-<hour>-<minutes>-<seconds>*.bak

magnus.conf.*<year>-<month>-<date>-<hour>-<minutes>-<seconds>*.bak

Example backup version are obj.conf.2003-11-25-16-58-47.bak and magnus.conf.2003-11-25-17-07-11.bak.

Run the Unattended Policy Server Installer

After you have installed the Policy Server on one system, you can reinstall it or install it on another system using an unattended installation mode. An unattended installation lets you install or uninstall the Policy Server without user interaction.

The installer provides a properties template (nete–ps–installer.properties) file that lets you pre–define installation variables. The default parameters, passwords, and paths in this file reflect the information you entered during the initial Policy Server installation.

In this file, you can either store encrypted or plain text passwords. If you are using encrypted passwords, for example, a shared secret or SiteMinder super user password, use the same values entered during the initial Policy Server installation. These passwords are encrypted in the file and cannot be modified. However, you can use plain text passwords by modifying the file.

The nete-ps-installer properties file is located in the *siteminder_home*/install_config_info directory.

siteminder_home

Specifies the Policy Server installation path.

To run the installer in the unattended installation mode

1. Modify the nete-ps-installer properties file with the settings you want.
2. From a Policy Server host system, copy the nete-ps-6.0-sp6-*os*.bin and nete-ps-installer.properties files to a temporary location, such as /tmp. Be sure that the UNIX user has the appropriate permissions to install from this directory.

   Note: To reinstall the Policy Server on the same system, copy these files to /tmp. To install the Policy Server on another system, copy these files to /tmp on that system.
3. From the /tmp directory, run the following command:

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

   os

   Specifies sol, rhel30, or hp.

The installer prompts that it is starting in unattended mode. When installing the Policy Server, the installer uses the parameters specified in the nete-ps-installer properties file. The -i silent setting instructs the installer to run in this unattended mode.

To stop the installation manually, press Ctrl + C.

To verify that the unattended installation completed successfully, see the CA_SiteMinder_Policy_Server_v6.0_SP6_InstallLog.log file in the *siteminder_home*/install_config_info directory. This log file contains the results of the installation.

More Information:

Configure Installation for Unattended Mode (see page 224)

Command Line Interface

The Command Line Interface allows you to write Perl scripts to configure and manage policy stores. The installation program installs a full version of Perl and puts the interface files in the *siteminder_home*/CLI directory

siteminder_home

Specifies the Policy Server installation path.

Example: /home/smuser/siteminder/CLI

To use the Command Line Interface, make sure the following directory is in your system's PATH environment variable before any other Perl bin directories on your machine.

For example: /home/smuser/siteminder/CLI/bin

Note: For more information on this interface, see the *Scripting Guide for Perl*.

Manually Edit the netegrity_docs Virtual Directory

For Sun Java System Web Servers:

As previously mentioned, we recommend that you install the documentation before the Policy Server. However, if did not do this and the documentation does not appear from the Policy Server User Interface you need to edit the netegrity_docs virtual directory.

To edit the netegrity_docs virtual directory

1. Open /<*sunjavasystem_home*>/servers/https-<*instance_name*>.domain.com/config/obj.conf, and ensure the following virtual directory entry in boldface points to the location where you installed the documentation:

   NameTrans fn="pfx2dir" from="/netegrity_docs" **dir="/export/smuser/netegrity/netegrity_documents**"

   Example: if you installed the documentation in another location such as /export/smuser/siteminder/netegrity_documents, change the /export/smuser/netegrity/netegrity_documents entry to the correct location.

2. After saving the obj.conf file, stop and restart the Web server, and the documentation should now appear from the Policy Server User Interface.

Next Steps

Now that you have installed the Policy Server on UNIX, complete the following:

1. Set up an LDAP directory server or relational database as a policy store to store your policy–related information. All Policy Servers in a SiteMinder installation must share the same policy store.

   Note: If you used the Policy Server installer or Policy Server Configuration wizard to configure the policy store automatically, you can skip this step.

2. Start the web server instance that the installer configured for the Policy Server User Interface.

3. Access the Policy Server User Interface.

4. Prepare the Policy Server for the Web Agent installation.
5. Install a Web Agent.

Note: For more information about installing a Web Agent, see the *Web Agent Installation Guide*.

More Information:

LDAP Directory Servers as a Policy or Key Store (see page 81)
Relational Databases as a Policy or Key Store (see page 111)
Access the Policy Server User Interface (see page 72)
How to Prepare the Policy Server for the Web Agent Installation (see page 74)

Access the Policy Server User Interface

Once you have installed the Policy Server and configured a policy store, access the Policy Server User Interface through a browser. Verify that the browser supports SiteMinder by entering the following URL:
http://www.netegrity.com/UItest

Note: The URL for the browser test is case-sensitive.

To access the Policy Server User Interface

1. On the Status tab of the Policy Server Management Console, be sure that the Policy Server is running.
2. Open a web browser and enter http://*host_name.domain*:*web_server_port* /siteminder.

   host_name

   Specifies the name of the Policy Server host system.

   domain

   Specifies the cookie domain of the Policy Server host system.

   web_server_port

   Specifies the port on which the web server is listening.

   Example: http://mymachine.myorg.org:81/siteminder

   The Policy Server User Interface login screen appears.
3. Click Administer SiteMinder.
4. Enter SiteMinder as the user name and enter the password you specified when configuring the policy store.

   The Policy Server User Interface opens.

5. If you have trouble logging into the Policy Server User Interface, reset the SiteMinder super user password by completing the following steps:

   a. Copy the smreg utility (smreg.exe) from the Policy Server installation kit to *siteminder_home*/bin.

   b. Execute the following command:

      `smreg -su super_user_password`

      super_user_password

      Specifies the password for the SiteMinder super user account.

      Note: Be sure that there is a space between -su and the super user password.

   c. Delete smreg.

      Deleting smreg prevents anyone from changing the super user password.

Configure Auto Startup

The following steps make sure the Policy Server restarts automatically when the Solaris system is re-booted.

To configure auto startup

1. Modify the S98M script by replacing every instance of the string “nete_ps_root” with an explicit path to the SiteMinder installation directory.

   Example: /export/Netegrity/siteminder

2. Change the directory to the siteminder installation directory.

3. Enter **su** and press ENTER**.**

   Note: Do not use the suse command.

   You are prompted for a password.

4. Enter the root password and press ENTER.

5. Enter **$ cp S98sm /etc/rc2.d** and press ENTER.

   s98sm automatically calls the stop-all and start-all executables, which stop and start the Policy Server’s service when the Solaris system is rebooted.

Note: If you are using a local LDAP directory server as a policy store, you must configure the LDAP directory to start automatically before starting the Policy Server automatically.

How to Prepare the Policy Server for the Web Agent Installation

Before installing the Web Agent, you must have installed the Policy Server and configured the policy and key stores. Before an administrator registers a trusted host at the Web Agent site, the following objects must be configured in the Policy Server User Interface:

- A SiteMinder Administrator that has the right to register trusted hosts.

  A trusted host is a client computer where one or more SiteMinder Web Agents are installed. The term trusted host refers to the physical system. There must be an administrator that you create in the Policy Server User Interface with the specific privilege to register trusted hosts. The default SiteMinder administrator, which you created during installation, already has these rights.

  To see if an administrator has these rights, check the administrator's properties using the Policy Server User Interface and make sure Register Trusted Hosts is checked.

  Note: For instructions on how to create a new administrator with rights to register trusted hosts, see the *Policy Design* guide.

- Host Configuration Object

  Defines the communication between the trusted host and the Policy Server after the initial connection between the two is made. Do not confuse this object with the trusted host's configuration file, SmHost.conf, which is installed at the trusted host after a successful host registration.

  The settings in the SmHost.conf file enable the host to connect to a Policy Server for the first connection only. Subsequent connections are governed by the Host Configuration Object.

  Note: For instructions on how to copy, create, and modify Host Configuration Objects in the Policy Server User Interface, see the *Policy Design* guide.

- Agent Configuration Object

  Holds parameter names and values for Web Agents and are the counterpart to Web Agent Configuration Files.

  - **For all Agents**

    The Agent Configuration Object must include a value for the DefaultAgentName. The DefaultAgentName identifies the Agent identity that the Web Agent uses when it detects an IP address on its Web server that does not have an Agent identity assigned to it. By default, the default Agent name is the name of the installed Web Agent.

- **For Domino Web Agents**

  The Agent Configuration Object must include values for the following parameters:

  DominoDefaultUser-If the user is not in the Domino Directory, and they have been authenticated by SiteMinder against another user directory, this is the name by which the Domino Web Agent identifies that user to the Domino server. This value is encrypted.

  DominoSuperUser-Ensures that all users successfully logged into SiteMinder will be logged into Domino as the Domino SuperUser.

- **For IIS Web Agents**

  The Agent Configuration Object must include values for the DefaultUserName and DefaultPassword parameters.

  DefaultUserName and DefaultPassword-Identify an existing Windows user account that has sufficient privileges to access resources on an IIS Web server protected by SiteMinder. When users want to access resources on an IIS Web server protected by SiteMinder, they may not have the necessary server access privileges. The Web Agent must use this Windows user account, which is previously assigned by an Windows administrator, to act as a proxy user account for users granted access by SiteMinder.

Note: For instructions on how to copy, create, and modify Agents and Agent Configuration Objects in the Policy Server User Interface, see the *Policy Design* guide. For Agent parameter descriptions, see the *Web Agent Guide*.

How to Uninstall the Policy Server and Documentation on UNIX Systems

Uninstalling the Policy Server and documentation on UNIX systems requires you to:

1. Shut down all instances of the Policy Server Management Console.
2. Make sure no Web Agents are configured to use the Policy Server you are uninstalling:
   a. Navigate to: *<Agent_install_directory>*/config

      Agent_install_directory

      Specifies the Web Agent Installation directory.

   b. Open the SmHost.conf file in a text editor.

c. Remove the Policy Server from the SmHost.conf file by deleting the entire line that begins "policyserver=" and contains the IP Address and port numbers for the Policy Server you are uninstalling.

d. Save SmHost.conf.

Note: Refer to the *Web Agent Guide* and the *Web Agent Installation Guide* for information on modifying the SmHost.conf file.

3. Use the smuser account to log into the UNIX environment, and run stop-all, located in the /siteminder directory, to stop the SiteMinder processes.
4. (Optional) Save the policy store data to an .smdif file using the smobjexport (see page 146) tool.
5. (Optional) Remove the policy store using one of the following tools:
   - To remove a policy store stored in an LDAP directory, use smldapsetup (see page 158).
   - To remove a policy store stored in an Oracle database, use sm_oracle_ps_delete.ps (see page 167).
6. Remove the Policy Server (see page 76).
7. Remove SiteMinder references (see page 77) from the obj.conf file.
8. Remove leftover items.
9. Uninstall the documentation (see page 79).

Remove the Policy Server

Removing the Policy Server involves deleting the SiteMinder installation directory and removing smprofile.ksh from .profile.

Note: Uninstalling the Policy Server will also remove the Policy Server Option Pack.

Important! Stop the Web Server and Policy Server before uninstalling the Policy Server from an HP-UX operating system. If you do not stop these servers, some Policy Server files remain after the installation.

To remove the Policy Server

1. In a console window, change to the *<siteminder_installation>*/install_config_info/nete-ps-uninstall directory

   siteminder_installation

   Specifies the directory where the Policy Server is installed.

2. Run the following command:

   ```
   ./uninstall
   ```

   If your JRE is not in the your PATH variable, run these two commands:

   - PATH=$PATH:*<JRE>*/bin

   JRE

   Specifies the location of your JRE.

   - export PATH

3. Press Enter to begin the uninstallation.

A status indicator shows that the Policy Server is being uninstalled. After finishing, the uninstaller indicates that the uninstallation went successfully.

To remove the siteminder directory

1. Change the directory to the one above the SiteMinder installation directory.

   Example: /export/smuser/netegrity, where the SiteMinder installation directory is /export/smuser/netegrity/siteminder.

2. Enter **$ rm -rf siteminder**, then press ENTER.

To remove smprofile.ksh

1. From your HOME directory, open .profile.
2. Locate and delete the line in .profile that contains smprofile.ksh.

   Example: ./export/smuser/siteminder/smprofile.ksh

3. Save .profile.

Remove SiteMinder References From IWS and ServletExec Files

After removing the SiteMinder files, remove SiteMinder references from the following:

Sun Java System—Remove SiteMinder References From obj.conf/magnus.conf

To remove SiteMinder references

1. Log in with an account that has privileges to access and modify the configuration of the web server.
2. At the Solaris command line, go to the *SunJavaSystem_home*/https-<hostname>/config folder and remove the following lines from the obj.conf file:

   NameTrans fn="assign-name" from="/servlet/*" name="*ServletExec_instance name*"

   NameTrans fn="assign-name" from="*.jsp*" name="*ServletExec_instance name*"

   NameTrans fn="pfx2dir" from="/siteminderm onitor" dir="/*siteminder_home*/monitor"

   NameTrans fn="pfx2dir" from="/sitemindercgi" dir="/*siteminder_home*/admin" name="cgi"

   NameTrans fn="pfx2dir" from="/siteminder" dir="/*siteminder_home*/admin"

   NameTrans fn="pfx2dir" from="/netegrity_docs" dir="/netegrity/netegrity_documents"

   <Object name="*ServletExec_instance name*">
   Service fn="ServletExecService" group="*ServletExec_instance name*"
   </Object>
3. Save and close the obj.conf file.
4. Remove the following lines from the magnus.conf, located in the same folder as the obj.conf.

   Init fn="init-cgi" SM_ADM_UDP_PORT="44444" SM_ADM_TCP_PORT="44444"

   Init fn="load-modules" shlib="/*Servlet_Exec_Install*/bin/ServletExec_Adapter.so" funcs="ServletExecInit,ServletExecService"

   Init fn="ServletExecInit"*ServletExec_instance name.instances="IP_Address:port*"
5. Save and close the magnus.conf file.
6. Restart the Web server.

ServletExec/AS—Remove Policy Server References from StartServletExec

To remove references from StartServletExec

1. Log in with an account that has privileges to access and modify the configuration of ServletExec.
2. At the Solaris command line, go to the /usr/NewAtlanta/ServletExecAS/*ServletExec_instance name* folder.

3. Remove the following lines from the StartServletExec script:

```
CLASSPATH=${NA_LIB}/servlet-api.jar:${NA_LIB}/jsp-
api.jar:${NA_LIB}/ServletExec60.jar:${NA_LIB}/ServletExecAdmin.jar:${NA_LIB}/
el-
api.jar:${NA_LIB}/jasper-el.jar:${JL}/tools.jar:${NA_LIB}/jstl.jar:${NA_LIB}/
appserv-
jstl.jar:${NA_LIB}/activation.jar:${NA_LIB}/mail.jar:${HOMEDIRPATH}/classes:/
siteminder_home/monitor/
smmonui.jar:/siteminder_home/lib/smconapi.jar:/siteminder_home/lib/smmonclien
tapi.jar
$SENAME $HOMEDIR $MIMEFILE $DOCROOTDIR -allow 127.0.0.1 -port $PORT $SEOPTS"
$SENAME $HOMEDIR $MIMEFILE $DOCROOTDIR -allow 127.0.0.1 -port $PORT $SEOPTS -addl
"/sitemindermonitor=/siteminder_home/monitor""
```

siteminder_home

Specifies the Policy Server installation path.

4. Save and close the StartServletExec script.
5. Restart ServletExec.

   The uninstallation is complete.

Remove Leftover Items

The com.zerog.registry.xml file is left on the system after you uninstall the Policy Server. Remove this file.

You can locate this file at one of the following:

- $HOME/.com.zerog.registry.xml
- /var/.com.zerog.registry.xml

Uninstall the Documentation

To uninstall the documentation

1. In a console window, change to the *<siteminder_installation>*/netegrity_documents/install_config_info/nete-sm-doc-uninstall directory where the *<siteminder_installation>* is /export/netegrity/siteminder

   Example:
   /export/netegrity/siteminder/netegrity_documents/install_config_info/nete-sm-doc-uninstall

2. Run the following command:

   ```
   ./uninstall
   ```

   If your JRE is not in the your PATH variable, run these two commands:

   ```
   PATH=$PATH:<JRE>/bin
   ```

   JRE

   Specifies the location of your JRE.

   ```
   export PATH
   ```

3. Press Enter to begin the uninstallation.

A status indicator shows that the SiteMinder documentation is being uninstalled. After finishing, the uninstaller indicates that the uninstallation went successfully.

Chapter 3: Configuring LDAP Directory Servers as a Policy or Key Store

This section contains the following topics:

LDAP Directory Servers as a Policy or Key Store

The SiteMinder policy store is the repository for all policy–related information. All Policy Servers in a SiteMinder installation must share the same policy store data, either directly or through replication. SiteMinder is installed with tools that let administrators move policy store data from one storage facility to another.

When you install the Policy Server, you can automatically configure one of the following directory servers as a policy store:

- Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet)
- Microsoft ADAM
- Microsoft AD LDS

You can configure the Policy Server to use another LDAP directory server, a SQL Server database, or an Oracle database as a policy store after you have completed the Policy Server installation. Also, after installation, you can use the Policy Server Management Console to point the Policy Server to another policy store.

Note: For a list of supported CA and third-party components, refer to the SiteMinder Platform Support Matrix on the Technical Support site.

To locate the support matrix from the Technical Support site

1. Click Support By Product.
2. Select CA SiteMinder from the Select a Product list.
3. Click CA SiteMinder Platform Support Matrices under Product Status.

You can download the latest JDK and JRE versions at the Sun Developer Network.

Important Considerations

To avoid possible policy store corruption, ensure that the server on which the policy store will reside is configured to store objects in UTF-8 form. For more information on configuring your server to store objects in UTF-8 form, see the documentation for that server.

Policy Store Schema Considerations

When manually configuring a policy store on Windows, you can choose one of two .smdif files:

- smpolicy.smdif
- smpolicy-secure.smdif

While both files contain the default policy store objects that you import into the policy store, there are a couple of factors to consider when choosing the file that best fits the requirements of your production environment:

- While smpolicy.smdif can be used with the Policy Server Configuration Wizard to automatically configure a policy store, smpolicy-secure.smdif can only be used to manually configure a policy store.
- The file smpolicy-secure.smdif provides additional security through enhanced default web agent configuration parameters.

The following table summarizes the differences between the default web agent configuration parameters in the two files:

Parameter Name	Value in smpolicy.smdif	Value in smpolicy-secure.smdif
BadCssChars	No value	<, >, ', ;,), (, &, +, %00
BadQueryChars	No value	<, >, ', ;,), (, &, +, %00
BadUrlChars	//, ./, /., /*, *., ~, \, %00-%1f, %7f-%ff, %25	smpolicy.smdif values plus: <, >, ', ;,), (, &, +
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	smpolicy.smdif values plus .jsp
ValidTargetDomain	Note: This parameter does not exist in smpolicy.smdif.	Provide a valid redirection domain as follows: validtargetdomain=".example.com"

Note: Before using smpolicy-secure.smdif, you must initialize the new web agent configuration parameter: validtargetdomain.

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.

Create a Policy Store in an LDAP Directory

The LDAP directory server can be the same directory server SiteMinder uses for user authentication and authorization, which simplifies the task of administering SiteMinder.

By default, the policy store is stored in an LDAP directory. The following lists the specific items that will be required in the process of creating an LDAP policy store or moving an existing policy store from a non-LDAP database or from an existing LDAP directory to another:

- **Secured Sockets Layer (SSL) Certificate Database** - If the targeted LDAP directory service communicates with a Policy Server over SSL, specifies the LDAP database where Certificates are located.
- **LDAP Server IP Address** - Specifies the targeted LDAP server IP address.
- **LDAP Port Number** - Specifies the port number on which the targeted LDAP service is listening on.
- **Distinguished Name (DN)** - Specifies the DN of an LDAP user with sufficient privileges for tasks such as i.e. the ability to creating, reading, modifying, and deleting objects in the LDAP tree underneath the policy store root object

  Example: cn=Directory Manager for Sun Java System Directory Server.
- **DN's Password** - Specifies the password of the Administrator DN.
- **Policy store Root DN** - Specifies the DN under which the policy store objects are defined.

  Example: o=test.com.

What To Do First

Depending on the directory for which you want to configure as a policy store, complete one of the following procedures:

- To configure CA Directory as a policy store, refer to Configure the Policy Server to Use CA Directory as a Policy Store (see page 84).
- To configure Sun Java System Directory Server Enterprise Edition as a policy store, refer to Configure a Policy Store in Sun Java System Directory Server Enterprise Edition (see page 91).
- To configure Microsoft Active Directory as a policy store, refer to Configure the Policy Server to Use Active Directory as a Policy Store (see page 96).
- To configure Microsoft ADAM or AD LDS as a policy store, refer to Configure the Policy Server to Use Microsoft ADAM/AD LDS as a Policy Store (see page 98).
- To configure Novell eDirectory as a policy store, refer to Configure the Policy Server to Use Novell eDirectory as a Policy Store (see page 99).
- To configure Oracle Internet Directory as a policy store, refer to Configure the Policy Server to Use OID as a Policy Store (see page 104).
- To configure IBM Directory Server as a policy store, refer to Configure the Policy Server to Use IBM Directory Server as Policy Store (see page 104).

How to Configure the Policy Server to Use CA Directory as a Policy Store

Configuring the Policy Server to use a CA Directory as a policy store requires you to:

1. Create a DSA for the policy store in a CA Directory.
2. Configure CA Directory as a policy store.
3. Verify the CA Directory cache configuration.

Create a DSA for the Policy Store in CA Directory

To create a DSA for the policy store in CA Directory, run the following command:

```
dxnewdsa DSA_Name port "o=DSA_name,c=country_code"
```

DSA_name

Specifies the name of the DSA.

port

Specifies the port on which the DSA is to listen.

o=*DSA_name*,c=*country_code*

Specifies the DSA prefix.

Example: "o=psdsa,c=US"

The dxnewdsa utility starts the new DSA.

Note: If the DSA does not automatically start, run the following:

```
dxserver start DSA_Name
```

Configure CA Directory as a Policy Store

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.

To configure CA Directory as a policy store

1. Copy the netegrity.dxc file into the CA Directory *DXHOME*\config\schema directory.

   Note: The netegrity.dxc file is installed with the Policy Server in *siteminder_home*\eTrust.

   siteminder_home

   Specifies the Policy Server installation path.

2. Create a SiteMinder schema file by copying the default.dxg schema file and renaming it.

   Note: The default.dxg schema file is located in *DXHOME*\config\schema\default.dxg.

   Example: Copy the default.dxg schema file and rename the copy to smdsa.dxg

3. Add the following lines to the bottom of the new SiteMinder schema file:

   ```
   # Netegrity Schema
   source "netegrity.dxc";
   ```

4. Edit the DXI file of the DSA (*DSA_name*.dxi) by changing the schema from default.dxg to the new SiteMinder schema file.

   DSA_name

   Represents the name of the DSA you created for the policy store.

   Note: The DXI file is located in *DXHOME*\config\servers.

5. Add the following lines to the end of the DXI file of the DSA:

   - **r12**

     ```
     # cache configuration
     set max-cache-size = 100;
     set cache-attrs = all-attributes;
     set cache-load-all = true;
     set ignore-name-bindings = true;
     ```

     Note: The max-cache-size entry is the total cache size in MB. Adjust this value based on the total memory available on the CA Directory server and overall size of the policy store.

   - **r12 SP1 or later**

     ```
     # cache configuration

     set ignore-name-bindings = true;
     ```

6. Copy the default limits DXC file of the DSA (default.dxc) to create a SiteMinder DXC file.

   Example: Copy the default DXC file and rename the copy smdsa.dxc.

   Note: The default DXC file is located in *DXHOME*\dxserver\config\limits.

7. Edit the settings in the new DXC file to match the following:

   ```
   # size limits
   set max-users = 1000;
   set credits = 5;
   set max-local-ops = 1000;
   set max-op-size = 4000;
   set multi-write-queue = 20000;
   ```

   Note: Editing the size limits settings prevents cache size errors from appearing in your CA Directory log files.

   Important! The multi–write–queue setting is for text–based configurations only. If the DSA is set up with DXmanager, omit this setting.

8. Save the DXC file.

9. Edit the DXI file of the DSA (*DSA_Name*.dxi) by changing the limits configuration from default.dxc to the new SiteMinder limits file.

   Example: change the limits configuration from default.dxc to smdsa.dxc.

   DSA_Name

   Represents the name of the DSA you created for the policy store.

   Note: The DXI file of the DSA is located in DXHOME\config\servers. If you created the DSA using DXmanager, the existing limits file is named dxmanager.dxc.

10. As the DSA user, restart the DSA using the following commands:

    `dxserver stop DSA_name`
    `dxserver start DSA_name`

    DSA_name

    Specifies the name of the DSA.

    The policy store schema is created.

11. Do the following to create a view into the DSA

    a. Launch the JXplorer GUI.

    b. Select the connect icon.

    Connection settings appear.

    c. Enter *host_name_or_IP_address* in the Host Name field.

    host_name_or_IP_address

    Specifies the host name or IP address of the CA Directory host system.

    d. Enter *port_number* in the Port number field.

    port_number

    Specifies the port on which the DSA is listening.

    e. Enter o=*DSA_name*,c=*country_code* in the Base DN field.

    Example: o=psdsa,c=US

    f. Select Anonymous from the Level list and click Connect.

    A view into DSA appears.

12. Create the base tree structure to hold the policy store data. Use the JXplorer GUI to create the following organizational units:

    a. Select the root element of your DSA.

    b. Under the root element, create an organizational unit named:

    Netegrity

    c. Under Netegrity, create an organizational unit (root element) named:

    SiteMinder

    d. Under SiteMinder, create an organizational unit (root element) named:

    PolicySvr4

    The base tree structure is created.

13. Use JXplorer to create an administrator that has the rights to create, delete, and modify objects in the DSA.

    Consider the following:

    - Be sure that the administrator is of object type inetOrgPerson.
    - Take note of administrator user name and password. You use this information when pointing the Policy Server to the policy store.

    Example: dn: cn=admin,o=yourcompany,c=in

14. From the Policy Server host system, open the Policy Server Management Console and click the Data tab.

    Database settings appear.

    Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.

15. Do the following to point the Policy Server at the CA Directory policy store:

    a. Select Policy Store from the Database list.

    b. Select LDAP from the Storage list.

    c. Configure the following settings in the LDAP Policy Store section:

        - LDAP IP Address
        - Root DN
        - Admin Username
        - Password
        - Confirm Password

    d. Click Apply.

        The policy store settings are saved.

    e. Click Test LDAP Connection to test the connection.

    If the connection is successful, SiteMinder returns a confirmation. If the connection is not successful, SiteMinder returns an error message. If you receive an error message, verify that the values you entered are correct and that the directory is running.

16. Do the following to set the SiteMinder superuser password:

    a. Copy the smreg utility from the top level of the Policy Server installation kit to *siteminder_home*\bin.

    siteminder_home

    Specifies the Policy Server installation path.

    b. Run the following command:

    ```
    smreg -su super_user_password
    ```

    super_user_password

    Specifies the password for the SiteMinder superuser account.

    Note: Be sure that there is a space between -su and the superuser password.

    c. Delete smreg.exe.

    Deleting smreg.exe prevents anyone from changing the superuser password without knowing the previous one.

17. Import the default policy store objects by running the following command:

    ```
    smobjimport -isiteminder_home\db\smdif\smpolicy.smdif
    -dsuper_user_administrator
    -wsuper_user_password -v
    ```

    siteminder_home

    Specifies the Policy Server installation path.

    Note: When manually configuring a policy store on Windows, you can import one of the following:

    - smpolicy.smdif
    - smpolicy–secure.smdif

    The file named smpolicy–secure provides additional security through enhanced default Web Agent configuration parameters.

    super_user_administrator

    Specifies the name of a SiteMinder account with superuser privileges.

    super_user_password

    Specifies the password for the SiteMinder superuser.

    Note: If an argument contains spaces, use double quotes around the entire argument.

Windows example: smobjimport -i“C:\Program Files\Netegrity\siteminder\db\smdif\smpolicy.smdif” -d"SM Admin" -wPassword -v

UNIX: smobjimport -i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

-v

Outputs error, warning, and comment messages in verbose format so you can monitor the status of the import.

The policy store is configured and you can now log in to the Policy Server User Interface.

More Information:

Policy Store Schema Considerations (see page 82)

Verify the CA Directory Cache Configuration

You can verify that the DXcache settings are enabled using the DXconsole.

Note: By default, the DxConsole is only accessible from localhost. For more information on using the set dsa command to let the DxConsole accept a connection from a remote system, refer to the *eTrust Directory Reference Guide*.

To verify that the cache is enabled

1. From a command prompt, enter the following to telnet to the DSA DXConsole port:

   `telnet DSA_Host DXconsole_Port`

   DSA_Host

   Specifies the host name or IP address of the system hosting the DSA.

   Note: If you are on the localhost, enter **localhost**. Entering a host name or IP Address results in a failed connection.

   DXConsole_Port

   Specifies the port on which the DXconsole is listening.

   Default: The DXconsole port is set to the value of the DSA port +1.

   Example: If the DSA is running on port 19389, the DXconsole port is 19390.

   The DSA Management Console appears.

2. Enter the following command:

   `get cache;`

   The DSA Management Console displays the current DSA DXcache settings and specifies if directory caching is enabled.

How to Configure a Policy Store in Sun Java System Directory Server Enterprise Edition

Configuring a policy store in Sun Java System Directory Server Enterprise Edition requires that you either:

- Automatically configure the policy store data using the Configuration Wizard through a GUI or console window (see page 66).
- Manually configure (see page 93) the policy store data.

smldapsetup and Sun Java System Directory Server Enterprise Edition

In a Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) directory server, smldapsetup creates the ou=Netegrity, *root* sub suffix and PolicySvr4 database.

root

The directory root you specified in the Root DN field on the Data tab of the Policy Server Management Console. This variable has to be either an existing root suffix or sub suffix.

Example: If your root suffix is dc=netegrity,dc=com then running smldapsetup produces the following in the directory server:

- A root suffix, dc=netegrity,dc=com, with the corresponding userRoot database.
- A sub suffix, ou=Netegrity,dc=netegrity,dc=com, with the corresponding PolicySvr4 database.

Example: If you want to place the policy store under ou=apps,dc=netegrity,dc=com, then ou=apps,dc=netegrity,dc=com has to be either a root or sub suffix of the root suffix dc=netegrity,dc=com.

If it is a sub suffix, then running smldapsetup produces the following:

- A root suffix, dc=netegrity,dc=com, with the corresponding userRoot database.
- A sub suffix, ou=apps,dc=netegrity,dc=com, with the corresponding Apps database.
- A sub suffix, ou=Netegrity,ou=apps,dc=netegrity,dc=com, with the corresponding PolicySvr4 database.

Note: For more information about root and sub suffixes, see the Sun Microsystems documentation.

Replicate the Policy Store on Sun Java System Directory Server Enterprise Edition

For Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet), SiteMinder r6.0 SP6 creates a UserRoot and a PolicySvr4 database. The PolicySvr4 database has suffix mappings pointing to it. To replicate this policy store, set up a replication agreement for the PolicySvr4 database directory.

Note: More information about a replication agreement, see the Sun Microsystems documentation.

After you create the replication agreement, replicate the SiteMinder indexes.

To replicate SiteMinder indexes

1. Generate the SiteMinder indexes:

   ```
   smldapsetup ldgen -x -findexes.ldif
   ```

   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.

2. Set up the indexes on a replica server:

   ```
   smldapsetup ldmod -x -findexes.ldif -hhost -preplicaport
   -dAdminDN -wAdminPW
   ```

   host

   Specifies the replica host.

   replicaport

   Specifies the replica port number.

   AdminDN

   Specifies the replica administrator DN.

   Example: cn=directory manager

   AdminPW

   Specifies the replica administrator password.

   The SiteMinder indexes are replicated.

More Information:

smldapsetup (see page 158)

Manually Configure Policy Store Data in an LDAP Directory

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.

To configure policy store data in an LDAP directory server manually

1. If applicable, use the vendor–specific software to create an LDAP directory server instance.
2. On the Policy Server host system, navigate to *siteminder_home*/bin.

   siteminder_home

   Specifies the Policy Server installation path.
3. Point the Policy Server at the LDAP directory server by running the following commands:

   ```
   smldapsetup status -hhost -pport -dAdminDN
   -wAdminPW -rrootDN -ssl1/0 -ccert
   smldapsetup reg -hhost -pport -dAdminDN
   -wAdminPW -rrootDN -ssl1/0 -ccert
   ```

   host

   Specifies the name or IP address of the LDAP directory server.

   port

   Specifies the port on which the LDAP directory server is listening.

   AdminDN

   Specifies the name of an LDAP user with privileges to create LDAP schema in the LDAP directory server. This user appears in the Admin Username field on the Data tab of the Policy Server Management Console after you run the smldapsetup utility.

   ADAM and AD LDS: Specifies the full domain name, including the guid value, of the directory server administrator.

   Example: CN=user1,CN=People,CN=Configuration,CN,{guid}

   AdminPW

   Specifies the password for the administrator DN.

rootDN

Specifies the DN location of the SiteMinder data in the LDAP directory server.

ADAM and AD LDS: Specifies the existing root DN location of the application partition in the directory server where the policy store schema must be created.

1/0

If you are connecting to the LDAP directory server over SSL, specify -ssl1 and -c*cert*

cert

Specifies the path of the directory where the SSL client certificate database file (cert7.db) exists.

Note: If client certificate database file exists in /app/siteminder/ssl, specify -capp/siteminder/ssl.

The smldapsetup utility tests the connection to the LDAP directory server. If the connection is successful, smldapsetup configures the Policy Server to use the LDAP directory server as the policy store.

4. Create the policy store schema by running:

```
smldapsetup ldgen -ffile_name
smldapsetup ldmod -ffile_name
```

file_name

Specifies the name of the LDIF file you are creating.

Example: smldapsetup ldmod -fpstoreschema.ldif

5. Change the SiteMinder super user password by completing the following steps:
   a. Copy the smreg utility (smreg.exe) from the Policy Server installation kit to *siteminder_home*\bin.
   b. Execute the following command:

```
smreg -su super_user_password
```

super_user_password

Specifies the password for the SiteMinder super user account.

Note: Be sure that there is a space between -su and the password.

c. Delete the smreg utility.

Deleting the smreg utility prevents someone from changing the super user password without knowing the previous one.

6. From *siteminder_home*/bin, import the basic SiteMinder objects required to set up a policy store by running:

```
smobjimport -isiteminder_home\db\smdif\smpolicy.smdif
-dSM_super_user_name -wsuper_user_password -v
```

siteminder_home

Specifies the Policy Server installation path.

smpolicy.smdif

Specifies the name of the file containing the default policy store objects that are imported into the policy store.

Note: When manually configuring a policy store on Windows, you can import one of the following:

- smpolicy.smdif
- smpolicy–secure.smdif

The file named smpolicy–secure provides additional security through enhanced default Web Agent configuration parameters.

SM_super_user_name

Specifies the name of the SiteMinder administrator with super user privileges.

super_user_password

Specifies the password for the SiteMinder super user.

Note: If an argument contains spaces, use double quotes around the entire argument.

Windows example: smobjimport -i“C:\Program Files\Netegrity\siteminder\db\smdif\smpolicy.smdif” -d"SM Admin" -wPassword -v

UNIX example: smobjimport -i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

-v

Outputs error, warning, and comment messages in verbose format so you can monitor the status of the import.

Be aware of the following:

- This step creates the default objects required by SiteMinder. The objects are automatically saved in their appropriate locations in the policy store.
- If you do not complete this step, required SiteMinder objects are not added to the policy store. As a result, you cannot use the Policy Server User Interface to configure policies.

7. Restart the Policy Server service by doing the following:
   a. Start the Policy Server Management Console.

      Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.

   b. Under the Status tab, stop the service by clicking the Stop button in the Policy Server group box.

      The stoplight icon changes from green to red.

   c. Click the Start button in the Policy Server group box to restart the service.

   d. Click OK to exit the Policy Server Management Console.

   (UNIX systems) Enter the commands stop–all followed by start–all.

   The policy store is configured and you can log into the Policy Server User Interface.

More Information:

smldapsetup (see page 158)
Import Policy Data Using smobjimport (see page 150)
Change the SiteMinder Super User Password Using smreg (see page 171)
Policy Store Schema Considerations (see page 82)

Configure the Policy Server to Use Active Directory as a Policy Store

Microsoft Active Directory is the native LDAP-compatible directory for Windows. Policy Servers installed on either Windows or UNIX systems can use Active Directory as a policy store. Moreover, the Policy Server and policy store can be installed on separate machines. For example, a Policy Server installed on a UNIX machine can use an Active Directory policy store on a Windows system.

Note: If Active Directory is to communicate with the Policy Server over SSL, ensure that the SSL client certificate contains the CN of the SubjectDN. The Policy Server crashes if the SSL client certificate does not contain this information.

You manually configure the Policy Server to use Active Directory as a policy store.

More Information:

Manually Configure Policy Store Data in an LDAP Directory (see page 93)

Support for Active Directory ObjectCategory Indexing Attribute

Unlike other LDAP-compatible directories, Active Directory does not index policy store objects using the objectClass attribute by default. Instead, the objects are indexed by the objectCategory attribute. To enhance searches, you can either configure objectClass as an indexable attribute (see the Active Directory documentation) or enable objectCategory support in the Policy Server.

Enable or Disable ObjectCategory Attribute Support

On Windows Systems:

To enable or disable ObjectCategory attribute support

1. Launch the Windows Registry Editor.
2. Locate the key HKLM\Software\Netegrity\SiteMinder\CurrentVersion\DS\LDAPProvider.
   a. To enable support, set the EnableObjectCategory value to 1.
   b. To disable support, set the EnableObjectCategory value to 0.

      Note: The default value is 0.

On UNIX systems:

To enable or disable ObjectCategory attribute support

1. In a text editor, open the SiteMinder sm.registry file, located in *<siteminder_installation>*/registry.
2. Locate the key

   HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider.
   a. To enable support, set the EnableObjectCategory value to 1.
   b. To disable support, set the EnableObjectCategory value to 0.

      Note: The default value is 0.

How to Configure the Policy Server to Use ADAM/AD LDS as a Policy Store

Configuring the Policy Server to use ADAM or AD LDS as a policy store requires you to:

1. Complete the prerequisites for configuring ADAM/AD LDS (see page 98) as a policy store.
2. Either:
   - Automatically configure the policy store data by running the Configuration Wizard using a GUI or console window (see page 66).
   - Manually configure (see page 93) the policy store data in the LDAP directory.

ADAM/AD LDS Policy Store Prerequisites

Be sure to meet the following prerequisites before configuring ADAM or AD LDS as a policy store:

- Create a policy store partition.
- (ADAM) Patch the ADAM Server

  Apply Microsoft patch Q840991 to the ADAM server. This patch lets you create users in the configuration partition. Only users with administrative rights in this partition can import the policy store schema. You can download the patch at www.microsoft.com or by contacting Microsoft Product Support.
- Allow users to be created in the application partition.

  Only an administrative user in the configuration partition can import the policy store schema. This user must have administrative rights over the configuration partition and all application partitions, including the policy store partition.

  Note: The following procedure assumes that you are familiar with configuration, application, and schema partitions.

To allow users to be created in the application partition

1. Open the ADSI Edit console.
2. Create a user in the configuration partition, reset the user's password, and give this user administrative rights over the configuration partition and all of the application partitions, including the policy store partition, by navigating to the following in the configuration partition:

   cn=directory service, cn=windows nt,

   cn=services,cn=configuration,cn={guid}
3. Locate the msDS-Other-Settings attribute.
4. Add the following new value to the msDS-Other-Settings attribute:

   ADAMAllowADAMSecurityPrincipalsInConfigPartition=1

5. In the configuration and policy store application partitions:
   a. Navigate to CN=Administrators, CN=Roles.
   b. Open the properties of CN=Administrators.
   c. Edit the member attribute.
   d. Do one of the following:
      - (ADAM 2000 and 2003) Click Add ADAM Account and paste the full DN of the user you created in the configuration partition.
      - (AD LDS) Click Add DN and paste the full DN of the user you created in the configuration partition.
   e. Go to the properties of the user you created and verify the value for the following object:

      msDS-UserAccountDisabled

      Be sure that the value is set to false.

Once you have met the prerequisites, do one of the following:

- Automatically configure the policy store data by running the Configuration Wizard using a GUI or console window.
- Manually configure the policy store data in the LDAP directory.

More Information:

Run the Configuration Wizard Using a GUI or Console Window (see page 66)
Manually Configure Policy Store Data in an LDAP Directory (see page 93)

Configure the Policy Server to Use Novell eDirectory as a Policy Store

In SiteMinder 6.x, you can configure the Policy Server to use a Novell eDirectory residing on a UNIX, Windows, or NetWare system as a policy store or user directory. To use eDirectory as a policy store or user directory, the Novell eDirectory schema must be extended to include SiteMinder 6.x objects.

Before you begin, be sure that you have the following installed:

- Novell eDirectory
- Novell Windows Login Client
- Novell ConsoleOne for Windows, UNIX, and Netware systems

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.

To configure Policy Store Data in a Novell eDirectory

1. From the Novell Client, navigate to the Novell directory where SiteMinder is installed:

   Windows: *siteminder_home*\novell

   siteminder_home

   Specifies the Policy Server installation path.

   UNIX: *siteminder_home*/novell

   siteminder_home

   Specifies the Policy Server installation path.

   This directory contains the Novell policy store schema file (Novell_Add_SM60.ldif).

2. Find the DN of the NCPServer for your Novell Server by entering the following in a command window on the Policy Server host system:

   `ldapsearch -h host -p port_number -b container -s sub -D admin_login -w password objectClass=ncpServer dn`

   Example: ldapsearch -h 192.168.1.47 -p 389 -b "o=nwqa47container" -s sub -D "cn=admin,o=nwqa47container" -w password objectclass=ncpServer dn

3. Manually edit the Novell_Add_SM60.ldif file by replacing every *<NCPServer>* variable with the value you found in the previous step.

   Example: if your sample DN value is cn=servername,o=servercontainer, you would replace every instance of *<NCPServer>* with cn=servername,o=servercontainer.

4. From the Policy Server host system, open the Policy Server Management Console and select the Data tab to bring it to the front.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.

5. Point the Policy Server at the directory by doing the following:

   a. Select Policy Store from the Database list.

   b. Select LDAP from the Storage list.

c. Configure the fields for the LDAP policy store under LDAP Policy Store. The following are sample values:

LDAP IP Address: 123.123.12.12:3500

Root DN: o=test

Note: Novell eDirectory has a 256 character limit in the DN. The longest root DN that the SiteMinder policy store can have is 256 characters.

Admin Username: cn=admin,ou=people,o=test

Password: <masked password>

Note: For more information about the LDAP settings, see the *Policy Server Management* guide for a complete description of the LDAP settings.

d. Click Apply.

e. Click Test LDAP Connection.

If the connection is successful, SiteMinder returns a confirmation. If the connection is not successful, SiteMinder returns an error message. If you receive an error message, verify that the values you entered are correct and that the directory is running.

Note: Once you have a successful connection, you can modify the Novell eDirectory policy store from the Policy Server host system.

6. Update the LDAP directory server with the Novell_Add_SM60.ldif file by doing the following:

a. Open up a command prompt window.

b. Navigate to the /siteminder/novell directory.

c. Enter the command:

```
smldapsetup ldmod -v -fNovell_Add_SM60.ldif
```

Important! For Novell, you do not need to run smldapsetup ldgen as you do for other LDAP directory servers such as Sun Java System Directory Server Enterprise Edition and Active Directory.

7. Change the SiteMinder super user password by completing the following steps:

a. Copy the smreg utility (smreg.exe) from the Policy Server installation kit to *siteminder_home*\bin.

b. Execute the following command:

```
smreg -su super_user_password
```

super_user_password

Specifies the password for the SiteMinder super user account.

Note: Be sure that there is a space between -su and the password.

c. Delete smreg.exe.

Deleting smreg.exe prevents someone from changing the super user password without knowing the previous one.

8. From *siteminder_home*/bin, import the basic SiteMinder objects required to set up a policy store by running:

```
smobjimport -isiteminder_home\db\smdif\smpolicy.smdif
-dSM_super_user_name -wsuper_user_password -v
```

siteminder_home

Specifies the Policy Server installation path.

smpolicy.smdif

Specifies the name of the file containing the default policy store objects that are imported into the policy store.

Note: When manually configuring a policy store on Windows, you can import one of the following:

- smpolicy.smdif
- smpolicy–secure.smdif

The file named smpolicy–secure provides additional security through enhanced default Web Agent configuration parameters.

SM_super_user_name

Specifies the name of the SiteMinder super user administrator.

super_user_password

Specifies the password for the SiteMinder super user.

Note: If an argument contains spaces, use double quotes around the entire argument.

Windows example: smobjimport -i“C:\Program Files\Netegrity\siteminder\db\smdif\smpolicy.smdif” -d"SM Admin" -wPassword -v

UNIX example: smobjimport -i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

-v

Outputs error, warning, and comment messages in verbose format so you can monitor the status of the import.

Be aware of the following:

- This step creates default objects required by SiteMinder. The objects are automatically saved in their appropriate locations in the policy store.
- If you do not complete this step, the required SiteMinder objects are not added to the policy store and you cannot use the Policy Server User Interface to configure policies.

9. Refresh the LDAP server to update Novell eDirectory by completing the following:
   a. From the Novell Client, open ConsoleOne.
   b. Double–click LDAP server from the directory tree.
   c. Click the Refresh NLDAP Server Now button.
10. Stop and start the Policy Server service by doing the following:
    a. Start the Policy Server Management Console.

       Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.

    b. Under the Status tab, click Stop.

       The stoplight icon changes from green to red.

    c. Click Start to restart the service.
    d. Click OK to exit the Policy Server Management Console.

    For UNIX systems, enter the commands stop–all followed by start–all.

    The policy store is configured and you can log into the Policy Server User Interface.

More Information:

smldapsetup (see page 158)
Import Policy Data Using smobjimport (see page 150)
Change the SiteMinder Super User Password Using smreg (see page 171)
Run the Policy Server Configuration Wizard (see page 25)

Limitations of Policy Store Objects in Novell eDirectory

Consider the following when working with Policy Store objects in a Novell eDirectory:

- When the policy store resides in Novell eDirectory, policy store objects cannot have names longer than 64 characters since eDirectory does not allow an attribute to be set to a value longer than 64. This affects Certificate Maps particularly since they routinely have long names by design.
- The Policy Server does not support LDAP referrals for policy stores residing in Novell eDirectory.

Configure the Policy Server to Use OID as a Policy Store

To configure the Policy Server to use OID as a Policy Store

1. Create a domain in OID using the ODM by right-clicking Entry Management and selecting Create.
2. In the Distinguished Name dialog:
   a. Click Add.
   b. Select the domain.
3. Enter:
   a. **dc=dcbok** for the Distinguished Name value.
   b. **dc** for the dc value.
4. Do the following:
   a. Create an organizational unit.
   b. Select the organizational unit.
   c. Enter ou=bok,dc=dcbok for Distinguished Name value and bok for the ou value.
5. Manually configure the Policy Store data.

The policy store is configured and you can now log into the Policy Server User Interface.

More Information:

Manually Configure Policy Store Data in an LDAP Directory (see page 93)

Configure the Policy Server to Use IBM Directory Server as Policy Store

To configure the Policy Server to use an IBM directory server as a Policy Store

1. Edit the V3.matchingrules file by adding the following line:

   ```
   MatchingRules=(2.5.13.15 NAME 'integerOrderingMatch' SYNTAX
   1.3.6.1.4.1.1466.115.121.1.27)
   ```

2. Using the IBM Directory Server Configuration Tool, create/load a server suffix if one does not exist.
3. Using the IBM Directory Server Web Administration Tool:
   a. Create a directory entry (for example, ou=Nete) for the Root DN of the policy server data.
   b. Create the root nodes (ou=PolicySvr4, ou=SiteMinder, ou=Netegrity) under ou=Nete.

4. Using the IBM Directory Server Configuration Tool, add the supplied schema file V3.siteminder60, which is located in *siteminder_home*\IBMDirectoryServer, to the Manage Schema Files section of the schema configuration.

   Note: If you are upgrading from SiteMinder 5.x, remove the old SiteMinder schema file before adding the new V3.siteminder60 file. For more information about upgrading, see the *SiteMinder Upgrade Guide*.

5. Restart the IBM Directory Server.

6. From the Policy Server host system, open the Policy Server Management Console and select the Data tab to bring it to the front.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.

7. Point the Policy Server at the directory by doing the following:

   a. In the Database drop-down menu, select Policy Store.

   b. In the Storage drop-down menu, select LDAP.

   c. Configure the fields for the LDAP policy store under LDAP Policy Store. The following are sample values for the fields:

      LDAP IP Address: 123.123.12.12:3500

      Root DN: o=test

      Admin Username: cn=admin,ou=people,o=test

      Password: <masked password>

      Note: For more information about the LDAP settings, see the *Policy Server Management* Guide.

   d. Click Apply.

   e. Click Test LDAP Connection.

   If the connection is successful, SiteMinder returns a confirmation. If the connection is not successful, SiteMinder returns an error message. If you receive an error message, verify that the values you entered are correct and that the directory is running.

8. Complete steps 5-7 in Manually Configure Policy Store Data in an LDAP Directory (see page 93).

   Note: IBM Directory Server referrals are incompatible with SiteMinder.

   The policy store is configured and you can now log into the Policy Server User Interface.

SiteMinder Key Store Overview

Web Agents use Agent keys to encrypt and decrypt SiteMinder cookies so the data they contain can be read. The Agent uses the key to encrypt cookies before sending them to a user's browser and to decrypt cookies received from other Web Agents. When a Web Agent starts up and makes a management call request, the Policy Server supplies the current set of keys. Each time that the Web Agent polls the Policy Server, the Agent again makes the management call. The Web Agent receives the updated keys. These keys are stored in either the policy store or in a separate store.

Configure a Key Store in an Existing Policy Store

To configure a key store in an existing policy store

1. Start the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. Select the Data tab to move it to the front.
3. In the Database drop-down list, select Key Store.
4. Select Use Policy Store database check box.
5. Click Apply to save the settings.
6. On the Data tab, click Test LDAP Connection to verify connectivity to the policy store in the LDAP directory.

Configure a Separate Key Store

To configure a separate key store

1. Start the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. Select the Data tab to move it to the front.
3. In the Database drop-down list, select Key Store.
4. In the Storage drop-down list, select LDAP.
5. (Optional) If applicable, deselect the Use Policy Store database check box.

6. In the LDAP Key Store group box, enter the following:
    a. In the LDAP IP Address field, enter the IP address (or host name) and port number of the LDAP directory, separated by a colon (:).

       Example, enter 123.123.12.12:321. If the port is not specified, SiteMinder uses port 389 as the default.

    b. In the Root DN field, enter the LDAP branch under which the SiteMinder policy store is located.

       Example: o=airius.com.

    c. In the Admin Username field, enter the DN of the LDAP directory administrator for the Policy Server being configured.

    d. Example, cn=Directory Manager.

    e. In the Password field, enter the LDAP directory administrator password.

    f. In the Confirm Password field, re-enter the LDAP directory administrator password.

    g. (Optional)If your system is communicating with the LDAP directory over SSL, select the Use SSL check box.

    h. Click Apply.
7. (Optional) If you are using SSL, enter the name of the certificate database in the Netscape Certificate Database File field on the Settings tab.
8. Click Apply to save the settings.
9. On the Data tab, click Test LDAP Connection to verify connectivity to the LDAP directory server.
10. Click OK to save the settings and close the Console.

Migrate an Existing Policy Store into an LDAP Directory

Using the smobjexport and smobjimport tools, you can migrate policy store data from other types of databases into LDAP policy stores or move policy stores in one LDAP directory to another.

The following list identifies the supported migrations:

- Oracle/SQL Server to LDAP
- LDAP to LDAP
- LDAP to Oracle/SQL Server

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: The following procedure assumes you have configured a new LDAP directory as a policy store to which you will import your existing policy store.

To migrate data from one policy store to another LDAP Directory

1. Export your existing policy store into an .smdif file by doing the following:
   a. Navigate to *siteminder_home*/bin
   b. Run:

      ```
      smobjexport -ofile_name -dsm_super_user_name
      -wsuper_user_password -v
      ```

      file_name

      Specifies the name of the output file to which you are exporting the data.

      sm_super_user_name

      Specifies the Super User name of the SiteMinder administrator.

      super_user_password

      Specifies the password for the SiteMinder Super User.

      Example: smobjexport -opstore.smdif -d"SM Admin" -wPassword -v

      Note: If the key store exists in the policy store, use the -k option too. By default, keys are not included in the export.

2. Run the import utility to import your old policy store into the new one:

   ```
   smobjimport -ifile_name -dsm_super_user_name -wsuper_user_password -v
   ```

   file_name

   Specifies the name of the file to which you exported the policy store.

sm_super_user_name

Specifies the Super User name of the SiteMinder administrator.

super_user_password

Specifies the password for the SiteMinder Super User.

Example: smobjimport -ipstore.smdif -d"SM Admin" -wPassword -v

Note: If the key store exists in the policy store, use the -k option.

3. Do the following:
   a. Verify that the Policy Server is pointing to the policy store.
   b. Make sure that the key store is configured correctly.

   The policy store is configured and you can now log into the Policy Server User Interface.

More Information:

smldapsetup (see page 158)
Export Policy Data Using smobjexport (see page 146)
Import Policy Data Using smobjimport (see page 150)
Point the Policy Server at the Policy Store (see page 109)
SiteMinder Key Store Overview (see page 106)

Point the Policy Server at the Policy Store

Once you have created a new policy store or key store, or migrated or moved an LDAP policy store, you must configure the Policy Server to use the LDAP directory. You can also use the Policy Server Management Console to configure additional Policy Servers to leverage an existing policy store in an LDAP directory.

When you use the Policy Server Management Console to change the Policy Store from ODBC to LDAP, the key store does not automatically switch to LDAP, even when it is set to use the same store as the policy store. You must manually change both to LDAP for the key store to be accepted by the Policy Server Management Console.

Note: Refer to the *Policy Server Management* guide for detailed information about using the Policy Server Management Console.

To point the Policy Server at the policy store

1. On the server where the Policy Server is installed, open the Policy Server Management Console and select the Data tab to bring it to the front.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. Do the following:

   a. In the Database drop-down menu, select Policy Store.

   b. In the Storage drop-down menu, select LDAP.

   c. In the LDAP Policy Store box, configure the fields for the LDAP policy store.

      The following lists sample values for the fields:

      LDAP IP Address: 123.123.12.12:3500

      Root DN: o=test

      Admin Username: cn=admin,ou=people,o=test

      Password: <masked password>

      Note: Refer to the *Policy Server Management* guide for a complete description of the LDAP settings.

   d. If the Policy Server is communicating with the LDAP directory over SSL, select the Use SSL check box.

   e. Click Apply after you have modified the LDAP fields.

   f. Click the Test LDAP Connection button to test the connection.

      If the connection is successful, SiteMinder returns a confirmation. If it is not successful, SiteMinder returns an error message. If you receive an error message, verify that the values you entered are correct and that the directory is running.

Chapter 4: Configuring SiteMinder Data Stores in a Relational Database

This section contains the following topics:

Relational Databases as a Policy or Key Store

The SiteMinder policy store is the repository for all policy–related information. All Policy Servers in a SiteMinder installation must share the same policy store data, either directly or through replication. SiteMinder is installed with tools that let administrators move policy store data from one storage facility to another.

When you install the Policy Server, you can automatically configure one of the following directory servers as a policy store:

- Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet)
- Microsoft ADAM
- Microsoft AD LDS

You can configure the Policy Server to use another LDAP directory server, a SQL Server database, or an Oracle database as a policy store after you have completed the Policy Server installation. Also, after installation, you can use the Policy Server Management Console to point the Policy Server to another policy store.

You can use a supported database to store SiteMinder policy store data. SiteMinder keys, audit logs, and session data can be stored in the policy store or in a separate database.

Storing keys in a separate database may be required to implement single sign–on functionality.

Note: For a list of supported CA and third-party components, refer to the SiteMinder Platform Support Matrix on the Technical Support site.

To locate the support matrix from the Technical Support site

1. Click Support By Product.
2. Select CA SiteMinder from the Select a Product list.
3. Click CA SiteMinder Platform Support Matrices under Product Status.

You can download the latest JDK and JRE versions at the Sun Developer Network.

Important Considerations

To avoid possible policy store corruption, ensure that the server on which the policy store will reside is configured to store objects in UTF-8 form. For more information on configuring your server to store objects in UTF-8 form, see the documentation for that server.

Policy Store Schema Considerations

When manually configuring a policy store on Windows, you can choose one of two .smdif files:

- smpolicy.smdif
- smpolicy-secure.smdif

While both files contain the default policy store objects that you import into the policy store, there are a couple of factors to consider when choosing the file that best fits the requirements of your production environment:

- While smpolicy.smdif can be used with the Policy Server Configuration Wizard to automatically configure a policy store, smpolicy-secure.smdif can only be used to manually configure a policy store.
- The file smpolicy-secure.smdif provides additional security through enhanced default web agent configuration parameters.

The following table summarizes the differences between the default web agent configuration parameters in the two files:

Parameter Name	Value in smpolicy.smdif	Value in smpolicy-secure.smdif
BadCssChars	No value	<, >, ', ;,), (, &, +, %00
BadQueryChars	No value	<, >, ', ;,), (, &, +, %00

BadUrlChars	//, ./, /., /*, *., ~, \, %00-%1f, %7f-%ff, %25	smpolicy.smdif values plus: <, >, ', ;,), (, &, +
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	smpolicy.smdif values plus .jsp
ValidTargetDomain	Note: This parameter does not exist in smpolicy.smdif.	Provide a valid redirection domain as follows: validtargetdomain=".example.com"

Note: Before using smpolicy-secure.smdif, you must initialize the new web agent configuration parameter: validtargetdomain.

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.

How to Configure a SiteMinder Data Store in a SQL Server Database

Configuring a SiteMinder data store in a SQL server database requires you to:

1. Create a SQL server database with a SiteMinder schema (see page 113).
2. Configure a SQL server data source (see page 116) for SiteMinder.
3. Configure policy, key, logging, or session data stores (see page 131).
4. Import default SiteMinder objects (see page 137) into the policy store.

Create a SQL Server Database With SiteMinder Schema

SiteMinder provides schema files to create the individual schema for storing policies, keys, logs, session data, and sample users. The following schema files are provided in the *siteminder_home*\db\SQL directory:

sm_mssql_ps.sql

Creates the SiteMinder policy store or key store (if you are storing keys in a different database) in a SQL Server database.

sm_mssql_logs.sql

Creates the schema for SiteMinder audit logs in a SQL Server database.

sm_mssql_ss.sql

Creates the schema for the SiteMinder session server in a SQL Server database.

smsampleusers_sqlserver.sql

(Optional) Creates the schema for SiteMinder sample users in a SQL Server database and populates the database with sample users. For example, the script includes a user named GeorgeC with a password of siteminder.

Create the database objects by running the appropriate SQL script using the SQL Server Enterprise Manager and SQL Server Query Analyzer.

Note: For more information about running SQL scripts, see your database documentation.

You can store SiteMinder data in a single SQL Server database or run each script separately to create a separate:

- policy store
- key store
- logging database
- session store
- sample users database

More Information:

Delete SiteMinder Data in ODBC Databases (see page 167)

Create the SQL Server Database for the Policy, Key, Logging, or Session Data Stores

If the Policy Server is installed on a UNIX system, copy the following SQL Server files from the *siteminder_home*/db/SQL directory to a temporary directory on a Windows system:

- sm_mssql_ps.sql
- sm_mssql_ss.sql
- sm_mssql_logs.sql
- smsampleusers_sqlserver.sql

In addition, be sure that the SQL Server database server is installed on the Windows system. If the Policy Server is on a Windows system, you can run these schema files from the *siteminder_home*/db/SQL directory.

Run the sm_mssql_ps.sql, sm_mssql_logs.sql, and sm_mssql_ss.sql scripts to create the following SiteMinder data in a single SQL Server database:

- policy store
- key store
- logging database
- session store

To run the scripts

1. Be sure that the SQL Server database instance that is to store the SiteMinder data is accessible from the Policy Server host system.
2. Using the SQL Server Enterprise Manager, create the database instance for the SiteMinder data store.

   Example: smdatastore.
3. Create the SiteMinder schema in a single SQL Server database:
   a. Open sm_mssql_ps.sql in a text editor and copy the contents of the entire file.
   b. Start the Query Analyzer and log in as the user who administers the Policy Server database information.
   c. In the Query Analyzer, select the database instance you created using the SQL Server Enterprise Manager from the database list at the top-middle of the screen.
   d. Paste the schema from sm_mssql_ps.sql into the query.
   e. Execute the query.
4. Import the sm_mssql_logs.sql or sm_mssql_ss.sql scripts into the same database instance by following the procedure you used for the sm_mssql_ps.sql script.

You can also store SiteMinder data in a separate SQL Server database by running each script separately to create a separate:

- policy store
- key store
- logging database
- session store
- sample users database

When running the sm_mssql_ps.sql or sm_mssql_logs.sql scripts to create SQL Server–based policy or logging stores, the following warnings are displayed:

Warning: The table 'smvariable5' has been created but its maximum row size (8746) exceeds the maximum number of bytes per row (8060). INSERT or UPDATE of a row in this table will fail if the resulting row length exceeds 8060 bytes.

Warning: The table 'smodbcquery4' has been created but its maximum row size (64635) exceeds the maximum number of bytes per row (8060). INSERT or UPDATE of a row in this table will fail if the resulting row length exceeds 8060 bytes.

Warning: The table 'smaccesslog4' has been created but its maximum row size (9668) exceeds the maximum number of bytes per row (8060). INSERT or UPDATE of a row in this table will fail if the resulting row length exceeds 8060 bytes.

These warnings are expected and do not cause any problems with the policy store or logging database.

More Information:

Create the SQL Server Database Schema For Logging (see page 183)

Configure a SQL Server Data Source for SiteMinder

If you are using ODBC, you need to configure a data source to let SiteMinder communicate with the SiteMinder data store.

More information:

SQL Server Authentication Mode Considerations (see page 116)

SQL Server Authentication Mode Considerations

SiteMinder data sources do not support Windows authentication. Configure the SiteMinder data source with the credentials of a user that is stored in the database.

Note: For more information about SQL Server authentication modes, see the vendor–specific documentation.

Create a SQL Server Data Source on Windows Systems

To create a SQL Server data source on Windows systems

1. Select Programs, Administrative Tools, Data Sources (ODBC) to access the ODBC Data Source Administrator**.**
2. Click the System DSN tab to move it to the front.

3. Click Add.

   The Create New Data Source dialog box appears.

4. Scroll down and select SiteMinder SQL Server Wire Protocol, and click Finish.

   The ODBC SQL Server Wire Protocol Driver Setup dialog box appears.

5. In this dialog, do the following:

   a. In the Data Source Name field, enter the Data Source name.

      Example: SM SQL Server Wire DS.

      Note: Take note of your data source name, as you will need it when configuring your ODBC database as a policy store.

   b. (Optional) In the Description field, enter a description of the data source.

   c. In the Server Name field, enter the name of an existing SQL server.

   d. In the Database name field, enter the name of an existing database instance.

   e. Click Test Connect to make sure to make sure the connection works.

   f. Click OK.

   The configuration is complete. Now, point the Policy Server to use the data source you just created by configuring your ODBC database as a policy store.

More Information:

Configure an ODBC Database as a Policy Store (see page 131)

Create a SQL Server Data Sources on UNIX Systems

The SiteMinder ODBC data sources are configured using a system_odbc.ini file, which you create by renaming sqlserverwire.ini, located in *policy_server_installation*/db, to system_odbc.ini. This system_odbc.ini file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the system_odbc.ini file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [SiteMinder Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the system_odbc.ini file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding a MS SQL Server Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the system_odbc.ini file if you create a new service name or want to use a different driver. You should have entries for the Oracle or SQL drivers under [SiteMinder Data Source].

Again, to configure a MS SQL Server data source, you must first create a system_odbc.ini file in the *policy_server_installation*/db directory. To do this, you need to rename sqlserverwire.ini, located in *policy_server_installation*/db, to system_odbc.ini.

Configure the SQL Server Wire Protocol Driver

No client is required for the wire protocol driver.

To configure the SQL Server wire protocol driver

1. Edit the $NETE_PS_ROOT/db/system_odbc.ini file by making the following entries under [ODBC Data Sources] and [SiteMinder Data Source].

```
[ODBC Data Sources]
Siteminder Data Source=DataDirect 6 SP3 SQL Server Wire Protocol
[SiteMinder Data Source]
Driver=nete_ps_root/odbc/lib/NSmsss24.so
Description=DataDirect 6 SP3 SQL Server Wire Protocol
Database=SiteMinder Data
Address=myhost, 1433
QuotedId=No
AnsiNPW=No
```

nete_ps_root

Specifies an explicit path, rather than one with an environment variable.

Example: export/smuser/siteminder.

SiteMinder Data

Specifies the SQL Server database instance name.

myhost

Specifies the IP address of the SQL Server database.

1433

Represents the default listening port for SQL Server.

Note: If no system_odbc.ini file exists, copy and rename sqlserverwire.ini to system_odbc.ini. The sqlserverwire.ini file is located in the $NETE_PS_ROOT/db directory.

You can edit these sections in the same manner to configure data sources for separate logs, keys, session, and sample users databases:

- [SiteMinder Logs Data Source]
- [SiteMinder Keys Data Source]
- [SiteMinder Session Data Source]
- [SmSampleUsers Data Source]

2. If you are using Microsoft SQL Server 2008 to function as any SiteMinder store, edit the [ODBC] section as follows:

```
TraceFile=nete_ps_root/db/odbctrace.out
TraceDll=nete_ps_root/odbc/lib/odbctrac.so
InstallDir=nete_ps_root/odbc
```

nete_ps_root

Specifies the explicit path to the Policy Server installation directory. This path cannot contain an environment variable.

3. Configure your policy, key, logging, or session data stores.

More Information:

Configure Policy, Key, Logging, or Session Stores (see page 131)

How to Configure a SiteMinder Data Store in an Oracle Database

Configuring a SiteMinder data store in an Oracle database requires you to:

1. Create an Oracle database with SiteMinder schema (see page 122).
2. Configure an Oracle data source (see page 124) for SiteMinder.
3. Configure policy, key, logging, or session data stores (see page 131).
4. Import default SiteMinder objects (see page 137) into the policy store.

Note: If you are configuring an Oracle 10g database, be sure that you have met the prerequisites for Oracle 10g databases.

Prerequisites for an Oracle 10g Database

After installing the Oracle 10g database, complete the following prerequisites:

- Create a table space for the policy store.
- Create a user with appropriate privileges to manage this table space in the database.

More Information:

Create an Oracle Database With SiteMinder Schema (see page 122)

Create an Oracle 10g Table Space for the Policy Store

Creating a table space for the policy store is a prerequisite for an Oracle 10g database only.

To create an Oracle 10g table space for the policy store

1. In the Oracle Enterprise Manager 10g Database Control, log in as the SYSDBA user with appropriate privileges to manage the Oracle database.
2. On the Oracle global database's configuration screen, select Administration, Tablespaces.
3. On the Tablespaces screen, click Create.
4. On the Create Tablespaces screen, enter a table space name, and click ADD.

   Example: NETE_TB
5. On the Create Tablespaces: Add Datafile screen:
   a. Enter a file name.

      Example: NETE_TB
   b. Specify the file size.

      Example: 100 MB
   c. Click Continue.

   Oracle creates the table space and displays it on the Tablespaces screen.

Complete the prerequisites by creating a user to manage the table space for the policy store.

More Information:

Create an Oracle 10g User to Manage the Policy Store's Table Space (see page 121)

Create an Oracle 10g User to Manage the Policy Store's Table Space

Creating a user to manage table space for the policy store is a prerequisite for an Oracle 10g database only.

To create a user to manage table space for the policy store

1. On the Oracle global database's configuration screen, select Administration, Users.
2. On the Create Tablespaces screen, click Create.
3. On the Create User screen, enter the:
   - Name for the user.

     Example: NETE
   - Password for the user.
   - Default Tablespace that you created.
   - Temporary tablespace.

     Example: TEMP
4. Click Roles.
5. Select Modify.
6. On the Modify Roles screen:
   a. Select CONNECT and RESOURCE as a roles for this user.
   b. Click Apply.
7. Start sqlplus in a command window, by entering:
   a. sqlplus
   b. the credentials for the policy store user created on the Create User screen.

   You have completed the prerequisites for an Oracle 10g database, and can now configure a SiteMinder data store for the database.

More Information:

Create an Oracle Database With SiteMinder Schema (see page 122)

Create an Oracle Database With SiteMinder Schema

SiteMinder provides schema files to create the individual schema for storing policies, keys, logs, session data, and sample users. The following schema files are provided in the *siteminder_home*\db\SQL directory:

sm_oracle_ps.sql

Creates the SiteMinder policy store or key store (if you are storing keys in a different database) in an Oracle database.

sm_oracle_logs.sql

Creates the schema for SiteMinder audit logs in an Oracle database.

sm_oracle_ss.sql

Creates the schema for the SiteMinder session server in an Oracle database.

smsampleusers_oracle.sql

(Optional) Creates the schema for SiteMinder sample users in an Oracle database and populates the database with sample users. For example, the script includes a user named GeorgeC with a password of siteminder.

Create the database objects by running the appropriate SQL script using SQL Plus for Oracle.

Note: For information about running SQL scripts, see your database documentation.

If you are creating a schema for an Oracle database, be sure to create an Oracle user, such as SMOWNER. Run the scripts as that user, which associates SiteMinder data files with the new user. We do not recommend that you create a schema with the SYS or SYSTEM users.

You can store SiteMinder data in a single Oracle database or run each script separately to create a separate:

- policy store
- key store
- logging database
- session store
- sample users database

More Information:

Delete SiteMinder Data in ODBC Databases (see page 167)

Create the Oracle Database For the Policy, Key, Logging, or Session Data Stores

If you are using an Oracle database, run the sm_oracle_ps.sql, sm_oracle_logs.sql, and sm_oracle_ss.sql scripts to create the following SiteMinder data in a single Oracle database:

- policy store
- key store
- logging database
- session store

To run the scripts

1. Be sure that the Oracle database instance that is to store the SiteMinder data is accessible from the Policy Server host system. Test the communication using tnsping or sqlplus.
2. Create the SiteMinder schema in the Oracle database:
   a. Log in to Oracle with sqlplus (or some other Oracle utility) as the user who administers the Policy Server database information.
   b. Import the scripts to create the SiteMinder schema:

      $NETE_PS_ROOT/db/sql/sm_oracle_ps.sql

      $NETE_PS_ROOT/db/sql/sm_oracle_logs.sql

      $NETE_PS_ROOT/db/sql/sm_oracle_ss.sql

      If you are using sqlplus, run the schema using an @ sign.

      Example: @$NETE_PS_ROOT/db/sql/sm_oracle_ps.sql

Note: Environment variables may not function in the SQL utility for Oracle. If you encounter problems when using the utility, specify an explicit path for $NETE_PS_ROOT, rather than one with an environment variable.

You can also store SiteMinder data in a separate Oracle database by running each script separately to create:

- a policy store
- a key store
- a logging database
- a session store
- a sample users database

For example, you can run the sm_oracle_logs.sql script to create a separate logging database.

More Information:

Configure an Oracle Data Source for SiteMinder (see page 124)

Configure an Oracle Data Source for SiteMinder

If you are using ODBC, you need to configure a data source for the Oracle wire protocol driver.

Create an Oracle Data Source on Windows Systems

To create an Oracle data source on a Windows system

1. Select Programs, Administrative Tools, Data Sources (ODBC) to access the ODBC Data Source Administrator.
2. Click the System DSN tab and click Add.

   The Create New Data Source dialog appears.
3. Scroll down and select SiteMinder Oracle Wire Protocol and click Finish.

   The ODBC Oracle Wire Protocol Driver Setup dialog appears.
4. Under the General tab, do the following:
   a. In the Data Source Name field, enter any name you want.

      Example: SM Oracle Wire DS

      Note: Take note of the data source name. The data source name is required when configuring your ODBC database as a policy store.

   b. (Optional) In the Description field, enter a description of the Oracle wire protocol data source.

   c. In the Host field, enter the name of the Oracle database host system.

   d. In the Port Number field, enter the port number on which the Oracle database is listening.

   e. In the SID field, enter the service name of the Oracle instance to which you want to connect. You specified this name in the tnsnames.ora file. The SID is the system identifier for the database instance.

The tnsnames.ora file contains service names and details that Oracle uses to identify and connect to Oracle instances. For example, if the tnsnames.ora file contains the following entry for an Oracle instance, enter **instance1** in the SID field.

```
instance1 =
 (DESCRIPTION =
 (ADDRESS = (PROTOCOL = TCP)(Host = myhost)(Port =1521))
 (CONNECT_DATA = (SID = SIDofinstance1))
 )
```

f. Test the connection with the database by clicking Test Connect.

5. Click OK to save the selections and exit the ODBC Oracle Wire Protocol Driver Setup.

   The configuration is complete. Configure SiteMinder to use the data source you created.

More Information:

Configure an ODBC Database as a Policy Store (see page 131)

Create an Oracle RAC Data Source on Windows Systems

Oracle RAC 9.2.0.6 and 10.1.0.4 instances can be configured with the Policy Server as a single data source name similar to that of a single instance Oracle database. However, the data source name for Oracle RAC is different than a regular ODBC data source.

In an Oracle RAC system, in addition to the SID or ServiceName for each Oracle instance, there is also a ServiceName for the entire Oracle RAC system. When configuring a data source, configure the data source name to use this ServiceName when connecting to an Oracle RAC.

To configure an Oracle RAC data source

1. Select Programs, Administrative Tools, Data Sources (ODBC) to access the ODBC Data Source Administrator**.**
2. Click the System DSN tab, and then click Add.

   The Create New Data Source dialog box appears.
3. Scroll down and select SiteMinder Oracle Wire Protocol and click Finish.

   The ODBC Oracle Wire Protocol Driver Setup dialog appears.
4. Under the General tab, do the following:
   a. In the Data Source Name field, enter any name for the data source.

      Note: Take note of the data source name, as you will need it when configuring your ODBC database as a policy store.

   b. In the Host field, enter the IP address of the first node in the Oracle RAC system. For Oracle RAC 10g, specify the virtual IP address.

c. In the Service Name field, enter the service name for the entire Oracle RAC system. For example, in the following tnsnames.ora file, the value SMDB is the service name for the entire Oracle RAC system (consisting of 3 nodes).

```
SMDB =
    (DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = nete_servername1)(PORT = 1521))
(ADDRESS = (PROTOCOL = TCP)(HOST = nete_servername2)(PORT = 1521))
(ADDRESS = (PROTOCOL = TCP)(HOST = nete_servername3)(PORT = 1521))
(LOAD_BALANCE = yes)
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = SMDB)
)
```

5. Under the Failover Tab, do the following:

   a. In the Alternate Servers field, specify the host name (virtual IP address), port number, and service name for all the remaining Oracle RAC nodes in the environment. The ServiceName is service name for the entire Oracle RAC system.

   b. Specify the AlternateServers to provide connection failover to the other Oracle nodes if the primary server is not accepting connections. The entry should have the following format:

      (HostName=nete_servername2:PortNumber=1521:ServiceName=nete_service name[, . . .])

   c. Check the LoadBalancing option. This turns on the client load balancing to help distribute new connections to keep RAC nodes from being overwhelmed with connection requests. When client load balancing is enabled, the order in which primary and alternate database servers are accessed is random.

6. Click OK to save the selections and exit the ODBC Oracle Wire Protocol Driver Setup.

The configuration is complete. Now, configure SiteMinder to use the data source you created.

More Information:

Configure an ODBC Database as a Policy Store (see page 131)

Create an Oracle Data Source on UNIX Systems

The SiteMinder ODBC data sources are configured using a system_odbc.ini file, which you create by renaming oraclewire.ini, located in *policy_server_installation*/db, to system_odbc.ini. This system_odbc.ini file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the system_odbc.ini file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [SiteMinder Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the system_odbc.ini file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding an Oracle Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the system_odbc.ini file if you create a new service name or want to use a different driver. You should have entries for the SQL Server or Oracle drivers under [SiteMinder Data Source].

Again, to configure an Oracle data source, you must first create a system_odbc.ini file in the *policy_server_installation*/db directory. To do this, you need to rename oraclewire.ini, located in *policy_server_installation*/db, to system_odbc.ini.

Configure the Oracle Wire Protocol Driver

To configure the Oracle wire protocol driver

1. Edit the $NETE_PS_ROOT/db/system_odbc.ini file by replacing the nete_serverid value for SID with the value that is appropriate for your Oracle instance. If no system_odbc.ini file exists, copy and rename oraclewire.ini to system_odbc.ini. The SID is the system identifier for the database instance. In the following tnsnames.ora file, the value instance1 is the SID.

   ```
   instance1 =
    (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(Host = myhost)(Port =1521))
    (CONNECT_DATA = (SID = instance1))
    )
   ```

The modified text for the policy store data source should appear as follows:

```
[SiteMinder Data Source]
Driver=nete_ps_root/odbc/lib/NSora24.so
Description=DataDirect 6 SP3 Oracle Wire Protocol
LogonID=uid
Password=pwd
HostName=nete_servername
PortNumber=1521
SID=nete_serverid
CatalogOptions=0
ProcedureRetResults=0
EnableDescribeParam=0
EnableStaticCursorsForLongData=0
ApplicationUsingThreads=1
```

nete_ps_root

Specifies an explicit path, rather than one with an environment variable.

uid

Specifies the user name of the database account that has full access rights to the database.

pwd

Specifies the password for the user.

nete_servername

Specifies the name of the Oracle database host system.

nete_serverid

Specifies the SID.

Note: Only enter ten characters or less for the SID value due to a limitation of the Oracle wire protocol driver.

You can edit these sections in the same manner to configure data sources for separate logs, keys, session, and sample users databases:

- [SiteMinder Logs Data Source]
- [SiteMinder Keys Data Source]
- [SiteMinder Session Data Source]
- [SmSampleUsers Data Source]

2. Configure your policy, key, logging, or session data stores.

More Information:

Configure Policy, Key, Logging, or Session Stores (see page 131)

Create an Oracle RAC Data Source on UNIX Systems

Oracle RAC 9.2.0.6 and 10.1.0.4 instances can be configured with the Policy Server as a single data source name similar to that of a single instance Oracle database. However, the data source name for Oracle RAC is different from a regular ODBC data source. In an Oracle RAC system, in addition to the SID or ServiceName for each Oracle instance, there is also a ServiceName for the entire Oracle RAC system. When configuring a data source, configure the data source name to use this ServiceName when connecting to an Oracle RAC.

To configure an Oracle RAC data source

1. Go to *NETE_PS_ROOT*/db

   NETE_PS_ROOT

   Specifies the SiteMinder installation directory.

2. Create a copy of the existing system_odbc.ini file.
3. Create a new system_odbc.ini file by copying the oraclewire.ini file to system_odbc.ini.
4. Modify the system_odbc.ini file as follows:
   a. Insert the ServiceName field.
   b. Insert the AlternateServers field.
   c. Insert the LoadBalancing field.
   d. Remove or comment the SID field.
5. In the ServiceName field, enter the ServiceName for the entire Oracle RAC system. For example, in the following tnsnames.ora file, the value SMDB is the ServiceName for the entire Oracle RAC system (consisting of 3 nodes).

```
SMDB =
  (DESCRIPTION =
  (ADDRESS = (PROTOCOL = TCP)(HOST = nete_servername1)(PORT = 1521))
  (ADDRESS = (PROTOCOL = TCP)(HOST = nete_servername2)(PORT = 1521))
  (ADDRESS = (PROTOCOL = TCP)(HOST = nete_servername3)(PORT = 1521))
  (LOAD_BALANCE = yes)
  (CONNECT_DATA =
     (SERVER = DEDICATED)
     (SERVICE_NAME = SMDB)
  )
 )
```

The modified text for a data source should appear as follows:

```
[Data Source Name]
Driver=nete_ps_root/odbc/lib/NSora24.so
Description=DataDirect 6 SP3 Oracle Wire Protocol
LogonID=uid
Password=pwd
HostName=nete_servername1
PortNumber=1521
ServiceName=nete_servicename
CatalogOptions=0
ProcedureRetResults=0
EnableDescribeParam=0
EnableStaticCursorsForLongData=0
ApplicationUsingThreads=1
AlternateServers=(HostName=nete_servername2:PortNumber=1521:ServiceName=nete_
servicename[, . . . ])
LoadBalancing=1
```

nete_ps_root

Specifies an explicit path to the directory where SiteMinder is installed.

uid

Specifies is the username of the database account

pwd

Specifies the password for the user.

nete_servername1

Specifies the IP address of the first Oracle RAC node. For Oracle RAC 10g, it specifies the virtual IP address.

nete_servicename

Specifies the ServiceName for the entire Oracle RAC system.

AlternateServers

Specifies the Hostname (virtual IP address), PortNumber, and ServiceName for the remaining Oracle RAC nodes in the environment.

ServiceName

Specifies service name for the entire Oracle RAC system. Specifying the AlternateServers provides connection failover to the other Oracle nodes, if the primary server is not accepting connections.

LoadBalancing=1

Turns on client load balancing, which helps distribute new connections to keep RAC nodes from being overwhelmed with connection requests.

When enabled, the order in which primary and alternate database servers are accessed is random.

The configuration is complete. Configure SiteMinder to use the data source you created.

More Information:

Configure an ODBC Database as a Policy Store (see page 131)

Configure Policy, Key, Logging, or Session Stores

You can use an Oracle or SQL Server database to store SiteMinder policy store data. SiteMinder keys, audit logs, and session data can be stored in the policy store or in a separate database.

Configure an ODBC Database as a Policy Store

To configure an ODBC database as a policy store

1. Start the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. Select the Data tab to move it to the front.
3. In the Storage drop-down list, select ODBC.
4. In the Database drop-down list, select Policy Store.
5. In the Data Source Information field, enter the name of the data source.
   - For Windows systems, this name must correspond to the name you entered in the Data Source field of the ODBC Oracle Wire Protocol Driver Setup dialog box, when you created your Oracle data source or to the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog box when you created your SQL data source.

- For UNIX systems, the value you enter must match the first line of the data source entry in the system_odbc.ini file when you created your SQL server data sources or your Oracle data sources. This file is located in $NETE_PS_ROOT/db. For example, the first line of the default entry in the system_odbc.ini file is [SiteMinder Data Source], so you would enter SiteMinder Data Source in the Data Source Name field. If you modified the entry in the system_odbc.ini file, you would enter that value in the Data Source Information field.

Note: When entering the data source name, do not include the brackets.

6. In the User Name and Password fields, enter the username and password of the database account that has full access rights to the Oracle or SQL Server database instance.
7. In the Confirm Password field, re-enter the password.
8. Specify the maximum number of database connections allocated to SiteMinder. For best performance, retain the default of 25 connections.
9. (Optional) Click Test Connection to make sure the connection works.
10. Click Apply to save the settings.
11. Click the Status tab.
12. Stop and restart the Policy Server.

More Information:

Create an Oracle Data Source on Windows Systems (see page 124)
Create an Oracle Data Source on UNIX Systems (see page 127)
Create a SQL Server Data Source on Windows Systems (see page 116)
Create a SQL Server Data Sources on UNIX Systems (see page 117)

Store Keys, Logging, and Session Data in the Policy Store

You can store keys, logging, and session information in the policy store to simplify administration tasks.

Note: The following procedures assume you are working with an Oracle or SQL Server database for which you have imported sm_oracle_ps.sql or sm_mssql_ps.sql, respectively. Each of these files hold key store and policy data. If you have not, create an Oracle or SQL Server database for policy, key, logging, and session data stores.

More Information:

Create the SQL Server Database for the Policy, Key, Logging, or Session Data Stores (see page 114)
Create the Oracle Database For the Policy, Key, Logging, or Session Data Stores (see page 123)

Store Key, Logging, and Session Information in an Oracle Database

To store keys, logging, and session information in an Oracle database

1. Be sure that the Oracle database instance that is to store the SiteMinder data is accessible from the Policy Server host system. Test the communication using tnsping or sqlplus.
2. Create the SiteMinder schema in the Oracle database:
   a. Log into Oracle with sqlplus or another Oracle utility as the user who administers the Policy Server database information.
   b. Import one or more of the following scripts to create the respective SiteMinder schema:
      - $NETE_PS_ROOT/db/sql/sm_oracle_ps.sql
        Creates the SiteMinder policy store; or if you are storing keys in different database, creates a key store.
      - $NETE_PS_ROOT/db/sql/sm_oracle_logs.sql
        Creates the schema for SiteMinder audit logs in an Oracle database.
      - $NETE_PS_ROOT/db/sql/sm_oracle_ss.sql
        Creates the schema for the SiteMinder session server in an Oracle database.

      If you are using sqlplus, run the schema using an @ sign.

      Example: @$NETE_PS_ROOT/db/sql/sm_oracle_ps.sql

      Note: Environment variables may not function in the SQL utility for Oracle. If you encounter problems when using the utility, specify an explicit path for $NETE_PS_ROOT, rather than one with an environment variable.
3. In the Policy Server Management Console, click the Data tab to move it to the front.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.
4. Select Key Store from the Database list.
5. Select the Use the policy store database check box and click Apply.
6. Select Audit Logs from the Database list.
7. Select the Use the policy store database check box and click Apply.
8. Click Test Connection to verify connectivity to the database server.
   - If it returns a success message, click OK to save the settings and exit.
   - If it returns a failure message, go back and recheck your data source settings.

Store Key, Logging, and Session Information in a SQL Server Database

To store keys, logging, and session information in a SQL Server database

1. Be sure that the SQL Server database instance that is to store the SiteMinder data is accessible from the Policy Server host system.
2. Using the SQL Server Enterprise Manager, create the database instance for the information type you want.
3. Create the SiteMinder schema in the database:
   a. Open one schema file in a text editor and copy the contents of the entire file. The schema files include:
      - sm_mssql_ps.sql
        Creates the SiteMinder policy store; or, if you are storing keys in a different database, creates a key store.
      - sm_mssql_logs.sql
        Creates the schema for SiteMinder audit logs.
      - sm_mssql_ss.sql
        Creates the schema for the SiteMinder session server.
   b. Start the Query Analyzer and log in as the user who administers the Policy Server database information.
   c. In the Query Analyzer, select the desired database instance from the database list at the top-middle of the screen.
   d. Paste the copied schema into the query.
   e. Execute the query.

      Note: Running sm_mssql_logs.sql causes warnings to display. These warnings are expected and do not cause problems with the policy store or logging database.
4. Repeat steps 2-3 for the remaining files.
5. In the Policy Server Management Console, click the Data tab to move it to the front.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.
6. Select Key Store from the Database list.
7. Select the Use the policy store database check box and click Apply.
8. Select Audit Logs from the Database list.

9. Select the Use the policy store database check box and click Apply.
10. Click Test Connection to verify connectivity to the database server.
    - If it returns a success message, click OK to save the settings and exit.
    - If it returns a failure message, go back a recheck your data source settings.

Configure a Database to Store Keys and Audit Logs

SiteMinder keys and audit logs can be stored in separate databases. Before configuring a separate database to store keys or audit logs, be sure that you have configured a separate database to function as the policy store.

Note: Storing keys in a separate database may be required to implement single sign–on functionality. For more information about key management, see the *Policy Server Management Guide*.

If you are working with a SQL Server database or an Oracle database, the following procedure assumes that you have imported sm_mssql_logs.sql or $NETE_PS_ROOT/db/sql/sm_oracle_logs.sql, respectively.

To configure SiteMinder to store keys or audit logs in different databases:

1. In the Policy Server Management Console, click the Data tab.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. Select Key Store or Audit Logs from the Database list.
3. Clear the Use the policy store database check box and click Apply.

   The fields in the Data Source Information section become active.
4. In the Data Source Information field, enter the name of the data source.
   - (Windows) The name you enter must correspond to the name you entered in the Data Source field of the ODBC Driver Setup dialog.
   - (UNIX) The value you enter must match the first line of the data source entry in the system_odbc.ini file. This file is located in $NETE_PS_ROOT/db. **Example:** The first line of the default entry in the system_odbc.ini file is [SiteMinder Data Source], so you would enter SiteMinder Data Source in the Data Source Name field. If you modify the entry in the system_odbc.ini file, you would enter that value in the Data Source Information field.

     Note: When entering the data source name, do not include the brackets.
5. In the User Name and Password fields, enter the user name and password of the database account that has full access rights to the database.

6. In the Confirm Password field, re–enter the password.
7. Specify the maximum number of database connections allocated to SiteMinder. For best performance, retain the default of five connections.
8. Click Test Connection to verify connectivity to the database server.
9. Click Apply to save the settings.

Configure a Database as a Session Store

Before configuring a relational database to store session data, make sure you have:

Created a separate session server database using sm_oracle_ss.sql or sm_mssql_ss.sql.

- Create a SQL Server Database With SiteMinder Schema (see page 113)
- Create an Oracle Database With SiteMinder Schema (see page 122)

Configured a SiteMinder Session Server Data Source for your respective database.

- Configure a SQL Server Data Source for SiteMinder (see page 116)
- Configure an Oracle Data Source for SiteMinder (see page 124)

To point SiteMinder to store session data in a relational database:

1. In the Policy Server Management Console, click the Data tab to move it to the front.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. In the Database drop-down list, select Session Server.
3. In the Storage drop-down list, select ODBC.
4. Select the Session Server enabled check box and click Apply.
5. In the Data Source Information field, enter the name of the data source.

   Example: SiteMinder Session Data Source.

   Note: This name must correspond to the name you entered in the Data Source field of the ODBC Driver Setup dialog box.
6. In the User Name and Password fields, enter the username and password of the database account that has full access rights to the database.
7. In the Confirm Password field, re-enter the password.
8. Specify the maximum number of database connections allocated to SiteMinder. For best performance, retain the default of 5 connections.

9. Click Test Connection to verify connectivity to the database server.
10. Click Apply to save the settings.

Import Default SiteMinder Objects into the Policy Store

When manually configuring a policy store, you are required to import the default SiteMinder objects. If you do not, you cannot use the Policy Server User Interface to configure policies.

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.

To import the default policy store objects

1. From the Policy Server host system, navigate to *siteminder_home*/bin
2. Change the SiteMinder super user password by completing the following steps:
   a. Copy the smreg utility (smreg.exe) from the Policy Server installation kit to *siteminder_home*\bin.
   b. Execute the following command:

      ```
      smreg -su super_user_password
      ```

      super_user_password

      Specifies the password for the SiteMinder super user account. The password is not case–sensitive, except in cases where the password is stored in an Oracle policy store. The default administrator name is SiteMinder. Once the Oracle policy store is configured, administrator user names for the Policy Server User Interface are case–sensitive.

      Note: Be sure that there is a space between -su and the password.

   c. Delete smreg.exe.

      Deleting smreg.exe prevents someone from changing the super user password without knowing the previous one.
3. From *siteminder_home*\bin, import the basic SiteMinder objects required to set up a policy store by running:

   ```
   smobjimport -isiteminder_home\db\smdif\smpolicy.smdif
   -dSM_super_user_name -wsuper_user_password -v
   ```

   siteminder_home

   Specifies the Policy Server installation path.

smpolicy.smdif

Specifies the name of the file containing the default policy store objects that are imported into the policy store.

Note: When manually configuring a policy store on Windows, you can import one of the following:

- smpolicy.smdif
- smpolicy–secure.smdif

The file named smpolicy–secure provides additional security through enhanced default Web Agent configuration parameters.

SM_super_user_name

Specifies the name of the SiteMinder super user.

super_user_password

Specifies the password for the SiteMinder super user.

If an argument contains spaces, use double quotes around the entire argument.

Windows example: smobjimport -i
“C:\Program Files\Netegrity\siteminder\db\smdif\smpolicy.smdif”
-d"SM Admin" -wPassword -v

UNIX example: smobjimport -i$NETE_PS_ROOT/db/smdif/smpolicy.smdif
-d"SM Admin" -wPassword -v

-v

Outputs error, warning, and comment messages in verbose format so you can monitor the status of the import.

Be aware of the following:

- This step creates default objects required by SiteMinder. The objects are automatically saved in their appropriate locations in the policy store.
- If you do not complete this step, the required SiteMinder objects are not added to the policy store and you cannot use the Policy Server User Interface to configure policies.

4. Restart the Policy Server service by doing the following:
   a. Start the Policy Server Management Console.

      Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.

   b. Under the Status tab, click Stop.

      The stoplight icon changes from green to red.

c. Click Start to restart the service.

d. Click OK to exit the Policy Server Management Console.

For UNIX systems, enter the commands stop–all followed by start–all.

The policy store is configured and you can now log into the Policy Server User Interface.

More Information:

Change the SiteMinder Super User Password Using smreg (see page 171)
Import Policy Data Using smobjimport (see page 150)
Policy Store Schema Considerations (see page 82)

Migrate an Existing Policy Store into a Relational Database

Using the smobjexport and smobjimport tools, you can migrate policy store data from other types of LDAP into database policy stores or move policy stores in one database to another.

The following list identifies the supported migrations:

- Oracle/SQL Servers to LDAP
- Oracle/SQL Server to Oracle/SQL Severs
- LDAP to Oracle/SQL Server

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.

The following procedure assumes you have created a SiteMinder data store in either an Oracle database or a SQL Server database to which you will export your data. Details exist in How to Configure a SiteMinder Data Store in a SQL Server Database (see page 113) and How to Configure a SiteMinder Data Store in an Oracle Database (see page 119).

To migrate data from one policy store to a Database

1. Export your existing policy store into an .smdif file by doing the following:
   a. Navigate to siteminder_home\bin
   b. Run:

      ```
      smobjexport -ofile_name -dsm_super_user_name
      -wsuper_user_password -v
      ```

      file_name

      Specifies the name of the output file to which you are exporting the data.

      sm_super_user_name

      Specifies the Super User name of the SiteMinder administrator.

      super_user_password

      Specifies the password for the SiteMinder Super User.

      Example: smobjexport -opstore.smdif -d"SM Admin" -wPassword -v

      Note: If the key store exists in the policy store, use the -k option. By default, keys are not included in the export.

2. Run the import utility to import your old policy store into the new one:

   ```
   smobjimport -ifile_name -dsm_super_user_name -wsuper_user_password -v
   ```

   file_name

   Specifies the name of the file to which you exported the policy store.

   sm_super_user_name

   Specifies the Super User name of the SiteMinder administrator.

   super_user_password

   Specifies the password for the SiteMinder Super User.

   Example: smobjimport -ipstore.smdif -d"SM Admin" -wPassword -v

   Note: If the key store exists in the policy store, use the -k option.

3. Verify that the Policy Server is pointing to the policy store.

   The policy store is configured and you can now log into the Policy Server User Interface.

More Information:

Point the Policy Server at the Policy Store (see page 141)
Export Policy Data Using smobjexport (see page 146)
Import Policy Data Using smobjimport (see page 150)

Point the Policy Server at the Policy Store

Once you have created a new policy store or key store, or migrated or moved an ODBC policy store, you must configure the Policy Server to use the ODBC database. You can also use the Policy Server Management Console to configure additional Policy Servers to leverage an existing policy store in an ODBC database.

When you use the Policy Server Management Console to change the Policy Store from LDAP to ODBC, the key store does not automatically switch to ODBC, even when it is set to use the same store as the policy store. You must manually change both to ODBC for the key store to be accepted by the Policy Server Management Console.

Note: Refer to the *Policy Server Management* guide for detailed information about using the Policy Server Management Console.

To point the Policy Server at the policy store

1. On the server where the Policy Server is installed, open the Policy Server Management Console and select the Data tab to bring it to the front.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. Do the following:

   a. In the Database drop-down menu, select Policy Store.

   b. In the Storage drop-down menu, select LDAP.

   c. In the LDAP Policy Store box, configure the fields for the LDAP policy store.

      The following lists sample values for the fields:

      LDAP IP Address: 123.123.12.12:3500

      Root DN: o=test

      Admin Username: cn=admin,ou=people,o=test

      Password: *masked_password*

      Note: For more information about the LDAP settings, see the *Policy Server Management Guide*.

   d. (Optional) If the Policy Server is communicating with the LDAP directory over SSL, select the Use SSL check box.

e. Click Apply after you have modified the LDAP fields.

f. Click the Test LDAP Connection button to test the connection.

If the connection is successful, SiteMinder returns a confirmation. If it is not successful, SiteMinder returns an error message. If you receive an error message, verify that the values you entered are correct and that the database is running.

Create a Sample User Directory for Oracle or SQL Server

SiteMinder provides schema files to create sample users to populate a user directory for the Policy Server. The following schema files are provided in the \siteminder\db\Sql directory:

smsampleusers_oracle.sql

Creates the schema for SiteMinder sample users in an Oracle database and populates the database with sample users. For example, if you look in the script, you can see a sample user named GeorgeC with a password of siteminder.

smsampleusers_sqlserver.sql

Creates the schema for SiteMinder sample users in a SQL Server database and populates the database with sample users. For example, if you look in the script, you can see a sample user named GeorgeC with a password of siteminder.

Note: These user directories are optional since your environment will have different ones.

Create the database objects by running the appropriate SQL script(s) using SQL Plus for Oracle or the SQL Server Enterprise Manager and SQL Server Query Analyzer.

Note: For information about running SQL scripts, refer to your database documentation.

More Information:

Delete SiteMinder Data in ODBC Databases (see page 167)

Create a Sample User Directory for Oracle

If you are using an Oracle database as a user directory, run the smsampleusers_oracle.sql script to create a schema for it.

To create a sample Oracle user directory

1. Make sure the Oracle database instance that will contain the SiteMinder sample user data is accessible from the Policy Server machine. Test the communication using tnsping or sqlplus.
2. Create the sample user directory schema in the Oracle database:
   a. Log in to Oracle with sqlplus (or some other Oracle utility) as the user who administers the Policy Server database information.
   b. Import the script to create the sample users schema:

      $NETE_PS_ROOT/db/sql/smsampleusers_oracle.sql

      If you are using sqlplus, run the schema using an @ sign.

      Example: @$NETE_PS_ROOT/db/sql/smsampleusers_oracle.sql

Note: Environment variables may not function in Oracle's SQL utility. If you encounter problems when using the utility, specify an explicit path for $NETE_PS_ROOT rather than one with an environment variable.

Create a Sample User Directory for SQL Server

If you are using a SQL Server database as a user directory, run the smsampleusers_sqlserver.sql script to create a schema for it.

To create a sample SQL Server user directory

1. Make sure the SQL Server database instance that will contain the SiteMinder sample user data is accessible from the Policy Server machine.
2. Using the SQL Server Enterprise Manager, create the database instance for the sample user directory.

   Example: smuserstore.
3. Create the SiteMinder schema in the SQL Server database:
   a. Open smsampleusers_sqlserver.sql in a text editor and copy the contents of the entire file.
   b. Start the Query Analyzer and log in as the user who administers the Policy Server database information.

c. In the Query Analyzer, select the smuserstore database instance from the database drop down list at the top middle of the screen.

d. Paste the sample users schema from smsampleusers_sqlserver.sql into the query.

e. Execute the query.

Chapter 5: Policy Server Tools

This section contains the following topics:

Policy Server Tools Overview

SiteMinder provides administrative tools to help you manage the SiteMinder environment. The following list describes the function of each tool:

- **smobjexport**—This tool contains arguments that let you export the following:
  - An entire policy store.
  - A specified policy domain.
  - The specified policy domain and all system objects used by the policy domain, such as administrators, Agents, authentication schemes and user directories.
  - Agent keys stored in the policy store along with the rest of the policy store data. By default, keys are not included in the export.
  - Only the Agent keys stored in the policy store.
  - Only variables.
- **smobjimport**—This tool imports policy data into the SiteMinder policy store.
- **smldapsetup**—This tool manages the SiteMinder policy store in an LDAP directory.
- **ODBC database SQL scripts**—This tool removes SiteMinder policy store and log schema from ODBC databases.
- **smpatchcheck**—This tool verifies that all required and recommended patches are installed on the Solaris Policy Server host system.
- **smreadclog**—This tool reads RADIUS log files the Policy Server creates.
- **smreg**—This tool changes the SiteMinder super user password.

Requirement When Using the Policy Server Tools on Linux Red Hat

For the Policy Server tools (smreg, smobjimport, smobjexport) to work correctly on a Linux Red Hat operating system, you must define the Policy Server host name in /etc/hosts. The host name must be defined in this location because these utilities generate adminoids and OIDs. The operating system uses the gethostid() and gettimeofday() Linux functions when generating these OIDs.

Windows 2008 Policy Server Tools Requirement

If you are running a SiteMinder utility or executable on Windows Server 2008, be sure to open the command–line window 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.

Export Policy Data Using smobjexport

The smobjexport tool exports the entire policy store or a single policy domain by creating two files: an .smdif (SiteMinder Data Interchange Format) and .cfg (environment configuration) file. The .smdif file standardizes SiteMinder data so you can import it to a different type of policy store. For example, you can export an .smdif file from an ODBC database and import it to an LDAP directory.

The environment configuration (.cfg) file contains environment-specific properties for the policy store such as IP Addresses, redirection URLs, shared secrets, agent names, logging settings, and .com extensions. Only the 5.0, 5.5, and 6.x versions of smobjexport create an environment configuration file, as this feature is not available for previous versions. Tabs separate the text in the .cfg file, and you can edit it as a tab-delimited file in any text editor or Microsoft Excel.

Note: Using the Scripting Interface, you can write Perl scripts to import and export particular objects rather than all the Policy Store objects. For more information, see the *Programming Guide for Perl*.

The following table describes the four fields of a sample registration scheme entry from the .cfg file.

Object OID	Object Class	Property Type	Value
reg scheme OID	SelfReg	RegistrationURL	http://your.url.com

The Object OID column is represented only by the *OID* variable since OIDs such as the following are too long to fit:

reg scheme OID = 0d-6dc75be0-1935-11d3-95cc-00c04f7468ef

Each entry's fields--Object OID, Object Class, Property Type, Value--can be edited in a text editor or Excel.

Note: For backward compatibility purposes, the smobjexport command line only references the .smdif file. As a result, the corresponding environment configuration file is created according to the following naming convention. The output file you specify with the smobjexport command has an .smdif extension (for example, *filename*.smdif), then the extension is replaced with .cfg (such as *filename*.cfg) for the configuration file. However, if the output file you specify does not have an .smdif extension (for example, *filename*.txt), then .cfg is appended to file name and extension (such as *filename*.txt.cfg).

smobjexport uses the following arguments to supply the information required to export the data:

-o*file_name*

Specifies the path and filename of the output .smdif file. If this argument is not specified, the default output file names are stdout.smdif and stdout.cfg. This filename should be a name other than the one used for smldapsetup ldgen -f*filename*; otherwise the export will be overwritten.

-f

Overwrites an existing output file.

-s*domain_name*

Exports only the specified policy domain.

-e*domain_name*

Exports the specified policy domain and all system objects used by the policy domain, such as administrators, Agents, authentication schemes, and user directories, including the following:

- If one of the system objects is a Host Configuration object, all Host Configuration objects are exported.
- If one of the system objects is an Agent Configuration object, all Agent Configuration Objects are exported.
- If one of the system objects is an affiliate (when the Policy Server Option Pack is installed), the entire domain to which the affiliate belongs is exported.

-c

Exports sensitive data as clear-text. Exporting data as clear-text allows you to migrate policy data from a SiteMinder deployment that uses one encryption key to another SiteMinder deployment that uses a different encryption key. To use -c, you must enter the credentials of a SiteMinder administrator who can manage all SiteMinder domain objects. Enter credentials using the -d and -w arguments.

-d*admin_name*

Specifies the login name of a SiteMinder Administrator that can manage all SiteMinder objects in the policy store being exported.

-w*admin_pw*

Specifies the password of the SiteMinder Administrator specified using -d.

-k

Exports Agent keys stored in the policy store along with the rest of the policy store data. By default, keys are not included in the export.

-x

Exports only the Agent keys stored in the policy store.

-v

Enables verbose mode.

-t

Enables low level tracing mode. This mode can be used to troubleshoot the export process.

-u

Export variables only.

-l

Creates a log file. Make sure the *file_name*.smdif file ends with an .smdif and not a .txt or other extension. If the *file_name*.smdif file ends with an .smdif extension, smobjexport creates a log file with a .log extension. However, if the *file_name*.smdif file ends with a .txt extension, smobjexport creates a *file_name*.txt.log file, which is incorrect since the log file must be in the *file_name*.log format.

-m

Exports IdentityMinder objects only.

-i

Exports specific IdentityMinder objects and all relevant system objects.

-j

Exports a specific IdentityMinder directory and all relevant system objects.

-?

Displays the help message.

Note: If the arguments contain spaces, use double quotes around the entire argument. For example, if the name of the SiteMinder administrator is *SiteMinder Admin*, the argument for smobjexport would be
-d" SiteMinder Admin".

To export data using smobjexport

1. Navigate to one of the following locations:
   - (Windows) *siteminder_home*\bin

     Note: For a complete listing of the smobjexport parameters, enter smobjexport -? at a command prompt.
   - (UNIX) *siteminder_home*/bin

     siteminder_home

     Specifies the Policy Server installation path.
2. Enter the following command:

   ```
   smobjexport -ofile_name.smdif -c -dadmin_name -wadmin_pw -v -t
   ```

   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.

   file_name

   Specifies the name of the .smdif output file that will contain the exported policy store data

   admin_name

   Specifies the name of a SiteMinder administrator that can manage all SiteMinder objects

   admin_pw

   Specifies the password for the specified SiteMinder administrator.

   Note: Be sure that the *file_name*.smdif file ends with a .smdif and not a .txt extension.

   Example: smobjexport -opstore.smdif -c -dSiteMinder -wpassword -v -t

   Note: The -o*file_name* argument should use a name other than the one used for the smldapsetup ldgen -f*file_name;* otherwise the export may be overwritten.

Export Policy Store Objects With Dependencies

When exporting policy store objects with dependencies by either running smobjexport with the –e option or by using the migration methods in the Command Line Interface:

- If any of the object's dependencies is a Host Configuration Object, then all Host Configuration Objects are exported.
- If any of the object's dependencies is an Agent Configuration Object, then all Agent Configuration Objects are exported.
- If any of the object's dependencies is an affiliate (when Policy Server Option Pack is installed), then the entire affiliate domain to which the affiliate belongs is exported.

Note: The -e option does not support export Affiliate domains.

Import Policy Data Using smobjimport

The smobjimport tool imports the entire policy store or a single policy domain using two files--an .smdif (SiteMinder Data Interchange Format) and a .cfg (environment configuration) file--created by smobjexport. The .smdif file standardizes SiteMinder data so you can import it into an ODBC or LDAP directory. For example, you can export an .smdif file from an ODBC database and import it to an LDAP directory. The environment configuration (.cfg) file contains environment-specific properties for the policy store such as the IP Addresses, redirection URLs, shared secrets, and logging settings. The text in the .cfg file is separated by tabs and you can read it in an Excel spreadsheet.

Using the Command Line Interface, you can write Perl scripts to import and export particular objects rather than all the Policy Store objects.

Note: The naming convention for smobjimport is the same as smobjexport in that it supports an .smdif file and .cfg file. Using smobjexport as an example, if the output file you specified with the smobjexport command has an .smdif extension (that is, *file_name*.smdif), then the extension is replaced with .cfg (such as *file_name*.cfg) for the configuration file. However, if the output file you specify does not have an .smdif extension (that is, *file_name*.txt), then .cfg is appended to file name and extension (such as *file_name*.txt.cfg).

smobjimport uses the following arguments to supply information required to import data:

-4

Allows you to import policy store data from SiteMinder 4.51/4.61.

-i*file_name*

Specifies the path and filename of the input .smdif file.

-f

Indicates that duplicate information should be overwritten. Be careful using this argument as it enables you to overwrite default SiteMinder objects that may have been imported into a new policy store by using smpolicy.smdif.

-c

Indicates that the input file contains sensitive data in clear-text. This argument allows to you import policy data from a SiteMinder deployment that uses one encryption key to another SiteMinder deployment that uses a different encryption key. This option requires the credentials of a SiteMinder administrator who can manage all SiteMinder domain objects. Enter credentials using the -d and -w arguments.

-d*admin_name*

Specifies the login name of a SiteMinder Administrator that can manage all SiteMinder objects.

-w*admin_pw*

Specifies the password of the SiteMinder Administrator specified in -d.

-k

Imports Agent keys stored in the policy store. If you import using this argument, and the policy store to which you are importing already contains keys, single sign-on for existing users may be interrupted. Note that keys are created each time you start the Policy Server.

-v

Enables verbose mode.

-t

Enables low level tracing mode. This can be used to troubleshoot the import process.

-l

Creates a log file. Make sure the *file_name*.smdif file ends with an .smdif and not a .txt or other extension. If the *file_name*.smdif file ends with an .smdif extension, smobjimport creates a log file with a .log extension. However, if the *file_name*.smdif file ends with a .txt extension, smobjimport creates a *file_name*.txt.log file, which is incorrect since the log file must be in the *file_name*.log format.

-r

Turns off automatic renaming of objects. By default, when smobjimport attempts to import an object with a name that already exists in the target policy store, it creates a duplicate object with a name of *name_oid*, where *name* is the name of the object, and *oid* is the object ID of the new duplicate object. If you use this flag to turn off the automatic renaming feature, smobjimport returns errors messages for any objects that could not be created because of naming conflicts.

-u

Import variables only.

-m

Import IdentityMinder objects only.

+m

Import SiteMinder objects only.

-?

Displays the help message.

-a1

Disables object store validation and helps increase the speed at which objects are imported.

Important! This parameter should only be used when importing data into a new policy store and when the imported .smdif file is consistent with regards to policy store objects.

-a2

Disables object store auditing and helps increase the speed at which objects are imported.

-a3

Disables object store cache updates and helps increase the speed at which objects are imported.

Important! Do no use this parameter when importing data into an existing policy store with more than one policy store pointing at it. Using this parameter disables cache synchronization between the Policy Servers.

-a

Same as setting -a1, -a2, and -a3 together.

Important! This should only be used on a new policy store. Do not use this parameter when importing data into an existing policy store since it could corrupt the policy store.

Note: If any of the arguments contain spaces, use double quotes around the entire argument. For example, if the name of the SiteMinder administrator is *SiteMinder Admin*, the argument for smobjimport would be -d"SiteMinder Admin". If the description of a SiteMinder object specified in the Policy Server User Interface is more than one line long, smobjimport will only import the first line of the description.

To import Policy data using smobjimport

1. Navigate to one of the following locations:
   - *(Windows) siteminder_home*\bin
   - *(UNIX) siteminder_home*/bin

   siteminder_home

   Specifies the Policy Server installation path.
2. Enter the following command:

   ```
   smobjimport -ifile_name -dadmin_name -wadmin_pw -v -t
   ```

   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.

   Example: smobjimport -ipstore.smdif -dSiteMinder -wpassword -v -t

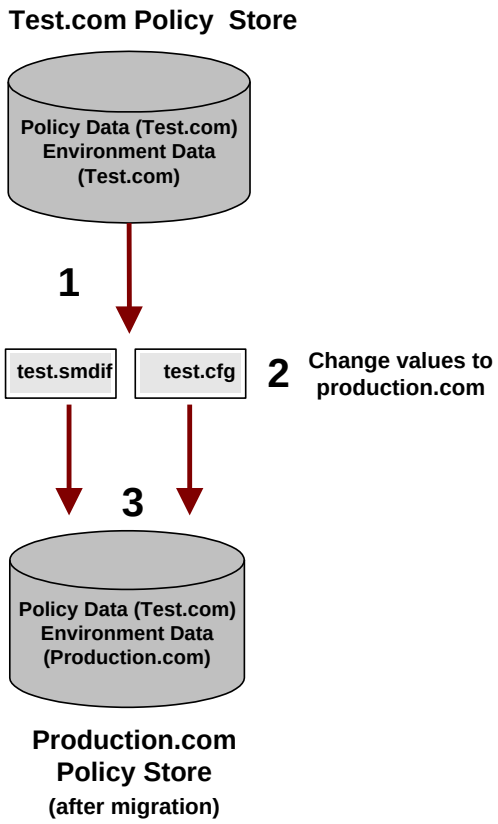
   Note: You only need to enter the .smdif file with the smobjimport command, since it automatically imports both the .smdif and .cfg files together if they are in the same directory. The environment properties stored in the .cfg file take precedence over the ones in the .smdif file. Thus, you can overwrite an environment's data by pairing the .smdif file with a different .cfg file when running smobjimport.

Migrate 6.x Policy Stores With Different Environments

The following sections detail migrating 6.x policy stores with in different environments.

Example 1 Policy Stores with Different Objects and Environments

In this example, there are two policy stores--one for test.com and another for production.com--containing different objects and environments. The goal is to migrate and override existing policy store data objects in production.com with those from test.com but keep production.com's environment settings by following the steps listed in the following figure.



1. Export the Test.com policy store into test.smdif, which backs up the policy data, and test.cfg, which preserves the environment settings.

   Note: The text in the .cfg file is separated by tabs and you can read it in any text editor or as a tab-delimited file in Microsoft Excel.

2. To change test.com's environment to match the settings in production.com, do the following:

   a. Using Microsoft Excel or a text editor, open test.cfg.

   b. Replace the test.com values with those from production.com. For illustrative purposes only, replace values such as IP Addresses, registration URLs, shared secrets, and agent names listed in the following table with those from production.com listed in the second table.

      Note: These are just four sample values and you will need to edit other values based on your own environment.

   Important! Make sure you only edit the Value entries and not the ones for Object OID, Object Class, Property Type.

Object OID	Object Class	Property Type	Value
Trusted Host OID	TrustedHost	IPAddr	192.216.167.23
reg scheme OID	SelfReg	RegistrationURL	http://test.url .com
auth scheme OID	Scheme	Secret	testpassword
agent OID	Agent	Name	testagent

The Object OID column is represented only by the OID variable since OIDs such as the following are too long to fit in the above table:

Trusted Host OID = 0d-6dc75be0-1935-11d3-95cc-00c04f7468ef

Object OID	Object Class	Property Type	Value
Trusted Host OID	TrustedHost	IPAddr	192.216.167.24
reg scheme OID	SelfReg	RegistrationURL	http://production.url.com
auth scheme OID	Scheme	Secret	productionpassword
agent OID	Agent	Name	productionagent

3. Import test.smdif and test.cfg, which you edited to include the values from production.com, into the Production.com policy store:

   ```
   smobjimport -itest.smdif -dSiteMinder -wpassword -v -f -t
   ```

   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: To override existing data and matching objects in the Production.com policy store with that of Test.com, use the **-f** argument.

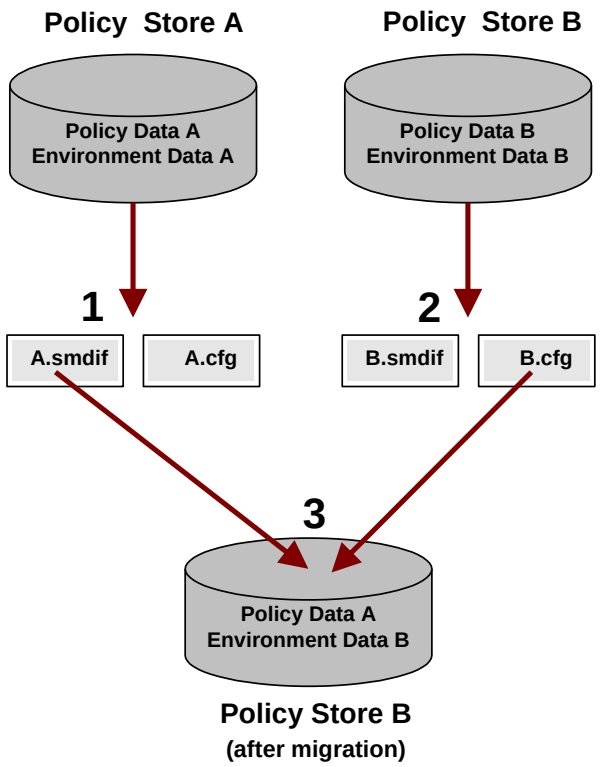
smobjexport and smobjimport let you export or import an entire policy store or an individual domain.

Note: For more information about exporting or importing individual objects on a smaller scale, see the *API Reference Guide for Perl*.

Example 2 Policy Stores with Same Objects But Different Environments

In this example, there are two synchronized 6.x policy stores--A and B--containing the same objects with the same object IDs (OIDs) but different environments. The goal is to migrate 6.x policy data from A into B and keep the original B environment settings by doing the steps listed in the following figure using the .smdif and .cfg files. The .smdif files (A.smdif and B.smdif) back up the policy data. The configuration files (A.cfg and B.cfg) expedite incremental updates between the stores and preserve environment-specific properties such as Agent IP Addresses, redirection URLs, shared secrets, Agent names, logging settings, and .com extensions.

The following figure shows this environment.



To migrate 6.x policy data from A into B and keep the original B environment settings:

1. Export policy store A into A.smdif, which backs up the policy data, and A.cfg, which preserves the environment settings.

   ```
   smobjexport -oA.smdif -c -dSiteMinder -wpassword -v -t
   ```

   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.

2. Export policy store B into B.smdif, which backs up the policy data, and B.cfg, which preserves the environment settings.

   ```
   smobjexport -oB.smdif -c -dSiteMinder -wpassword -v -t
   ```

3. Import policy data from A into B and preserve B's environment settings by:
   a. Renaming B.smdif to B.smdif.bak.
   b. Renaming A.smdif to B.smdif.
   c. Ensuring that B.smdif and B.cfg are in the same directory.
   d. Importing B.smdif (which used to be A.smdif) and B.cfg into policy store B.

      ```
      smobjimport -iB.smdif -dSiteMinder -wpassword -v -f -t
      ```

      To override existing data in policy store B with that of A, use the -f argument. You can override matching objects with this argument since you already backed up policy store B into B.smdif and B.cfg during the export.

Note: You can also migrate policy store data and the environment using the Scripting Interface for Perl. For more information, see the *API Reference Guide for Perl*.

smobjimport imports B.smdif and B.cfg into policy store B. The policy data in B.smdif, which contains policy data from A, overrides matching data in policy store B. The B environment settings stored in B.cfg overrides the settings stored in A.smdif. Thus, policy store B contains policy data from A, but the environment settings from B.

Note: If there are objects in A.smdif that do not have counterparts in B, then B.cfg will not override environment settings for non-matching objects.

smldapsetup

The smldapsetup utility allows you to manage an LDAP policy store from the command line. Using smldapsetup, you can configure an LDAP policy store, generate an LDIF file, and remove policy store data and schema.

To use smldapsetup, specify a mode, which determines the action that smldapsetup will perform, and arguments, which contain the values that are used to configure the LDAP server.

The following table contains the modes you can use with smldapsetup and the arguments each mode uses:

Modes	Arguments
reg	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1*|*0*, -c*certdb*, -k1

Modes	Arguments
ldgen	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -m*n*, -ssl*1*|*0*, -c*certdb* -f*ldif*, -t*tool*, -s*suffix*, -e, -k
ldmod	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1*|*0*, -c*certdb*, -f*ldif*, -s*suffix*, -e, -k, -i
remove	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1*|*0*, -c*certdb*, -k
switch	none
revert	-v
status	-v

To use smldapsetup

1. Navigate to one of the following locations:
   - (Windows) *siteminder_home*\bin
   - (UNIX) *siteminder_home*/bin

   siteminder_home

   Specifies the installed location of SiteMinder.

2. Enter the following command:

   `smldapsetup mode arguments`

   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.

   Example: smldapsetup reg -hldapserver.mycompany.com -d"LDAP User" -wMyPassword123 -ro=security.com

   Note: When running smldapsetup, make sure that the LDAP user you specify has the appropriate administrator privileges to modify schema in the LDAP Directory Server. If this user does not have the proper privileges, then the LDAP server will not allow you to generate the policy store schema. After running the smldapsetup command, this user appears in the Admin Username field on the Data tab of the Policy Server Management Console.

More Information:

Modes for smldapsetup (see page 160)
Arguments for smldapsetup (see page 161)

Modes for smldapsetup

The mode indicates the action that smldapsetup performs. You can specify a mode to connect to the LDAP server, generate an LDIF file, configure an LDAP policy store and remove policy data.

The modes for smldapsetup include:

reg

Tests the connection to the LDAP server. If the connection succeeds, smldapsetup configures the SiteMinder LDAP server as its policy store using the -h*host*, -p*portnumber*, -*duserdn*, -w*userpw*, -r*root*, -ssl*1/0* and -c*certdb* arguments.

ldgen

Automatically detects supported LDAP servers and generates an LDIF file with the SiteMinder schema. The generated file is used by smldapsetup ldmod to create the SiteMinder schema. If the -e argument is specified, smldapsetup ldgen creates an LDIF file that can be used with ldmod to delete the SiteMinder schema. Use the -m switch to skip automatic detection of LDAP servers. The ldgen mode requires the -f switch unless previously configured in reg mode.

ldmod

Connects to the LDAP server and the SiteMinder schema without populating the policy store with any data. It requires the LDAP modify program and the LDIF file, specified with the -*fldif* argument. If you specify the -h*host*, -p*port_number*, -d*userdn*,-w*userpw*, -r*root*, -ssl*1/0* and -c*certdb* arguments, smldapsetup ldmod will modify the LDAP directory specified using these arguments. If you do not specify -h*host*, -p*portnumber*, -d*userdn*, -*wuserpw*, -r*root*, -ssl*1/0* and -c*certdb*, smldapsetup ldmod uses the LDAP directory previously defined using smldapsetup reg or the Policy Server Management Console.

remove

Connects to the LDAP server, then removes all policy data stored under the SiteMinder LDAP node that corresponds to the current version of smldapsetup. If you specify the -*hhost*, -p*port_number*, -d*userdn*,-w*userpw*, -r*root*, -ssl*1/0* and -c*certdb* arguments, smldapsetup remove will remove policy data from the LDAP directory specified by these arguments. If you do not specify -h*host*, -p*port*, -d*userdn*, -w*userpw*, -r*root*, -*ssl1/0* and -c*certdb*, smldapsetup remove will remove the policy data from the LDAP directory previously defined using smldapsetup reg or the Policy Server Management Console.

switch

Reconfigures the Policy Server to use LDAP rather than ODBC. It does not prepare the LDAP store or the LDAP connection parameters before making the change.

revert

Reverts to ODBC policy store from LDAP. The only argument used with this mode is -v.

status

Verifies that the LDAP policy store connection parameters are configured correctly. It requires the -v argument. If you specify the -h*host*, -p*port_number*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1/0* and -c*certdb* arguments, smldapsetup status tests the connection to the LDAP directory specified using these arguments. If you do not specify -h*host*, -p*port_number*, -*duserdn*, -w*userpw*, -r*root*, -ssl*1/0* and -c*certdb*, smldapsetup status verifies the connection to the LDAP directory previously defined using smldapsetup reg or the Policy Server Management Console.

From the Data tab in the Policy Server Management Console, you can view or change the settings you configured with the reg, switch and revert functions using a GUI interface. You must use smldapsetup to perform the ldgen, ldmod, remove, and status functions.

Arguments for smldapsetup

Arguments allow you to specify the information used by the modes to manage the LDAP policy store. If you do not specify arguments, smldapsetup uses the values configured in the Policy Server Management Console.

Note: smldapsetup does not allow spaces between an argument and its value. For example, the -h argument should be specified as follows:
smldapsetup ldmod -hldapserver.mycompany.com

The arguments you can specify in an smldapsetup call are listed below:

-h*host*

Specifies the fully qualified name of the LDAP server; the relative name, if the machines are in the same domain (-hldapserver); or the IP address (-h123.12.12.12). If you do not specify a host, smldapsetup uses the previously configured value as the default.

Example: -hldapserver.mycompany.com

-p*port_number*

Specifies a non-standard LDAP port. The LDAP port must be specified if the LDAP server is using a non-standard port or if you are moving a server to a new server that uses a different port, such as moving from a server using SSL to one that is not. If a port is not specified, the previous configuration values are used. If no previous port configuration has been specified, smldapsetup uses the default ports 389, if SSL is not being used, or 636, if SSL is being used.

-d*userdn*

Specifies the LDAP user name of a user with the power to create new LDAP directory schema and entries. This is not necessarily the user name of the LDAP server administrator. If you do not specify a user name, smldapsetup uses the previously configured name as the default.

-w*userpw*

Specifies the password for the user identified in the -d argument. If you do not specify a password, smldapsetup uses the previously configuration value.

Example: -wMyPassword123

-r*root*

Specifies the distinguished name of the node in the LDAP tree where SiteMinder will search for the policy store schema. If you do not specify a root, smldapsetup uses the previously configured root.

Example: -ro=security.com

-e

When specified with smldapsetup ldgen, generates an LDIF file that can delete the SiteMinder schema. The generated file must be used with smldapsetup ldmod to remove the schema.

-m*n*

Skips automatic detection of LDAP servers and specify type of LDAP policy store where *n* is one of the following:

2

iPlanet v4 LDAP servers.

3

Active Directory LDAP servers.

4

Oracle Internet Directory.

5

iPlanet v5.

6

Sun Directory Servers.

9

Active Directory Application Mode (ADAM).

-f*ldif*

Specifies the absolute or relative path to an LDIF file from the directory in which smldapsetup is being executed.

Example: -f../siteminder/db/smldap.ldif

Default: if you do not specify a path, smldapsetup uses the current directory as the default.

-t*tool*

Specifies the absolute or relative path, including filename and extension, of the ldapmodify command line utility. Ldapmodify is used to configure the server schema using the LDIF format commands. LDAP servers and SiteMinder provide a copy of ldapmodify. If the utility is not in the default location, use this argument to specify its location.

-ssl*1_or_0*

Specify -ssl1 to use an SSL-encrypted connection to the LDAP server, and -ssl0 to use a non-SSL connection. If you do not specify a value for -ssl, smldapsetup uses the previously configured value. If the LDAP connection has not been configured before, the initial default value is 0.

-c*cert*

This argument must be specified when using an SSL encrypted (-ssl1) LDAP connection. Specifies the path of the directory where the SSL client certificate database file, which is usually called cert7.db for the Netscape Navigator Web browser, exists.

Example: If cert7.db exists in /app/siteminder/ssl, specify -c/app /siteminder/ssl when running smldapsetup ldmod -f/app/siteminder/pstore.ldif -p81 -ssl1 -c/app/siteminder/ssl.

Note: For policy stores using an SSL-encrypted connection to Sun Java System LDAP, make sure the key3.db file exists in the same directory as cert7.db.

-k-k1

Enables you to use smldapsetup to set up or modify a key store if you are storing key information in a different LDAP directory. If you specify -k, smldapsetup checks to see if the Policy Server is pointing to the key store before performing any functions. If the Policy Server is not pointing to the key store, smldapsetup issues a warning. If you specify -k1, in conjunction with smldapsetup ldgen and the other arguments for a new policy store, smldapsetup creates a separate key store in the location you specify. If you do not specify -k or -k1, smldapsetup will modify the policy store.

-v

Enables verbose mode for troubleshooting. With -v, smldapsetup logs its command-line arguments and configuration entries as it performs each step in the LDAP migration.

-i*userDN*

Specifies the distinguished name of an account that should be used by SiteMinder to make modifications to the policy store. This argument allows an administrator account to retain control of the SiteMinder schema while enabling another account that will be used for day-to-day modifications of SiteMinder data. When a change is made using the Policy Server User Interface, the account specified by this argument is used. Be sure to enter the entire DN of an account when using this argument.

-q

Enables quiet mode for no questions to be asked.

-u

Creates a 6.x upgrade schema file (LDIF).

-x

Use the -x argument with ldmod to generate replication indexes for another 5.x Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) LDAP directory server.

-ssuffix

This option allows you to specify a suffix other than the default parent suffix when configuring the 6.x Policy Server's schema in a Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) LDAP directory server.

Example: assume the following:

ou=Apps,o=test.com is the Policy Store root.

o=test.com is the root suffix.

ou=netegrity,ou=Apps,o=test.com is the sub suffix.

If you do not use the -s parameter with smldapsetup, the Policy Server assigns ou=Apps,o=test.com as a parent suffix of ou=netegrity,ou=Apps,o=test.com. To change this and have the appropriate parent suffix set, run smldapsetup using the -s parameter while specifying o=test.com.

-?

Displays the help message.

Note: If the arguments contain spaces, you must enter double quotes around the entire argument. For example, if the name of the SiteMinder administrator is LDAP user, the argument for smldapsetup would be: -d”LDAP user".

smldapsetup and Sun Java System Directory Server Enterprise Edition

In a Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) directory server, smldapsetup creates the ou=Netegrity, *root* sub suffix and PolicySvr4 database.

root

The directory root you specified in the Root DN field on the Data tab of the Policy Server Management Console. This variable has to be either an existing root suffix or sub suffix.

Example: If your root suffix is dc=netegrity,dc=com then running smldapsetup produces the following in the directory server:

- A root suffix, dc=netegrity,dc=com, with the corresponding userRoot database.
- A sub suffix, ou=Netegrity,dc=netegrity,dc=com, with the corresponding PolicySvr4 database.

Example: If you want to place the policy store under ou=apps,dc=netegrity,dc=com, then ou=apps,dc=netegrity,dc=com has to be either a root or sub suffix of the root suffix dc=netegrity,dc=com.

If it is a sub suffix, then running smldapsetup produces the following:

- A root suffix, dc=netegrity,dc=com, with the corresponding userRoot database.
- A sub suffix, ou=apps,dc=netegrity,dc=com, with the corresponding Apps database.
- A sub suffix, ou=Netegrity,ou=apps,dc=netegrity,dc=com, with the corresponding PolicySvr4 database.

Note: For more information about root and sub suffixes, see the Sun Microsystems documentation.

Remove the SiteMinder Policy Store using smldapsetup

To remove the SiteMinder policy store data and schema from an LDAP directory, you must first delete the data, then remove the schema.

Important!

- Before removing the SiteMinder policy store data, be sure that the Policy Server is pointing to the policy store that contains the data you want to delete. smldapsetup will remove the data from the policy store to which the Policy Server is pointing. Additionally, export the policy store data to an output file and create a backup of the file before removing the data.
- If you are running a SiteMinder utility or executable on Windows Server 2008, be sure to open the command–line window 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.

To remove the policy store using smldapsetup

1. Navigate to the following location:
   - (Windows) *siteminder_home*\bin
   - (UNIX) *siteminder_home*/bin

   siteminder_home

   Specifies the installed location of SiteMinder.
2. Remove the policy store data by entering the following command:

   ```
   smldapsetup remove -hLDAP_IP_Address -pLDAP_Port
   -d LDAP_Admin -wLDAP_Admin_Password -rLDAP_Base_DN
   -v
   ```

   Example: smldapsetup remove -h192.169.125.32 -p552 -d"cn=directory manager" -wfirewall -rdc=ad,dc=test,dc=com -v

   Note: Removing the policy store data may take a few moments.

3. Generate the LDIF file you will use to delete the schema by entering the following:

   `smldapsetup ldgen -e -fldif`

   ldif

   Specifies the name of the LDIF file you are generating.

   Example: smldapsetup ldgen -e -fdelete.ldif

4. Remove the SiteMinder schema by executing the following command:

   `smldapsetup ldmod -fldif`

   ldif

   Specifies the name of the LDIF file you generated using smldapsetup ldgen -e.

   Example: smldapsetup ldmod -fdelete.ldif

More Information:

Export Policy Data Using smobjexport (see page 146)

Delete SiteMinder Data in ODBC Databases

SiteMinder provides SQL scripts that delete the SiteMinder schema from ODBC databases. The following list describes each SQL script:

sm_oracle_ps_delete.sql

Removes the SiteMinder 6.x policy store and data from an Oracle database.

sm_oracle_logs_delete.sql

Removes SiteMinder 6.x logs stored in an Oracle database if the database was created using sm_oracle_logs.sql.

sm_oracle_ss_delete.sql

Removes the SiteMinder 6.x Session Server tables and data from an Oracle database.

sm_mssql_ps_delete.sql

Removes the SiteMinder 6.x policy store and data from an SQL database.

sm_mssql_logs_delete.sql

Removes SiteMinder 6.x logs stored in an SQL database if the database was created using sm_mssql_logs.sql.

sm_mssql_ss_delete.sql

Removes the SiteMinder 6.x Session Server tables and data from a SQL database.

sm_db2_ps_delete.sql

Removes the SiteMinder 6.x policy store and data from a DB2 database.

sm_db2_logs_delete.sql

Removes SiteMinder 6.x logs stored in a DB2 database if the database was created using sm_db2_logs.sql.

sm_db2_ss_delete.sql

Removes the SiteMinder 6.x Session Server tables and data from a DB2 database.

The ODBC database SQL scripts are in the following location:

- (Windows) *siteminder_home*\db

  siteminder_home

  Specifies the Policy Server installation path.

- (UNIX) *siteminder_home*/db

  siteminder_home

  Specifies the Policy Server installation path.

Delete the database objects by running the appropriate SQL script using DB2, SQL Plus for Oracle, or SQL Server Query Analyzer.

Note: For more information about running SQL scripts, see your database documentation.

smpatchcheck

The smpatchcheck tool lets you determine whether you have the Solaris patches required for the Policy Server and Web Agent installed on your system. Smpatchcheck can be run on the Solaris versions listed on the SiteMinder Platform Matrix. To access this matrix, go to Technical Support and search for the SiteMinder Platform Support Matrix.

To use smpatchcheck

1. Navigate to *siteminder_home*/bin

   siteminder_home

   Specifies the Policy Server installation path.

2. Enter smpatchcheck.

   Smpatchcheck looks for each required/recommended patch and then displays its status.

   For example:

```
Testing for Required Patches:
  Testing for Patch: 106327-09 ... NOT Installed
Testing for Recommended Patches:
  Testing for Patch: 106541-08 ... Installed
  Testing for Patch: 106980-00 ... Installed
SiteMinder Patch Check: Failed
```

Smpatchcheck returns one of the following messages:

Failed

One or more of the required patches is not installed.

Partially Failed

One or more of the recommended patches is not installed.

Success

All of the required and recommended patches are installed.

Read RADIUS Log Files With Smreadclog

This tool is used to read RADIUS log files generated by the Policy Server. It is useful for troubleshooting the Policy Server when used as a RADIUS authentication server. Options are provided to display individual RADIUS attributes that are exchanged between NAS and SiteMinder.

Smreadclog uses the following arguments to supply information required to read RADIUS log files:

-i*input_file*

Specifies the filename of the log file.

-o*output_file*

Specifies the filename of the output file.

-s*secret*

Specifies the shared secret that can be used to decode RADIUS passwords.

-r

Indicates that a hex dump of an entire RADIUS packet be displayed.

-a

Indicates that RADIUS attributes should be displayed individually.

-d

Indicates that RADIUS attributes should be displayed according to their definition in the policy store. This option displays actual attribute names as well as attribute values formatted based on their attribute type. Without this option, only the attribute name and value are displayed as a hex string.

-p*radius_server*

Records and replays RADIUS activity of the Policy Server service against your RADIUS server.

-m*authentication_port*

Specifies the port used for RADIUS authentication if that port is not the default port, 1645.

-n*accounting_port*

Specifies the port used for RADIUS accounting if that port is not the default port, 1646.

Note: For information about deploying the Policy Server as a RADIUS authentication server, see the *Policy Design* guide.

To use smreadclog

1. Navigate to one of the following locations:
   - (Windows) *siteminder_home*\bin
   - (UNIX) *siteminder_home*/bin

   siteminder_home

   Specifies the Policy Server installation path.
2. Enter the following command:

   ```
   smreadclog -iinput_file -ooutput_file
   -ssecret -r -a -d -pradius_server -mport_number
   -nport_number
   ```

   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.

   Example: smreadclog -iradiuslog.txt -oradiuslog2.txt
   -ssecret -r -a -d -p123.123.12.12

SiteMinder Test Tool

The SiteMinder Test Tool is a utility that simulates the interaction between Agents and Policy Servers. It tests the functionality of the Policy Server. During testing, the Test Tool acts as the Agent, making the same requests to the Policy Server as a real Agent. This lets you test your SiteMinder configuration before deploying it.

Note: For more information about the Test Tool, see the *Policy Design Guide*.

Change the SiteMinder Super User Password Using smreg

To change the super user password

1. Be sure that Policy Server is running and configured with a policy store.
2. Change the SiteMinder super user password by completing the following steps:
   a. Copy the smreg utility (smreg.exe) from the Policy Server installation kit to *siteminder_home*\bin.
   b. Execute the following command:

      ```
      smreg -su super_user_password
      ```

      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: Be sure that there is a space between -su and the password.

   c. Delete smreg.

      Deleting smreg prevents someone from changing the super user password.

Chapter 6: Configuring the OneView Monitor

This section contains the following topics:

OneView Monitor Overview

The OneView Monitoring infrastructure consists of a number of modules that enable the monitoring of SiteMinder components. Included is the Monitor process that runs in the context of a Java Runtime Environment (JRE). The Monitor GUI's HTML pages are generated by Java Server Pages (JSPs) and servlets hosted on a ServletExec servlet engine running on the same machine as the Policy Server.

The OneView Monitor utility monitors the following SiteMinder components:

- Policy Server
- Web Agents

Note: More information about using the OneView Monitor exists in the *Policy Server Management Guide*.

System Requirements for OneView Monitor GUI

The following requirements exist for the OneView Monitor GUI:

- JDK: Make sure you have the required Java SDK. For the required version, search for the SiteMinder Platform Matrix on the Technical Support site. You can download the latest Java SDK at the Sun Developer Network (SDN).
- Servlet Engine: Make sure you have the required ServletExec/ISAPI for Windows or ServletExec/AS for UNIX. For the required versions, search for the SiteMinder Platform Matrix on the Technical Support site.
- For a list of supported Web Servers for Windows and UNIX systems, search for the SiteMinder Platform Matrix on the Technical Support site.

Oneview Monitor GUI Configuration During Policy Server Installation

During the Policy Server installation, you can have the install program automatically configure the OneView Monitor GUI.

If you did not have the OneView Monitor GUI automatically configured by the Policy Server installer, you can set it up using the Policy Server Configuration Wizard (nete-ps-config.exe or nete-ps-config.bin, which is located in the <*siteminder_installation*>/install_config_info directory).

More Information:

Run the Policy Server Configuration Wizard (see page 25)
Run the Configuration Wizard Using a GUI or Console Window (see page 66)

How to Configure the OneView Monitor GUI on Windows/IIS

Configuring the OneView Monitor GUI on Windows/IIS requires you to:

1. Read the prerequisites (see page 175) to installing ServletExec on Windows.
2. Install ServletExec/ISAPI on Windows/IIS.

   Note: The Monitor GUI's HTML pages are generated by Java Server Pages (JSPs) and servlets hosted on a ServletExec servlet engine running on the Policy Server host system.
3. Assign modify permissions to the Internet guest account for the *siteminder_home*\monitor\settings folder.
4. Set permissions for the IIS Users (see page 175).
5. If you did not use the Policy Server installer to automatically configure the OneView Monitor GUI, configure it by running the Policy Server Configuration Wizard.

   Note: For more information on the Policy Server Configuration Wizard, see Run the Policy Server Configuration Wizard (see page 25).
6. Start the OneView Monitor service (see page 178).
7. Access the OneView Monitor GUI (see page 178).

Prerequisites to Installing ServletExec on Windows

CA recommends that you read the ServletExec documentation before installing ServletExec. If ServletExec is not running properly, then the OneView Monitor GUI does not work since it relies on ServletExec's servlet engine.

Note: You can access the ServletExec documentation on the New Atlanta Web site.

Install ServletExec/ISAPI on Windows/IIS

To install ServletExec/ISAPI on Windows/IIS

1. If you have an earlier version of ServletExec:
   a. If desired, back up the ServletExec Data and Servlets sub–directories.
   b. Remove the earlier version.
2. Run the ServletExec ISAPI installer.

   Note: For more information about installing ServletExec ISAPI, see the ServletExec documentation.
3. Stop and restart the IIS Admin Web service and IIS Web server.

Set Permissions for IIS Users After Installing ServletExec

Because ServletExec/ISAPI runs as part of the IIS process, it runs as different users at different times. As a result, you must set the following permissions for the ServletExec installation directory and subdirectories.

To set permissions for IIS users after installing ServletExec, be sure that the user that runs IIS (for example, Network Services) has read and write access to the entire directory tree under C:\Program Files\New Atlanta.

More Information:

Start the OneView Monitor Service (see page 178)

Limitation of OneView Monitor GUI/IIS Web Agent on Same Machine

CA does not support the configuration of the IIS-based OneView Monitor GUI and the IIS Web Agent on the same machine if the Agent has Registration Services enabled. With this configuration, there is a conflict with the same instance of ServletExec.

How to Configure the OneView Monitor GUI on UNIX/Sun Java System

Configuring the OneView Monitor GUI on a UNIX/Sun Java System requires you to:

1. Read the prerequisites (see page 176) to installing ServletExec.
2. Disable servlets (see page 176) in Sun Java System (Sun One/iPlanet) 6.0.
3. Install ServletExec/AS (see page 177) on UNIX/Sun Java System.
4. If you did not have the Policy Server installation program auto-configure the OneView Monitor GUI.

   Note: Details on auto-configuring exist in Run the Configuration Wizard Using a GUI or Console Window (see page 66). Details on manually configuring exist in Manually Configure the OneView Monitor GUI on UNIX/Sun Java System 6.0 (see page 215).
5. Start the OneView Monitor Service (see page 178).
6. Access the OneView Monitor GUI (see page 178).

Prerequisites to Installing ServletExec

CA recommends that you read the ServletExec documentation before installing ServletExec. If ServletExec is not running properly, then the OneView Monitor GUI does not work since it relies on ServletExec's servlet engine.

You can access the ServletExec documentation on the New Atlanta Web site.

Disable Servlets in Sun Java System 6.0

Ensure you follow the steps in this section before installing ServletExec.

To disable servlets in Sun Java System 6.0

1. Open the Sun Java System Enterprise Administration Server home page by entering the following URL in a browser: http://<yourserver.com>:<portnumber>

   yourserver.com

   Specifies the domain name of the Enterprise Administration Server

   port

   Specifies the port number
2. In the Select a Server drop-down menu, select the target server, and then click Manage.

3. Select the Java tab.
4. Deselect Enable Java for class defaultclass and Enable Java Globally and click OK.
5. Stop and restart the Web server so the settings can take effect.

Install ServletExec/AS on UNIX/Sun Java System

The Monitor GUI's HTML pages are generated by Java Server Pages (JSPs) and servlets hosted on a ServletExec servlet engine running on the same machine as the Policy Server.

To install ServletExec

1. Log in to the UNIX account where you want to install the Policy Server.

   Note: You must log in as the same user who installed the Sun Java System Web server.

2. Run the ServletExec AS installer.

   Note: For more information on running the ServletExec AS installer, refer to New Atlanta Communications' ServletExec documentation. Consider the following before installing ServletExec:

   - Make sure you have permission to create a new file in /tmp. New Atlanta recommends installing ServletExec in /usr/local/NewAtlanta. Installing ServletExec in /usr/local/NewAtlanta may change the permissions for the obj.conf file and the Sun Java System start script. After the installation, be sure the owner of obj.conf and the start script is the same user who owns the Web server.
   - When prompted, install a Web server adaptor and an instance of ServletExec.
   - When prompted, ensure that the installer does not modify the Web server's configuration files. If you let the installer modify the Web server's obj.conf and magnus.conf configuration files, the Web server instance fails to run after you configure the OneView Monitor GUI on this instance.

3. After the installation program completes, restart the Web server.

More Information:

Start the OneView Monitor Service (see page 178)

Start the OneView Monitor Service

To start the OneView Monitor service

1. Make sure the IPC port numbers are available.

   The OneView Monitor uses the following port numbers to communicate with the Policy Server processes:

   - Monitoring Agent: 44449
   - Monitor: 44450

   To see which port numbers are unavailable, open a Command Window and enter:

   ```
   netstat -an
   ```

   Note: For more information on changing the port numbers, see the P*olic*y Server Management Guide.

2. Using the Status tab of the Policy Server Management Console, start the Monitor service.

Access the OneView Monitor GUI

To access the OneView Monitor GUI

Enter the following URL in a browser:

http://*server:<portnumber>*/siteminder**monitor**

server

Specifies the Web Server's IP Address

portnumber

Specifies the port number.

Monitor a Policy Server Cluster

The OneView Monitor can be configured to monitor a Policy Server cluster when one Policy Server is set up as a centralized monitor for other Policy Servers in a cluster.

Note: More information on the OneView Monitor exists in the *Policy Server Management Guide*.

Chapter 7: Prerequisites for Running Reports Using Crystal Reports

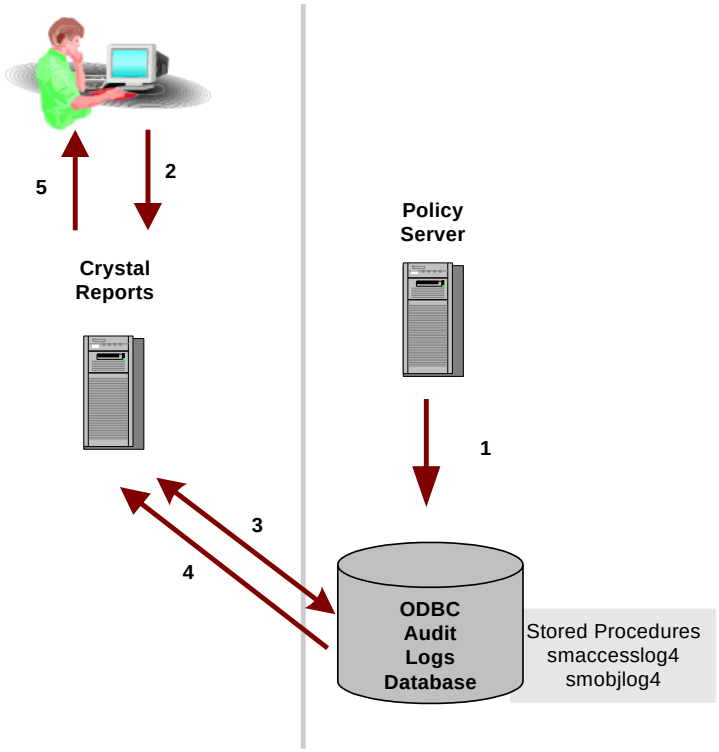
This section contains the following topics:

Crystal Reports in a Policy Server Environment

In SiteMinder 6.0, the Policy Server does not install a Crystal Reports Server as with previous SiteMinder 5.x and 4.x versions. However, the Policy Server still generates audit logs and stores the necessary reporting information in a SQL Server or Oracle database. The Policy Server 6.0 installation program installs sample reports files (.rpt) that are compatible with Crystal Reports 9.0.

Note: These sample files are provided so that customers can continue to use Crystal Reports to read reporting data from the Policy Server's audit logging database. However, CA does not provide support for using the sample files.

The following figure shows a sample Crystal Reports 9.0 and Policy Server environment:



In the above figure, the Policy Server resides on either a UNIX or Windows platform, with a database for audit logs. Crystal Reports resides on a Windows platform, and is configured to communicate with the audit logs database.

The following steps describe the events that occur in a Crystal Reports and Policy Server environment when a user requests a report:

1. The Policy Server generates audit logs and stores the information in an ODBC (SQL Server or Oracle) database. The Policy Server writes reporting information to the database using the SiteMinder logs data source.
2. A user requests a report using Crystal Reports.
3. When the user selects a report to run, Crystal Reports creates a SQL select statement based on the user's filter criteria and retrieves the information required by the report from the database. Report information is located in the smaccesslog4 and smobjlog4 tables of audit logs database. Crystal Reports reads the reporting information from the audit logs database using the ODBC Crystal Reports data source.

4. The result set of the SQL select statement is passed to Crystal Reports.
5. Crystal Reports passes the formatted report information to the user.

Before You Begin

Verify that the following requirements are met:

- You have Crystal Reports 9.0 Developer and Crystal Reports 9.0 Application Server installed, as you will need this software to modify and run the SiteMinder reports.
- For Crystal Reports, apply the latest Crystal Enterprise 9 Database and Export Drivers Monthly Hot Fix (MHF) update, CE90DBEXWIN_EN.ZIP or later, available at the BusinessObjects site.
- You will need an Oracle or SQL Server client installed on the Crystal Reports' machine if you do not use the Oracle or SQL Server wire protocol drivers when configuring a Crystal Reports data source.
- For a list of supported operating systems, Web Servers, databases, Web browsers, see the SiteMinder Platform Matrix for 6.0. To access this matrix, go to the Technical Support site and search for the SiteMinder Platform Matrix for 6.0.

How to Configure the Policy Server for Crystal Reports

To configure Crystal Reports to run SiteMinder reports:

1. Create a logging database schema. The Policy Server generates audit logs and stores the necessary reporting information in a SQL Server or Oracle database.
   - Create the Oracle Database Schema For Logging (see page 182).
   - Create the SQL Server Database Schema For Logging (see page 183).
2. Create the stored procedures database schema.
   - Create the Oracle Database Schema For Stored Procedures (see page 184).
   - Create the SQL Server Database Schema For Stored Procedures (see page 185).
3. Create an ODBC logs data source to write to the logging database.
   - Configure an Oracle ODBC Logs Data Source (see page 186).
   - Configure a SQL Server ODBC Logs Data Source (see page 187).
4. Create an ODBC Crystal Reports data source to read from the logging database.
   - Configure an Oracle ODBC Crystal Reports Data Source (see page 188).
   - Configure a SQL Server ODBC Crystal Reports Data Source (see page 189).
5. Configure a Database to Store Audit Logs (see page 191).
6. Modify SiteMinder Reports to Use the Crystal Reports Data Source (see page 192)

Create the Oracle Database Schema For Logging

You may have already created an Oracle logging database when you created the Oracle database with the SiteMinder schema. If you already created a logging database, do not run sm_oracle_logs.sql again, as it will overwrite the current database with a new one.

If you are using Oracle to store reports information, run the sm_oracle_logs.sql script to create a schema for logging. If there is no schema in the database to log data, reports will not work. This script is included in the <*siteminder_installation*>\db\SQL directory.

siteminder_installation

Specifies the installed location of SiteMinder.

To create the Oracle database schema for logging

1. Make sure the Oracle database instance that will contain the SiteMinder logs data is accessible from the Policy Server machine. Test the communication using tnsping or sqlplus.
2. Create the SiteMinder schema in the Oracle database:
   a. Log in to Oracle with sqlplus (or some other Oracle utility) as the user who administers the Policy Server database information.
   b. Import the script to create a schema for logging:

      $NETE_PS_ROOT/db/sql/sm_oracle_logs.sql

      Note: If you are using sqlplus, run the schema using an @ sign.

      Example: @$NETE_PS_ROOT/db/sql/sm_oracle_logs.sql

   Note: Environment variables may not function in Oracle's SQL utility. If you encounter problems when using the utility, specify an explicit path for $NETE_PS_ROOT rather than one with an environment variable.
3. Create the Oracle database schema for stored procedures.

Note: The 6.x Policy Server and OneView Monitor services still start even if they are unable to connect to the audit logs database.

More Information:

Create the Oracle Database Schema For Stored Procedures (see page 184)

Create the SQL Server Database Schema For Logging

You may have already created a SQL Server logging database when you created the SQL Server database with SiteMinder schema. If you already created a logging database, do not run sm_mssql_logs.sql again as it will overwrite the current database with a new one.

If you are using SQL Server to store reports information, run the sm_mssql_logs.sql script to create a schema for logging. If there is no schema in the database to log data, reports will not work. This script is included in the <*siteminder_installation*>\db\SQL directory.

siteminder_installation

Specifies the installed location of SiteMinder.

To create the SQL Server database schema for logging

1. Make sure the SQL Server database that will contain the SiteMinder logs data is accessible from the Policy Server machine.
2. Using the SQL Server Enterprise Manager, create the logs database instance.
3. Create the SiteMinder schema in the SQL Server database:
   a. Open sm_mssql_logs.sql in a text editor and copy the contents of the entire file.
   b. Start the Query Analyzer and log in as the user who administers the Policy Server database information.
   c. In the Query Analyzer, select the logs database instance from the database drop down list at the top-middle of the screen.
   d. Paste the schema for logging from sm_mssql_logs.sql into the query.
   e. Execute the query.
4. Create the SQL Server database schema for stored procedures.

Note: The 6.x Policy Server's services (Policy Server and OneView Monitor) start even if they are unable to connect to the audit logs database.

More Information:

Create the SQL Server Database Schema For Stored Procedures (see page 185)

Create the Oracle Database Schema For Stored Procedures

If you are using Oracle to store reporting information, run the SmReportStoredProcedures_Oracle.sql script to create a schema for stored procedures in the logging database. You need to create the stored procedures, which the report files need to extract results from the database. This script is included in the <*siteminder_installation*>\reports directory.

siteminder_installation

Specifies the installed location of SiteMinder.

To create the Oracle database for stored procedures

1. Make sure the Oracle logging database instance that will contain the stored procedures schema is accessible from the Policy Server machine. Test the communication using tnsping or sqlplus.
2. Create the stored procedures schema in the Oracle logging database:
   a. Log in to Oracle with sqlplus (or some other Oracle utility) as the same Oracle user that you used to run the sm_oracle_logs.sql script.
   b. Import the script to create a schema for stored procedures:

      $NETE_PS_ROOT/reports/SmReportStoredProcedures_Oracle.sql

      Note: If you are using sqlplus, run the schema using an @ sign.

      Example: @$NETE_PS_ROOT/reports/ SmReportStoredProcedures_Oracle.sql
3. Configure the Oracle ODBC logs data source.

More Information:

Configure an Oracle ODBC Logs Data Source (see page 186)

Create the SQL Server Database Schema For Stored Procedures

If you are using SQL Server to store reporting information, run the SmReportStoredProcedures_SqlServer.sql script to create a schema for stored procedures in the logging database. You create the stored procedures because the report files need to extract results from the database. This script is included in the <*siteminder_installation*>\reports directory.

siteminder_installation

Specifies the installed location of SiteMinder.

To create the SQL Server database schema for stored procedures

1. Make sure the SQL Server logging database instance that will contain the stored procedures schema is accessible from the Policy Server machine.
2. Create the stored procedures schema in the SQL Server logging database:
   a. Open SmReportStoredProcedures_SqlServer.sql in a text editor and copy the contents of the entire file.
   b. Start the Query Analyzer and log in to SQL Server as the same user who ran the sm_mssql_logs.sql script.
   c. In the Query Analyzer, select the logs database instance from the database drop down list at the top-middle of the screen.
   d. Paste the schema for stored procedures from SmReportStoredProcedures_SqlServer.sql into the query.
   e. Execute the query.
3. Configure the SQL Server ODBC logs data source.

More Information:

Configure a SQL Server ODBC Logs Data Source (see page 187)

Next Steps

After creating the logging database schema and stored procedures, you need to:

1. Create an ODBC logs data source to write to the Policy Server's logging database:
   - Configure an Oracle ODBC Logs Data Source (see page 186).
   - Configure a SQL Server ODBC Logs Data Source (see page 187).

2. Create an ODBC Crystal Reports data source to read from to the Policy Server's logging database:
   - Configure an Oracle ODBC Crystal Reports Data Source (see page 188).
   - Configure a SQL Server ODBC Crystal Reports Data Source (see page 189).
3. Configure a Database to Store Audit Logs (see page 191).
4. Modify SiteMinder Reports to Use the Crystal Reports Data Source (see page 192).

Configure an Oracle ODBC Logs Data Source

The SiteMinder Logs Data Source allows the Policy Server to write logging messages to an Oracle database. Crystal Reports reads messages from this database to create reports.

To create and configure the SiteMinder Logs Data Source

1. Select Programs, Administrative Tools, Data Sources (ODBC) to access the ODBC Data Source Administrator**.**
2. Click the System DSN tab and click Add. The Create New Data Source dialog box appears.
3. Scroll down and select SiteMinder Oracle Wire Protocol and click Finish. The ODBC Oracle Wire Protocol Driver Setup dialog appears.
4. Under the General tab, do the following:
   a. In the Data Source Name field, enter any name you want.

      Example: SiteMinder Logs Data Source.

      Note: Take note of this name, as you will need it when you configure the database to store audit logs.

   b. (Optional) In the Description field, enter a description of the Oracle wire protocol logs data source.

   c. In the Host field, enter the machine name where the Oracle database is installed.

   d. In the Port Number field, enter the port number where Oracle is listening on the machine.

   e. In the **SID** field, enter the service name of the Oracle instance that you want to connect, which you specified in the tnsnames.ora file. The SID is the system identifier for the database instance.

The tnsnames.ora file contains service names and details that Oracle uses to identify and connect to Oracle instances. For example, if the tnsnames.ora file contains the following entry for an Oracle instance, enter **instance1** in the SID field.

f. instance1 =

```
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(Host = myhost)(Port =1521))
(CONNECT_DATA = (SID = SIDofinstance1))
 )
```

g. Test the connection with the database by clicking Test Connect.

5. Click OK to save the selections and exit the ODBC Oracle Wire Protocol Driver Setup.
6. Configure the database to store audit logs.

More Information:

Configure a Database to Store Audit Logs (see page 191)

Configure a SQL Server ODBC Logs Data Source

The SiteMinder Logs Data Source allows the Policy Server to write logging messages to a SQL Server database. Crystal Reports reads messages from this database to create reports.

To create and configure the SiteMinder Logs Data Source

1. Select Programs, Administrative Tools, Data Sources (ODBC) to access the ODBC Data Source Administrator**.**
2. Click the System DSN tab to move it to the front.
3. Click Add.

   The Create New Data Source dialog box appears.
4. Scroll down and select SiteMinder SQL Server Wire Protocol and click Finish.

   The ODBC SQL Server Wire Protocol Driver Setup dialog box appears.
5. In this dialog, do the following:
   a. In the Data Source Name field, enter the Data Source name
   b. Example: SiteMinder Logs Data Source.

      Note: Take note of this name, as you will need it when you configure the database to store audit logs.

   c. (Optional) In the Description field, enter a description of the data source.
   d. In the Server Name field, enter the name of an existing SQL server.

e. In the Database name field, enter the name of an existing database instance.

f. Click Test Connect to make sure to make sure the connection works.

g. Click OK.

6. Configure the database to store audit logs.

More Information:

Configure a Database to Store Audit Logs (see page 191)

Configure an Oracle ODBC Crystal Reports Data Source

The Crystal Reports Data Source allows Crystal Reports to read messages from the Policy Server's Oracle logging database.

Note: You will need an Oracle client installed on the Crystal Reports' machine to use the Oracle client driver in this section.

To create and configure the Crystal Reports Data Source

1. Select Programs, Administrative Tools, Data Sources (ODBC) to access the ODBC Data Source Administrator.
2. Click the System DSN tab to move it to the front.
3. Click Add.

   The Create New Data Source dialog box appears.
4. Scroll down and select the CR Oracle ODBC Driver 4.10 driver and click Finish.

   The ODBC Oracle Driver Setup dialog box appears.
5. Under the General tab, do the following:

   a. In the Data Source Name field, enter **Crystal Reports Oracle Data Source.**

   b. (Optional) In the Description field, enter a description of the data source.

c. In the Server Name field, enter the Oracle service name. Do not use blank spaces in the name.

   This is the Oracle client connection string (TNS) referenced in the Oracle Easy Configuration dialog box. Your version of Oracle may cause this dialog box to appear differently.

   The service name is the name assigned to an Oracle instance specified in the tnsnames.ora file. This file contains service names and details that Oracle uses to identify and connect to Oracle instances. For example, if the tnsnames.ora file contains the following entry for an Oracle instance, enter instance1 in the Server Name field.

   ```
   instance1 =
    (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(Host = myhost)(Port =1521))
    (CONNECT_DATA = (SID = SIDofinstance1))
    )
   ```

6. (Optional) Test the connection with the database by clicking Test Connect.
7. Click the Advanced tab
8. Check Procedure Returns Results and click Apply and OK.
9. Click OK to save the selections and exit the ODBC Oracle Driver Setup.

   The configuration is complete.
10. Edit the SiteMinder reports files to use this Crystal Reports data source.

More Information:

Modify SiteMinder Reports to Use the Crystal Reports Data Source (see page 192)

Configure a SQL Server ODBC Crystal Reports Data Source

The Crystal Reports Data Source allows Crystal Reports to read messages from the Policy Server's SQL Server logging database.

Note: You will need a SQL Server client installed on the Crystal Reports' machine to use the SQL Server client driver in this section.

To create and configure the Crystal Reports Data Source

1. Select Programs, Administrative Tools, Data Sources (ODBC) to access the ODBC Data Source Administrator.
2. Click the System DSN tab to move it to the front.
3. Click Add.

   The Create New Data Source dialog box appears.

4. Scroll down and select SQL Server and click Finish.

   The Create New Data Source to SQL Server dialog box appears.

5. In this dialog, do the following:

   a. In the Name field, enter **SQL Serv CR Reports Data Source**.

      Note: You must enter this name exactly as shown for the reports to work properly.

   b. (Optional) In the Description field, enter a description of the data source.

   c. In the Server field, enter the name of an existing SQL server.

   d. Click Next.

   e. The second Create New Data Source to SQL Server dialog box appears.

6. In this second dialog, do the following:

   a. Select the With SQL Server authentication using a login ID and password entered by the user radio button.

   b. Enter the login name and password of the SQL Server user who administers the Policy Server's logging database and click Next.

7. In the third dialog, do the following:

   a. If you do not want to connect to the default database, check Change the default database to, and select the database instance from the drop-down menu.

      Example: logs.

   b. Click Next.

8. In the fourth dialog, click Finish.

9. (Optional) In the ODBC Microsoft SQL Server Setup dialog, click Test Data Source to make sure the connection works and click OK.

   The configuration is complete.

   You can now edit the SiteMinder reports files to use this Crystal Reports data source.

More Information:

Modify SiteMinder Reports to Use the Crystal Reports Data Source (see page 192)

Configure a Database to Store Audit Logs

Before configuring an Oracle or SQL Server database to store audit logs, ensure you have created the database for schema logging and configured an ODBC logs data source.

Details on creating a database for schema logging exist in:

- Create the Oracle Database Schema For Logging (see page 182)
- Create the SQL Server Database Schema For Logging (see page 183)

Details on configuring an ODBC logs data source exist in

- Configure an Oracle ODBC Logs Data Source (see page 186)
- Configure a SQL Server ODBC Logs Data Source (see page 187)

To point the Policy Server to store audit logs in a database

1. In the Policy Server Management Console, click the Data tab to move it to the front.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. In the Database drop-down list, select Audit Logs.
3. In the Storage drop-down list, select ODBC.
4. (If necessary) Clear the Use Policy Store database check box and click Apply.

   The fields in the Data Source Information group box become active.

5. In the Data Source Information field, enter the name of the data source, which should be **SiteMinder Logs Data Source**.

   Note: This name must correspond to the SiteMinder Logs Data Source name you entered in the Data Source Name field when you configured your ODBC logs data source.

6. In the User Name and Password fields, enter the user name and password of the user who administers the Policy Server's logging database.
7. In the Confirm Password field, re-enter the password.
8. Specify the maximum number of database connections allocated to SiteMinder. For best performance, retain the default of 5 connections.
9. Click Test Connection to verify connectivity to the database server.
10. Click Apply to save the settings.

Modify SiteMinder Reports to Use the Crystal Reports Data Source

By default, all of the SiteMinder reports .rpt files installed in the *<siteminder_installation>*\reports directory are configured to use the SiteMinder Reports Data Source, which is the data source that allows Crystal Reports to read from the logging database. If your Crystal Reports data source name does not match SiteMinder Reports Data Source, then you will have trouble running reports. You modify each reports file so that it uses the Crystal Reports data source name you created when you configured your ODBC Crystal reports data source.

To modify SiteMinder reports to user the Crystal Reports data source

1. Go to Start, Programs, Crystal Reports.
2. Open one of the SiteMinder Activity, Intrusion, Administrative, or Time Series reports (.rpt) files in Crystal Reports.
3. Select Database, Set Datasource Location.
4. Under Replace with, in the Set DataSource Location dialog, expand Create New Connection, ODBC (RDO).
5. Under Data Source name, in the ODBC (RDO) dialog, select the Crystal Reports data source name you created and click Next.
6. In the next ODBC (RDO) dialog:
   a. Enter the user name and password of the user who administers the Policy Server's logging database.
   b. Make sure the correct name of the Policy Server's logging database appears in the Database drop down menu.
   c. Click Finish.
7. Under Replace with, in the Set DataSource Location dialog:
   a. Expand *<logging_database>* -> dbo -> Stored Procedures.

      logging_database

      Specifies the name of the Policy Server's logging database.

      Example: 60logs.

b. Highlight the report name under Stored Procedures and under Current Data Source at the top of the dialog.

   Example: SmGetIntrusionAll;1

c. Click Update.

8. In the Enter Parameter Values dialog, enter the appropriate parameters you want.

   Note: Oracle supports dates in the mm/dd/yyyy format. SQL database supports dd/mm/yyyy.

9. Click Close and save the report.

10. To preview the report, select Report, Refresh Report Data.

Note: To view SiteMinder reports using Crystal Reports, see the *Policy Server Management* guide.

More Information:

Configure an Oracle ODBC Crystal Reports Data Source (see page 188)
Configure a SQL Server ODBC Crystal Reports Data Source (see page 189)

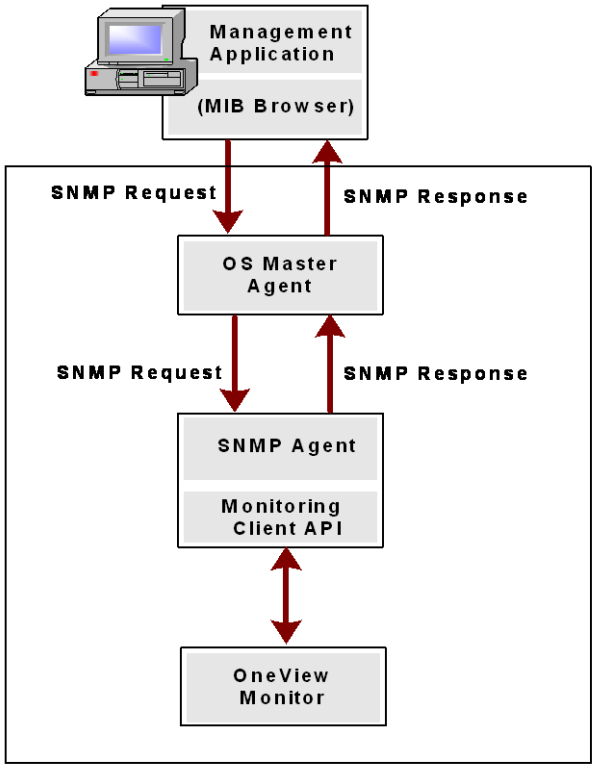
Chapter 8: SNMP Support

This section contains the following topics:

SNMP Support Overview

SNMP support includes a Management Information Base (MIB), an SNMP Agent, and the Event SNMP Trap library. You can configure the SNMP Agent and Event SNMP Trap library independently and enable one or disable the other or vice versa. The SNMP Agent enables monitoring applications to retrieve operational data from the OneView Monitor. The SNMP Agent sends data to the SNMP manager and supports SNMP request handling.

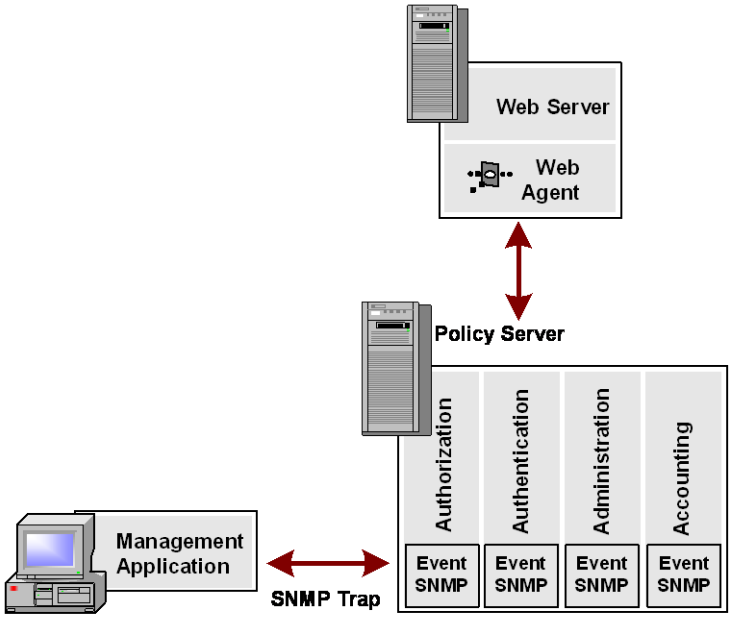
The following figure shows the architecture between the management application, OS Master Agent, SNMP Agent, and the OneView Monitor.



The OS Master Agent, such as the native Solaris SunSolstice Master Agent, invokes the SNMP Agent once you restart the Master Agent. Upon receiving an SNMP request from the management application the OS Master Agent forwards the SNMP request to the SNMP Agent. The SNMP Agent contacts the OneView Monitor, retrieves the required information using Monitor Client API, and then sends the response to the Master Agent. The Master Agent, in turn, forwards the response to the management application.

If you do not configure the SNMP Agent during the Policy Server installation, all the SNMP files are still installed in case you want to use the Agent later. However, to get the Agent running, you need to manually get the Agent started by configuring the SNMP Agent on a Windows or UNIX system.

The Event SNMP Trap library converts some SiteMinder events into SNMP traps before sending them to the management application as noted in the following figure. The trap library captures events sent by the Policy Server, decides if SNMP traps are to be generated on a given event, and generates a trap.



Note: More information on the SNMP Agent and the OneView Monitor exists in the *Policy Server Management Guide*.

Prerequisites for Windows and UNIX Systems

You need to have a Master Agent installed with your operating system before installing or using the SNMP Agent.

Windows Prerequisites

SiteMinder SNMP support on Windows requires the SNMP service. For more information about installing the SNMP service, see the Windows online help system.

UNIX Systems Prerequisites

The following section details UNIX prerequisites for SNMP support:

Solaris

You need the native Solaris SunSolstice Master Agent, which comes with the operating system.

Linux

For the supported Master Agent on Red Hat Advanced Server 3.0, upgrade the net-snmp package to net-snmp-5.1-2.1 or greater.

To upgrade the net-snmp package to net-snmp-5.1-2.1 or greater, use the following setting in net-snmpd instead of-c public -v 1 -p 8001 localhost .1.3.6.1.4.1.2552:

```
proxy -c public -v 1 localhost:8001 .1.3.6.1.4.1.2552
```

Configure the SNMP Agent on Windows

To configure the SNMP agent on Windows

1. Be sure that the NETE_PS_ROOT environment variable is set to the SiteMinder installation directory. The Policy Server installation program should have already done this.
2. Open *siteminder_home*\config\snmp.conf file and edit the last row to contain the full path to *siteminder_home*\log\snmp.log.

   Note: You only need to do this if you did not specify the Policy Server installation program to automatically configure SNMP.

   Correct example: LOG_FILE=C:\Program Files\Netegrity\siteminder\ log\snmp.LOG

   Incorrect example: LOG_FILE=$NETE_PS_ROOT\log\snmp.log
3. Edit the w*indows_dir*/java_service.ini file.

   Note: You only need to do this if you did not specify the Policy Server installation to automatically configure SNMP.

   a. Set SERVICE_BINARY_NAME to the full path name of JavaService.exe.

      Example: SERVICE_BINARY_NAME=c:\winnt\JavaService.exe

   b. Set WORKING_DIR to the full path to directory *siteminder_home*\bin:

      Example: WORKING_DIR=C:\Program files\Netegrity\siteminder\bin

   c. Set JRE_PATH to the full path of javaw.exe.

4. Run *siteminder_home*\bin\thirdparty\proxyreg.exe to change the registry keys for the apadll.dll and snmp.conf:

   `proxyreg.exe full_path_for_apadll.dll full_path_for_snmp.conf`

   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.

   Example: proxyreg.exe "c:\program files\netegrity\siteminder\ bin\ thirdparty\apadll.dll" "c:\programfiles\netegrity\ siteminder\ config\ snmp.conf"

5. Run *WINNT dir*/JavaService.exe with the -install option, to register the Netegrity SNMP agent as a WINNT service.
6. Start the Netegrity SNMP agent by using the Windows Services dialog box.
7. Restart the SNMP service.

How to Configure SNMP Event Trapping on Windows

Configuring SNMP event trapping on Windows requires you to:

1. Enable SNMP event trapping (see page 199).
2. Configure snmptrap.config (see page 200).

Enable SNMP event trapping

To enable SNMP event trapping

1. Launch the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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. Click the Advanced tab.
3. In the Event Handler's field at the bottom, enter the full path to the EventSNMP.dll.
4. Click OK.

After enabling SNMP event trapping, configure the snmptrap.conf file.

More Information:

Configure snmptrap.conf (see page 200)

Configure snmptrap.conf

To configure the SNMP configuration file

1. Edit snmptrap.conf.

   Note: snmptrap.conf is located in *policy_server_home*\config.

   policy_server_home

   Specifies the Policy Server installation location.

2. For the specified trap(s) that you want to receive, uncomment out the appropriate line(s).
3. Specify the IP Address, port number, and community for where you want the trap to be sent.
4. Save the snmptrap.config file with the new changes.
5. Restart the Policy Server.

More Information:

Stop and Restart the Policy Server (see page 202)

Configure the SNMP Agent on UNIX Systems

To configure the SNMP Agent on UNIX systems

1. Ensure the NETE_PS_ROOT environment variable is set to the SiteMinder installation directory. The Policy Server installation program should have already done this.

   Example: /home/smuser/siteminder

2. Edit the file /etc/snmp/conf/RunSubagent.sh:

   a. Set the correct JRE path:
   JAVA_HOME=$INSTALL_HOME/bin/jdk/<required_version>/jre

   b. Set the correct SiteMinder path:

   Example: INSTALL_HOME=/home/smuser/siteminder

   Note: The INSTALL_HOME variable should contain the full path for the SiteMinder installation directory.

3. Restart the SNMP daemon on Solaris
   a. Become root.
   b. Goto /etc/rc3.d.
   c. Execute the S76snmpdx script twice, as follows:

      sh S76snmpdx stop to stop the running Solaris master agent.

      sh S76snmpdx start to start the Solaris master agent and Netegrity subagent.

How to Configure SNMP Event Trapping on UNIX Systems

Configuring SNMP event trapping on UNIX systems requires you to:

1. Enable SNMP event trapping (see page 201).
2. Configure snmptrap.config (see page 201).

Enable SNMP event trapping

To enable SNMP event trapping

1. Launch the Policy Server Management Console.
2. Click the Advanced tab.
3. In the Event Handler's field at the bottom, enter the full path to libeventsnmp.so.

   Example: /home/smuser/siteminder/lib/libeventsnmp.so
4. Click OK.

After enabling SNMP event trapping, configure the snmptrap.config file.

More Information:

Configure snmptrap.config (see page 201)

Configure snmptrap.config

To configure snmptrap.config

1. Edit snmptrap.config, which is located in /home/smuser/siteminder/config.
2. For the specified trap(s) that you want to receive, uncomment out the appropriate line(s).
3. Specify the IP Address, port number, and community for where you want the trap to be sent.
4. Save the snmptrap.config file with the new changes.
5. Restart the Policy Server.

More Information:

Stop and Restart the Policy Server (see page 202)

Stop and Restart the Policy Server

In order for the SNMP configurations changes to take effect, you need to stop and restart the Policy Server using the Status tab of the Policy Server Management Console.

Test SNMP Gets for Red Hat Enterprise Linux Advanced Server

You should test SNMP Gets after configuring SNMP.

To test SNMP Gets

1. Start the native SNMP master agent. On Red Hat AS, the master agent is not started automatically on start up as is the case on Solaris and HP-UX. To start the master agent, go to the /etc/rc1.d directory and run the following command (run as root):

   ```
   K50snmpd start
   ```

2. Start the Netegrity subagent using the following command (run as root):

   ```
   sh /etc/init.d/NetegrityAgent
   ```

3. To stop the Netegrity subagent on Red Hat AS, run the following command as root:

   ```
   sh $NETE_PS_ROOT/etc/snmp/conf/StopSubagent.sh
   ```

Test SNMP Gets for HP-UX

You should test SNMP Gets after configuring SNMP.

To test SNMP Gets

1. Start the Native Agent Adaptor with the script "/sbin/init.d/SnmpNaa" using the following command as root:

   ```
   nohup sh /sbin/init.d/SnmpNaa start
   ```

2. Start the Netegrity subagent with the script "/sbin/init.d/SnmpNetegrity" using the following command (run as root):

   ```
   nohup sh /sbin/init.d/SnmpNetegrity start
   ```

3. To stop the Netegrity subagent on HP-UX, run the following command as root:

   ```
   sh /sbin/init.d/SnmpNetegrity stop
   ```

Appendix A: Troubleshooting

This section contains the following topics:

Working with a SiteMinder License

Symptom:

- I am currently using the Policy Server evaluation license and want to acquire and add a permanent license.
- I have a SiteMinder license, but cannot find it.
- I have a SiteMinder license, but do not know how to update it with a new product key.

Solution:

To request a SiteMinder license

1. Go to the Technical Support site.
2. Click CA Licensing Inquires. This link is located under Address Licensing Needs.

   The CA Customer Care site opens in a new window.
3. Click Licensing Issue Request. This link is located under Contact Us.

   An online request form opens in a new window.
4. Complete the required information and click Submit.

To add a permanent SiteMinder license to a Policy Server

1. Request a SiteMinder license.
2. Access the Policy Server host system.
3. Do one of the following:
   - (Windows) Navigate to *siteminder_home*\license
   - (UNIX) Navigate to *siteminder_home*/license

   siteminder_home

   Specifies the Policy Server installation path.
4. Copy the license.dat file to the license directory.
5. Restart the Policy Server.

To find an existing SiteMinder license

1. Log into the Technical Support site.
2. Click Licensing. Licensing is located on the left side under Support.

   The CA Licensing screen appears.
3. Click View Licenses. View Licenses is located under SiteMinder and Identity Manager Licenses.

   All license details, including the respective key, appear.

To apply a SiteMinder license key to the license file

1. Access the Policy Server host system.
2. Do one of the following:
   - (Windows) Navigate to *siteminder_home*\license
   - (UNIX) Navigate to *siteminder_home*/license

   siteminder_home

   Specifies the Policy Server installation guide.
3. Open the license.dat file.
4. Copy and paste the license key acquired from the Support site into the license file.
5. Save the license file
6. Restart the Policy Server.

Database may be corrupt message

Valid on Windows and UNIX Systems

Symptom:

When I try to migrate policy store data from one LDAP Directory Server or relational database to another, the Policy Server displays a message that the database may be corrupt.

Solution:

When migrating the policy store, you must import the smpolicy.smdif file before importing your exported policy store's data even if you are migrating between the same version of SiteMinder. If you import your old policy store data before importing smpolicy.smdif, SiteMinder may issue the "Database may be corrupt" message. You can fix your corrupted policy store by importing smpolicy.smdif after importing your old policy store data. However, you should import the smpolicy.smdif file first.

More Information:

Migrate an Existing Policy Store into an LDAP Directory (see page 108)
Migrate an Existing Policy Store into a Relational Database (see page 139)

SiteMinder Administration Server Error: Could not log in. (Error 3)

Valid on Windows

Symptom:

I have received the following SiteMinder Administration server error: Could not log in. (Error 3)

Solution:

Reset the SiteMinder super user password for the policy store:

1. Copy the smreg utility (smreg.exe) from the Policy Server installation kit to *siteminder_home*\bin.
2. Execute the following command:

   `smreg -su` *`super_user_password`*

   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.

   super_user_password

   Specifies the password for the SiteMinder super user account.

   Note: Be sure that there is a space between -su and the password.
3. Delete smreg.exe.

   Deleting smreg.exe prevents someone from changing the super user password.

Policy Server User Interface Does Not Appear on Windows

Valid on Windows

Symptom:

I have installed the Policy Server, but it does not appear.

Solution:

If you installed an Internet Information Server (IIS) Web Server on a port other than 80, the Policy Server User Interface may not appear. Editing the Policy Server User Interface shortcut URL should fix the problem.

To edit the shortcut URL.

1. Right-click Start and select Open All Users.
2. Double-click Programs.
3. Double-click SiteMinder.
4. Highlight the Policy Server User Interface icon, right click, and select Properties.
5. Select the Web Document tab.
6. In the URL field on the Web Document tab, change the port number to the one you configured for the IIS Web Server.

   Example: if your IIS Web Server is located on port 81, change:

   http://*<fully qualified domain name>*:80/siteminder/index.htm

   to http://*<fully qualified domain name>*:81/siteminder/index.htm
7. Click Apply and OK.

If you are still have difficulty getting the Policy Server User Interface to display, run the Policy Server User Interface Browser Compatibility Test at the following URL: http://www.netegrity.com/uitest

If the panel is a solid box, click Details for more troubleshooting information.

Unable to proceed. No response from SiteMinder Message

Valid on Windows and UNIX Systems

Symptom:

I have received the "Unable to proceed. No response from SiteMinder" message.

Solution:

Stop and restart the Policy Server using the Policy Server Management Console's Status tab.

Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.

Policy Server Fails to Start After Installation

Valid on Windows and UNIX Systems

Symptom:

I have installed the Policy Server, but it is not starting.

Solution:

You may have the wrong JRE version installed. Make sure you have the correct JRE version.

Note: For a list of supported CA and third-party components, refer to the SiteMinder r6.0 SP6 Platform Support Matrix on the Technical Support site.

AE failed to load library 'smjavaapi'. System error

Valid on Windows and UNIX Systems

Symptom:

During Authorization, I receive the "AE failed to load library 'smjavaapi'. System error: The specified module could not be found." error message.

Solution:

Set the PATH variable to *<SiteMinder_installation>*\config\JVMOptions.txt for Windows or the LD_LIBRARY_PATH to *<SiteMinder_installation>*/config/JVMOptions.txt for UNIX systems.

Locate Logging Messages if Smobjimport Fails During Import

Valid on UNIX Systems

Symptom:

The smobjimport fails when I attempt to import an .smdif file.

Solution:

Read the error and warning message logging information in the *<importfilename>*.log and *<importfilename>*.tmp files.

Missing Icons on the System and Domains tab of the Policy Server UI

Valid on UNIX Systems

Symptom:

The Policy Server user interface is missing icons on the System and Domain tabs.

Solution:

Clear the Web browser cache by deleting all of the temporary internet files.

Cannot Access Online Manuals from Policy Server User Interface

Valid on Windows

Symptom:

I am unable to access the online manuals from the Policy Server user interface

Solution:

If you get the following message using Internet Explorer: “Access to the specified device.path, or file is denied trying to access online manuals from UI”, you may need to install Acrobat Reader from www.adobe.com.

You may also need to manually edit the netegrity_docs Virtual Directory.

More Information:

Manually Create the netegrity_docs Virtual Directory on IIS 6.0 (see page 213)

Adobe Acrobat Reader Won't Install

Valid on Windows

Symptom:

When I try to install Adobe Acrobat, the installation program hangs.

Solution:

If the Acrobat Reader installation program hangs while the Policy Server service is running, stop it using the Policy Server Management Console's Status tab. After stopping the service, the installation program should start.

Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.

Windows/IIS Virtual Path to /siteminderdmonitor Does Not Exist

Valid on Windows

Symptom:

The virtual path to the /siteminderdmonitor does not exist under Default Web Site in the IIS Microsoft Management Console.

Solution:

Create the virtual path.

To create the virtual path

1. From the Start menu, go to: Programs, Administrative Tools, Internet Service Manager.
2. Select Default Web Site.
3. From the Action menu, select New, Virtual Directory.

   The Virtual Directory Wizard opens.
4. Specify the name (alias) of the virtual directory. For example: siteminderdmonitor

   Note: You can specify any name for the alias as siteminderdmonitor is an example

5. Click Next.
6. Specify the path to *<siteminder_installation>*\monitor\.
7. Click Next.
8. Select the Allow Execute Access permission.
9. Click Finish.

Policy Stores with Large Numbers of Objects

Valid on Windows and UNIX Systems

Symptom:

My Policy store has returned the exception java.lang.IndexOutOfBounds to the Policy Server User Interface.

Solution:

Policy Stores with large numbers of objects may return the exception java.lang.IndexOutOfBounds to the Policy Server User Interface.

Define the registry key \HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\ObjectStore \MaxObjects to a value lower than 100 (such as 50).

SSL initialization failed: error -8174 (security library: bad database.)

Valid on Windows and UNIX Systems

Symptom:

When I run smldapsetup ldmod -fpstore -ssl1 -c/app/siteminder/ssl/cert7.db for policy stores that are using an SSL-encrypted connection to Oracle Directory Server (formerly Sun Directory Server Enterprise Edition), I receive the following error message:

"SSL initialization failed: error -8174 (security library: bad database.)"

Solution:

1. Make sure the key3.db file exists in the same directory as cert7.db for the Netscape Web browser.
2. Rerun this smldapsetup command, and, for the -c option, specify the path of the directory where the SSL client certificate database file, cert7.db, exists.

   Example: if cert7.db exists in /app/siteminder/ssl, specify -c/app/siteminder/ssl/cert7.db

More Information:

smldapsetup (see page 158)

Winsock error 10054 message

Valid on Windows

Symptom:

When I try to log into the Policy Server, I receive the "Unable to proceed, winsock error 10054" message.

Solution:

One of the following could be the cause of the problem:

- The policy store does not contain the proper SiteMinder schema. Make sure you imported the correct SiteMinder schema.
- The Policy Server is not running. To start this server, use the Status tab on the Policy Server Management Console.

  Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut 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.
- The Policy Server is not connected to the policy store properly. Using the Data tab on the Policy Server Management Console, click Test Connection to make sure the policy store connects successfully. If it does not, reenter the data source information values on the Data tab by pointing the Policy Server at the policy store.

More Information:

LDAP Directory Servers as a Policy or Key Store (see page 81)
Relational Databases as a Policy or Key Store (see page 111)
Point the Policy Server at the Policy Store (see page 109)

Problem With Using Active Directory as a User Store

Symptom:

When I use Active Directory as a user store, the Policy Server issues error messages that it cannot connect to this store.

Solution:

When creating an Active Directory-based user store, make sure you specify a fully qualified host name (for example, host.domain.com) in the Policy Server User Interface and do not use the machine's IP Address. Moreover, make sure you can ping host.domain.com and domain.com from the machine where the Policy Server is installed since Active Directory sends referrals to the Policy Server that are identified by the fully qualified host name. If the fully qualified host names are invalid and unreachable, the Policy Server issues error messages.

Manually Create the netegrity_docs Virtual Directory on IIS 6.0

Symptom:

I have installed the documentation, but it does not appear in the Policy Server User Interface.

Solution:

If you installed the documentation after the Policy Server and the documentation does not appear in the Policy Server User Interface:

1. Start the Internet Information Services (IIS) Manager.
2. Under Default Web Site, create the netegrity_docs virtual directory and point it to C:\Program Files\Netegrity\netegrity_documents.

   Note: The example lists the absolute path to the default netegrity_documents installation location. If you installed the documentation in a different location, then specify the correct path.

The documentation should now appear from the Policy Server User Interface when you select Help, Online Manuals.

Fix Modified UNIX/Sun Java System Web Server Configuration Files

As mentioned in the procedure for installing the ServletExec/AS on a UNIX/Sun Java System, we advise not allowing ServletExec to modify the Sun Java System Web server's configuration files (obj.conf and magnus.conf). However, if ServletExec did modify these files during installation, the Web server instance fails after you configure the Policy Server User Interface and OneView Monitor GUI using the Policy Server installer/wizard. The ServletExec installer puts entries in these files that conflict with those from the Policy Server.

To keep the Web server instance from failing, remove the conflicting entries from the Sun Java System Web Server instance's obj.conf and magnus.conf files.

1. Open /*<sunjavasystem_home>*/servers/https-*<web_server_instance_name>*.domain.com /config/magnus.conf, and remove the first line:

   ```
   Init fn="ServletExecInit"
   <ServExec_instance_name>.instances="<IP_address>:<portnumber> "
   ```

   ServExec_instance_name

   Specifies the name of your SerlvetExec instance.

   IP_address

   Specifies the IP Address of the machine where ServletExec is installed.

   portnumber

   Specifies the port number for the SerlvetExec instance.

   Note: The Policy Server Configuration Wizard added the correct entry at the end of the file.

2. Open /*<sunjavasystem_home>*/servers/https-*<web_server_instance_name>*.domain.com /config/obj.conf, and remove lines four and five from the top of the file:

   ```
   NameTrans fn="assign-name" from="/servlet/*" name="<ServExec_instance_name>"
   NameTrans fn="assign-name" from="*.jsp*" name="<ServExec_instance_name>"
   ```

   Important! Do not remove the name="se-<ServExec_instance_name>" entries in lines two and three since these were added by the Policy Server Configuration Wizard.

3. In the same obj.conf file, remove the second to the last <Object *name="<ServExec_instance_name>*"> section from the end of the file:

   ```
   <Object name="<ServExec_instance_name>">
   Service fn="ServletExecService" group="<ServExec_instance_name>"
   </Object>
   ```

Important! Do not remove the <Object name="se-<ServExec_instance_name>"> entry since this one was added by the Policy Server Configuration Wizard.

4. After saving these files, you should be able to start the Web server instance from the Sun Java System Web Server Administration Server page.

NETE_PS_ALT_CONF_FILE Environment Variable on Solaris

After installing the Policy Server on Solaris, the nete_ps_env.ksh script may have the following entry:

```
export NETE_PS_ALT_CONF_FILE=/export/siteminder/config/.siteminder.conf
```

The NETE_PS_ALT_CONF_FILE environment variable is used by the stop-all and start-all scripts, which stop and start the Policy Server's service. The .siteminder.conf file is a temporary, run-time file created by these scripts and has no affect your SiteMinder configuration.

Do not modify the NETE_PS_ALT_CONF_FILE environment variable.

Manually Configure the OneView Monitor GUI on UNIX/Sun Java System 6.0

If you do not configure the OneView Monitor GUI using the Policy Server Configuration Wizard, you can configure it manually by modifying the following Sun Java System web server and ServletExec files:

- obj.conf
- magnus.conf
- StartServletExec

The Policy Server Configuration Wizard performs the following procedure automatically so these steps are provided as a reference to help you troubleshoot OneView Monitor GUI issues.

1. Open /usr/local/NewAtlanta/ServletExecAs/se-*instance_name*/StartServletExec in a text editor.

   instance_name

   Specifies the name of the ServletExec instance.

2. Do the following:

   a. Find the PORT=8888 entry.

      Example:

      THISHOST="testmachine"

      PORT=8888

      SEINSTANCE="testmachine-servexecinstance"

   b. Change the port of communication with web server to any free port.

      Example: PORT=7777

   c. Extend the CLASSPATH definition by adding the entries in boldface to the end of the CLASSPATH:

      ```
      CLASSPATH=${NA_LIB}/servlet-api.jar:${NA_LIB}/jsp-
      api.jar:${NA_LIB}/ServletExec60.jar:${NA_LIB}/ServletExecAdmin.jar:${NA_L
      IB}/el-
      api.jar:${NA_LIB}/jasper-el.jar:${JL}/tools.jar:${NA_LIB}/jstl.jar:${NA_L
      IB}/appserv-
      jstl.jar:${NA_LIB}/activation.jar:${NA_LIB}/mail.jar:${HOMEDIRPATH}/class
      es:siteminder_home
      /monitor/smmongui.jar:siteminder_home/lib/smconapi.jar:siteminder_home/li
      b
      /smmonclientapi.jar
      ```

      siteminder_home

      Specifies the Policy Server installation path.

   d. Extend the document directories definition by adding the entries in boldface to:

      $SENAME $HOMEDIR $MIMEFILE $DOCROOTDIR-port $PORT $SEOPTS **-addl "/sitemindermonitor=***siteminder_home***/monitor""**

      siteminder_home

      Specifies the Policy Server installation path

      Note: There are two quotes at the end of the entry above.

3. For Sun Java System 6.0, open */sun_java_system_home/* https-*instance_name*/config/magnus.conf.

   sun_java_system_home

   Specifies the Sun Java System installation path.

   instance_name

   Specifies the name of the Sun Java System instance.

4. Move the Init fn="load-modules" section to the end of the file between the following new Init fn="init-cgi" and Init fn="ServletExecInit" sections:

   ```
   Init fn="init-cgi" SM_ADM_UDP_PORT="44444" SM_ADM_TCP_PORT="44444"
   Init fn="load-modules" shlib="ServletExec_home/bin/ServletExec_Adapter.so"
   funcs="ServletExecInit,
   ServletExecFilter,ServletExecService"
   Init fn="ServletExecInit"
   configFile="ServletExec_home/config/webadapter.properties"
   ```

   ServletExec_home

   Specifies the ServletExec installation path.

   Example: /export/NewAtlanta/ServletExecAS

5. Open */sun_java_system_home*/https-*instance_name*/config/obj.conf and do the following:

   a. Add the following lines, in this order, under <Object name="default">:

   ```
   <Object name="default">
   NameTrans fn="assign-name" from="*.jsp*" name="instance_name"
   NameTrans fn="assign-name" from="/servlet/*" name="instance_name"
   NameTrans fn="pfx2dir" from="/siteminder monitor"
   dir="siteminder_home/monitor"
   ```

   instance_name

   Specifies the name of the SerlvetExec instance.

   siteminder_home

   Specifies the Policy Server installation path.

   Important! The last entry must be after the other two to ensure proper configuration of the OneView Monitor GUI.

   b. Add the following to the end of the file:

   <Object name="*instance_name*">

   Service fn="ServletExecService" group="*instance_name*"

   </Object>

instance_name

Specifies the name of the SerlvetExec instance.

6. Restart the web server and ServletExec.

Set JRE in PATH Variable Before Uninstalling Any SiteMinder Component

Symptom:

When I attempt to uninstall the Policy Server, Web Agent, Policy Server Option Pack, Web Agent Option Pack, SDK, or SAML Affiliate Agent, the uninstallation program stops and issues one of the following error messages:

- “Could not find a valid Java virtual machine to load. You need to reinstall a supported Java virtual machine.”
- "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program."

Solution:

Make sure the JRE is in the PATH variable.

Set the JRE in the PATH Variable on Windows

To Set the JRE in the PATH variable

1. Go to the Control Panel.
2. Double-click System.
3. In the Environment Variables dialog, add the location of the JRE to the Path system variable.

Set the JRE in the PATH Variable on Solaris

To set the JRE in the PATH variable

Run the following commands:

1. PATH=$PATH:<JRE>/bin

   JRE

   Specifies the location of your JRE.

2. export PATH

ODBC Policy Store Import Fails with UserDirectory Error

Symptom:

I receive an error message stating that the policy store failed operation "save" for object type "UserDirectory" when importing policy store data into an ODBC policy store.

Solution:

It is possible that the server name in the ODBC store's userDirectory object is longer than 512 characters, which by default, exceeds the limit allowed by the MS SQL Server and Oracle policy store schema scripts that are shipped with SiteMinder.

Do one of the following:

If you are trying to import policy data into a supported version of a MS SQL Server policy store:

1. Open sm_mssql_ps.sql.

   Note: This schema script is located in *policy_server_home*\db\SQL.

2. Search for the following text:

   CREATE TABLE smuserdirectory5

3. Modify "server smstringreq512N," to one of the following depending on your needs:

   - server smstringreq1024,N
   - server smstringreq4000,N

4. Re-import the policy store schema into the policy store.
5. Import the policy store data.

If you are trying to import policy data into a supported version of an Oracle policy store:

1. Open sm_oracle_ps.sql.

   Note: This schema script is located in *policy_server_home*\db\SQL.

2. Search for the following text:

   CREATE TABLE smuserdirectory5

3. Modify "server VARCHAR2(512) NOT NULL," to one of the following depending on your needs:

   - server VARCHAR2(1024) NOT NULL,
   - server VARCHAR2(4000) NOT NULL,

4. Re-import the policy store schema into the policy store.
5. Import the policy store data.

Appendix B: Unattended Installation

This section contains the following topics:

Unattended Installation

Once you have installed the Policy Server, you can reinstall it on the same machine or install it on a separate machine using an unattended installation mode. In this mode, the installer installs or uninstalls the Policy Server without any end-user interaction.

This chapter describes how to modify the Policy Server's installation configuration file to:

- Enable an unattended Policy Server installation
- Pre–define installation variables
- Store encrypted or plain text passwords

Modify the Installer Configuration File

To enable an unattended Policy Server installation, you must modify the settings in the nete-ps-installer.properties configuration file using a text editor. The default parameters in the file reflect the information you entered during the initial Policy Server installation. Change the default values to best suit your environment. Before modifying this file, back up the original for safekeeping.

The file is located in the following location:

*siteminder_home/*install_config_info

siteminder_home

Specifies the Policy Server installation path.

The following is an example of the nete-ps-installer.properties file created during the initial Policy Server installation.

```
### General Information
DEFAULT_INSTALL_DIR=$NETE_PS_ROOT$
DEFAULT_SHORTCUTS_DIR=$USER_SHORTCUTS$
DEFAULT_JRE_ROOT=$NETE_JRE_ROOT$
DEFAULT_BROWSER=$NETE_PS_BROWSER$
DEFAULT_SMPROFILE_CHOICE=$SMPROFILE_CHOICE$
# DEFAULT_ENCRYPTKEY=<To define Encryption Key, insert string here and uncomment
line.>
ENCRYPTED_ENCRYPTKEY=$ENCRYPTED_ENCRYPTKEY$

### Feature Selection
DEFAULT_OVMGUI_CHOICE=$OVMGUI_CHOICE$
DEFAULT_WEBSERVERS_CHOICE=$WEBSERVERS_CHOICE$
DEFAULT_SNMP_CHOICE=$SNMP_CHOICE$
DEFAULT_POLICYSTORE_CHOICE=$POLICYSTORE_CHOICE$

### OneView Monitor GUI
DEFAULT_JDK_ROOT=$NEW_NETE_JDK_ROOT$
DEFAULT_SERVLETEXEC_INSTANCE_NAME=$SERVLETEXEC_INSTANCE_NAME$
DEFAULT_SERVLETEXEC_ROOT=$SERVLETEXEC_ROOT$
DEFAULT_SERVLETEXEC_PORT=$SERVLETEXEC_PORT$

### Web Server(s)
# This is a list of web server instance information.
# Format:
instance_name_1,type_1,root_folder_1;instance_name_2,type_2,root_folder_2; etc...
# Valid Types:  iPlanet, IIS
# Example: To configure IIS and 2 iPlanet instances, called https-A and https-B, installed
under C:\server :
# DEFAULT_WEBSERVER_INFO=,IIS,;https-A,iPlanet,C:\server;https-B,iPlanet,C:\server
DEFAULT_WEBSERVER_INFO=$WEB_SERVER_INFO$
DEFAULT_IPLANET_WEBSERVER_ROOT=$IPLANET_WEBSERVER_ROOT$

### SNMP

# DEFAULT_ROOT_PW=<To define root password, insert string here and uncomment
line.>
ENCRYPTED_ROOT_PW=$ENCRYPTED_ROOT_PW$
```

```
### Policy Store
DEFAULT_POLICYSTORE_TYPE=$LDAP_TYPE$
DEFAULT_POLICYSTORE_IP=$LDAP_IP$
DEFAULT_POLICYSTORE_PORT=$LDAP_PORT$
DEFAULT_POLICYSTORE_ADMINDN=$LDAP_ADMINDN$
# DEFAULT_POLICYSTORE_ADMINPW=<To define LDAP Admin password, insert string
here and uncomment line.>
ENCRYPTED_POLICYSTORE_ADMINPW=$ENCRYPTED_LDAP_ADMINPW$
DEFAULT_POLICYSTORE_ROOTDN=$LDAP_ROOTDN$
DEFAULT_POLICYSTORE_USER_CHOICE=$LDAP_USER_CHOICE$
DEFAULT_POLICYSTORE_USERDN=$LDAP_USERDN$
# DEFAULT_POLICYSTORE_USERPW=<To define LDAP user password, insert string here
and uncomment line.>
ENCRYPTED_POLICYSTORE_USERPW=$ENCRYPTED_LDAP_USERPW$
DEFAULT_INIT_LDAP_CHOICE=$INIT_LDAP_CHOICE$
# DEFAULT_SM_ADMINPW=<To define LDAP SiteMinder Super User password, insert
string here and uncomment line.>
ENCRYPTED_SM_ADMINPW=$ENCRYPTED_SM_ADMINPW$
```

Guidelines for Modifying the Configuration File

Follow these guidelines when editing a configuration file:

- Do not add extra spaces between the parameter name, the equals sign (=), and the attribute value.
- Save the file after you make changes.
- Do not manually edit any encrypted passwords in this file since they are encrypted for security reasons and cannot be edited in plain text. If you want to add plain text passwords, comment out the encrypted password parameter and uncomment the plain text reference.
- Make a back up the of the nete-ps-installer.properties file before modifying the original since the file holds all of the values you entered during the initial Policy Server installation.

Note: The sections in this chapter follow the order of the parameters in the configuration file.

Configure Installation for Unattended Mode

To run the installer in unattended mode

1. Modify the nete-ps-installer.properties file with the settings you want, as noted in the following sections:
   - Configure General Policy Server Information (see page 225)
   - Configure Policy Server Features (see page 226)
   - Configure OneView Monitor GUI (see page 226)
   - Configure the Web Server (see page 227)
   - SNMP Password (see page 227)
   - Configure the LDAP Policy Store (see page 228)
2. From a Policy Server host system, copy the nete-ps-6.0-sp6-*os*.bin and nete-ps-installer.properties files to a temporary location on the system to which you are installing or reinstalling the Policy Server.

   os

   Specifies win32, sol, rhel30, or hp.

   Note: If you are installing to UNIX, be sure that the user who is to run the installation has the appropriate permissions to install from this directory.
3. From the temporary directory, run one of the following:
   - (Windows) nete-ps-6.0-sp6-win32.exe -f nete-ps-installer.properties -i silent
   - (UNIX) ./nete-ps-6.0-sp6-*os*.bin -f nete-ps-installer.properties -i silent

   os

   Specifies sol, rhel30, or hp.

   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.

Configure General Policy Server Information

The General Information section allows you to set the following:

DEFAULT_INSTALL_DIR

Specifies the location of the Policy Server installation.

DEFAULT_SHORTCUTS_DIR

Specifies the location of the SiteMinder program icon.

Example: C:\\Documents and Settings\\All Users\\Start or /SiteMinder

Note: The icon feature only works on Windows.

DEFAULT_JRE_ROOT

Specifies the JRE installation location.

DEFAULT_BROWSER

(UNIX only) Specifies the installation location of the browser.

DEFAULT_SMPROFILE_CHOICE

(UNIX only) Specifies if smprofile.ksh should be added to the .profile file. Specify **true** for yes; specify **false** for no.

DEFAULT_ENCRYPTKEY

Allows you to enter a cleartext encryption key, which secures data sent between the Policy Server and the policy store.

Note: If you comment out the ENCRYPTED_ENCRYPTKEY parameter and uncomment DEFAULT_ENCRYPTKEY, then the unattended installer uses the cleartext encrypt key value from DEFAULT_ENCRYPTKEY. The DEFAULT_ENCRYPTKEY parameter is commented out by default after the initial Policy Server installation.

ENCRYPTED_ENCRYPTKEY

Shows the encrypted encryption key, which secures data sent between the Policy Server and the policy store. You entered this key during the initial Policy Server installation and cannot change it.

Important! Do not modify this encrypted value since any change will break the communication between the Policy Server and policy store when you run an unattended installation.

If you comment out the DEFAULT_ENCRYPTKEY parameter and uncomment ENCRYPTED_ENCRYPTKEY, then the unattended installer uses the encrypted encryption key value from ENCRYPTED_ENCRYPTKEY.

Configure Policy Server Features

The Feature Selection section lets you set the following:

DEFAULT_OVMGUI_CHOICE

If you want the installer to configure the OneView Monitor GUI on the web server automatically, set this value to **true**. Otherwise, set this value to **false**.

DEFAULT_WEBSERVERS_CHOICE

If you want the installer to configure the Policy Server User Interface, documentation, SiteMinder CGI scripts, and OneView Monitor on the web server automatically, set this value to **true**. Otherwise, set this value to **false**.

DEFAULT_SNMP_CHOICE

If you want the installer to configure SNMP support with the Policy Server, then set this value to **true**. Otherwise, set this value to **false**.

DEFAULT_POLICYSTORE_CHOICE

If you want the installer to configure the policy store automatically, then set this value to **true**. Otherwise, set this value to **false**.

OneView Monitor GUI

If you set the DEFAULT_OVMGUI_CHOICE parameter to true, then set the following:

DEFAULT_JDK_ROOT

Specifies the JDK installation location.

DEFAULT_SERVLETEXEC_INSTANCE_NAME

(UNIX only) Specifies the name of the ServletExec instance.

Example: se-testmachine-60psGUI

DEFAULT_SERVLETEXEC_ROOT

Specifies the ServletExec installation location.

Example: C:\\Program Files\\New Atlanta\\ServletExec ISAPI or /export/NewAtlanta/ServletExecAS

DEFAULT_SERVLETEXEC_PORT

(UNIX only) Specifies the port number of the ServletExec instance.

Example: 7676

Configure the Web Server

If you set the DEFAULT_WEBSERVERS_CHOICE parameter to **true** in when configuring Policy Server features to have the installation configure the Web server, then set the following:

DEFAULT_WEBSERVER_INFO

(IIS) Specify *<type>* ,*<root_folder>*.

type

Type is Microsoft IIS**.**

root_folder

Root folder is the <siteminder_installation>\bin\IIS folder.

(Sun Java System) Specify *<instance_name>*, *<instance_config_folder>.*

instance_name

Specifies the Sun Java System instance name.

instance_config_folder

Specifies the Sun Java System location of the instance's configuration file directory.

Example:
https-instance1,/*<sunjavasystem_home>*/servers/https-instance1/config;https-instance2,/*<sunjavasystem_home>*/servers/https-instance1/config

Note: Use a semicolon (;) to separate multiple instances, as shown in the example.

DEFAULT_IPLANET_WEBSERVER_ROOT

(Sun Java System) Specifies the root Sun Java System installation location.

Note: This parameter does not apply to IIS.

SNMP

If you want to modify the SNMP password, do the following:

DEFAULT_ROOT_PW

Allows you to enter a cleartext SNMP password for the UNIX system's root user. If you comment out the ENCRYPTED_ROOT_PW parameter and uncomment DEFAULT_ROOT_PW, then the unattended installer uses the cleartext SNMP password from DEFAULT_ROOT_PW.

Default: The DEFAULT_ROOT_PW parameter is commented out after the initial Policy Server installation.

ENCRYPTED_ROOT_PW

Shows the encrypted SNMP password for the UNIX system's root user. You entered this password during the initial UNIX Policy Server installation and cannot change it.

Important! Do not modify this encrypted password since any change will break the communication between the Policy Server and the SNMP Agent. If you comment out the DEFAULT_ROOT_PW parameter and uncomment ENCRYPTED_ROOT_PW, then the unattended installer uses the encrypted password from ENCRYPTED_ROOT_PW.

Configure the LDAP Policy Store

You set the DEFAULT_POLICYSTORE_CHOICE parameter to **true** when configuring Policy Server features to have the installation configure the LDAP policy store, then set the following:

DEFAULT_POLICYSTORE_TYPE

Specifies the type of LDAP Directory Server for the policy store.

DEFAULT_POLICYSTORE_IP

Specifies the IP Address (or host name) of the machine where the LDAP Directory Server resides.

Example: 172.26.4.238.

DEFAULT_POLICYSTORE_PORT

Specifies the port number for the LDAP instance that you are configuring as a policy store.

Example: 1356.

DEFAULT_POLICYSTORE_ADMINDN

Specify the LDAP Directory Server's administrator user name.

Example: cn=Directory Manager.

DEFAULT_POLICYSTORE_ADMINPW

Allows you to enter a cleartext password for the LDAP Directory Server's administrator. If you comment out the ENCRYPTED_LDAP_ADMINPW parameter and uncomment DEFAULT_LDAP_ADMINPW, then the unattended installer uses the cleartext password from DEFAULT_LDAP_ADMINPW.

Default: The DEFAULT_LDAP_ADMINPW parameter is commented out after the initial Policy Server installation.

ENCRYPTED_POLICYSTORE_ADMINPW

Shows the encrypted password for the LDAP Directory Server's administrator. You entered this password during the initial Policy Server installation and cannot change it.

Important! Do not modify this password since it is encrypted.If you comment out the DEFAULT_LDAP_ADMINPW parameter and uncomment ENCRYPTED_LDAP_ADMINPW, then the unattended installer uses the encrypted password from ENCRYPTED_LDAP_ADMINPW.

DEFAULT_POLICYSTORE_ROOTDN

Specifies the root DN.

Example: o=test.com.

DEFAULT_POLICYSTORE_USER_CHOICE

If you want to specify a different LDAP user account to update SiteMinder data, then set this value to **true**. Otherwise, enter **false**.

DEFAULT_POLICYSTORE_USERDN

Specifies the DN for the different LDAP user.

Example: uid=SMAdmin, ou=people, o=security.com.

DEFAULT_POLICYSTORE_USERPW

Allows you to enter a cleartext password for the different LDAP user. If you comment out the ENCRYPTED_LDAP_USERPW parameter and uncomment DEFAULT_LDAP_USERPW, then the unattended installer uses the cleartext password from DEFAULT_LDAP_USERPW.

Default: The DEFAULT_LDAP_USERPW parameter is commented out after the initial Policy Server installation.

ENCRYPTED_POLICYSTORE_USERPW

Shows the encrypted password for the different LDAP user. You entered this password during the initial Policy Server installation and cannot change it.

Important! Do not modify this password since it is encrypted.

If you comment out the DEFAULT_LDAP_USERPW parameter and uncomment ENCRYPTED_LDAP_USERPW, then the unattended installer uses the encrypted password from ENCRYPTED_LDAP_USERPW.

DEFAULT_INIT_POLICYSTORE_CHOICE

If you are initializing a new LDAP instance, then set this value to **true**. Otherwise, enter **false**.

DEFAULT_SM_ADMINPW

Allows you to enter a cleartext password for the SiteMinder Super User. If you comment out the ENCRYPTED_SM_ADMINPW parameter and uncomment DEFAULT_SM_ADMINPW, then the unattended installer uses the cleartext password from DEFAULT_SM_ADMINPW.

Default: The DEFAULT_SM_ADMINPW parameter is commented out after the initial Policy Server installation.

ENCRYPTED_SM_ADMINPW

Shows the encrypted password for the SiteMinder Super User. You entered this password during the initial Policy Server installation and cannot change it.

Important! Do not modify this password since it is encrypted.

If you comment out the DEFAULT_SM_ADMINPW parameter and uncomment ENCRYPTED_SM_ADMINPW, then the unattended installer uses the encrypted password from ENCRYPTED_SM_ADMINPW.

Appendix C: Configuring the Policy Server for an International Environment

This section contains the following topics:

Policy Servers in an International Environment

The Policy Server supports SiteMinder data stores residing in an Oracle or SQL Server database, and LDAP servers for an international environment.

Important Planning Considerations Before Installing the Policy Server

Consider the following before installing the Policy Server:

- Use supported operating system and third-party software

  For a list of supported operating systems, Web Servers, databases, Web browsers, LDAP Directory Servers, and servlet engines, go to the Technical Support site and search for the SiteMinder Platform Matrix for 6.0. This matrix lists the Policy Server components supported on a Japanese operating system.

- Create supported databases

  Before creating databases for storing policy, user, or session data, make sure they are formatted with UTF-8 encoding.

- Understand which Policy Server User Interface fields that support multi-byte characters in an internationalized environment
- Understand which Policy Server components support multi-byte and ASCII characters in an internationalized environment

Policy Server User Interface Fields Supporting Multi-byte Characters

The following dialog box fields from the Policy Server User Interface support multi-byte characters in an internationalized environment:

Field Name	Dialog Where Field is Located	Access Dialog By Selecting:
All Description fields	All dialogs	Any dialog that has a Description field
All Name fields except dialogs listed in next column	All dialogs except Name fields in: ■ SiteMinder Agent Dialog ■ SiteMinder Agent Group Dialog ■ SiteMinder Agent Configuration Object Dialog ■ SiteMinder Host Configuration Object Dialog ■ SiteMinder Agent Type Dialog	Access Dialog by selecting: ■ Edit, Create Agent ■ Edit, System Configuration, Create Agent Group ■ Edit, System Configuration, Create Agent Conf Object ■ Edit, System Configuration, Create Host Conf Object ■ Edit, System Configuration, Create Type
DN field under the User Session Caches group	SiteMinder Cache Management Dialog	Tools, Manage Cache
Value and Enter Single Value fields	SiteMinder Host Configuration Object's Edit Parameter Dialog	Edit, System Configuration, Create Host Conf Object, click Add
Root, Start, and End fields for the LDAP and AD namespaces	SiteMinder User Directory Dialog	Edit, System Configuration, Create User Directory
Username field	SiteMinder User Directory Dialog's Credentials and Collection tab	Edit, System Configuration, Create User Directory
Filter (binoculars) fields	SiteMinder Policy Domain Dialog	Edit, System Configuration, Create Domain
Manual Entry field in the Condition group Value field in the Infix Notation group	SiteMinder Password Policy Dialog's SiteMinder User Lookup screen	Edit, System Configuration, Create Password Policy
Function Parameter field of the SiteMinder Active Rule editor dialog	SiteMinder Rule and SiteMinder Global Rule dialogs	Click a realm and select Create Rule Under Realm

■ Variable Value field in the Static option. ■ DN Spec field in the DN Attribute option. ■ Parameters field in Active Response option.	SiteMinder Response and Global Response dialogs	Click a response and select Create Response
■ On the Users tab, the Manual Entry field in Condition group and the Value field in Infix Notation group. ■ On the Rules tab, the Filter fields (binoculars) of the Set Response and Set Global Response dialogs. ■ On the Advanced tab, the Function Parameter field in Active Policy group.	SiteMinder Policies and Global Policies dialogs	Click Policies and select Policy
■ Value field in Attribute-Value option. ■ Search Expression field in the LDAP Query option.	SiteMinder User Lookup screen	In multiple dialogs

Policy Server Components Supporting Multi-byte Characters

The following Policy Server components support multi-byte and ASCII characters in an internationalized environment:

- Policy Server User Interface
- Policy Server Management Console
- HTML Forms authentication schemes
- Password Services

  Note: Passwords are limited to ASCII characters only.
- Responses
- Post Preservation
- SiteMinder Test Tool

- Audit logging to text files

  Note: Audit logging multi-byte character information to a database is not supported even if you created the database for UTF-8 character encoding.
- smobjexport and smobjimport
- DMS Self Registration
- Java Agent API

Configure SiteMinder Data Stores Supporting International Characters

You can configure SiteMinder data stores in SQL Server or Oracle databases. When configuring these data stores, be aware that the Policy Server only supports UTF-8 encoding and, as a result, you must use databases that support this encoding type.

Note: This section applies to configuring SiteMinder data stores in relational databases. More information on configuring these stores in LDAP servers exists in LDAP Directory Servers as a Policy Store or Key Store.

Configure an International SiteMinder Data Store in SQL Server

To create policy, keys, session, or key stores, configure a SiteMinder data store in the SQL Server database.

Note: By default, SQL Server supports UTF-8 character encoding.

More Information:

How to Configure a SiteMinder Data Store in a SQL Server Database (see page 113)

Configure an International SiteMinder Data Store in Oracle

To configure an international SiteMinder data store in Oracle

1. On the machine where Oracle is installed, create a custom Oracle database that supports UTF-8 character encoding.

   Note: For more information and instructions, see Oracle's documentation.

   To verify if an existing Oracle database supports UTF-8 character encoding, run the following query:

   Select * from nls_database_parameters where parameter = 'NLS_CHARACTERSET'

2. Create policy, keys, session, or key stores for the Policy Server, by configuring a SiteMinder data store in the Oracle database.

More Information:

How to Configure a SiteMinder Data Store in an Oracle Database (see page 119)

Solaris/LINUX Red Hat Policy Server Logging UTF-8 Characters to an Oracle Database

A Solaris/LINUX Red Hat Policy Server can log UTF-8 characters to an Oracle audit log database. To enable this configuration, you need to set the following environment variables:

For a simplified Chinese operating system

- LANG=zh_CN.utf8

For a Japanese operating system

- LANG=jp_JP.UTF-8

You set the LANG variable system-wide or just for the Policy server process.

Note: To avoid impacting any other applications, make sure that you set this variable for the Policy Server process only.

Database Driver Variable

- IANAAppCodePage=utf-8

You set this variable in the appropriate data source definition section of the system_odbc.ini file, installed in *<policy_server_installation>*/db.

Oracle Client Settings

Since the Policy Server uses the Oracle wire protocol driver, an Oracle client is not necessary. However, if you need an Oracle SQLPLUS client in your environment to read data from the audit log database, you may have to set one or both of the following environment variables to correctly display the multi-bytes characters:

For a simplified Chinese operating system

- LANG=zh_CN.utf8

For a Japanese operating system

- LANG=jp_JP.UTF-8

For the Oracle SQLPlus Client

- NLS_LANG (For example, NLS_LANG=Japanese_Japan.UTF8)

Note: For more information, see the operating system and database client configuration manual.

Configure a Japanese User Store in SQL Server

Using the smsampleusers_sqlserver.sql file installed with the Policy Server, you can configure a user store in a SQL Server database. This file is installed in the <*siteminder_installation*>\db\SQL directory.

To configure a Japanese user store in SQL Server

1. Edit the smsampleusers_sqlserver.sql file, by doing the following:
   a. Replace every varchar instance with **nvarchar**.
   b. Place an **N** before any insert statement with international strings.

      Japanese example:

      insert into SmUser (UserID , Name, Password,
      LastName, FirstName, ...)

      values (12, **N**' やまもと ',
      'siteminder','guest','guest','guest@mycompany.com...)
2. Import the smsampleusers_sqlserver.sql file.

   Note: More information on importing the smsampleusers_sqlserver.sql file exists in How to Configure a SiteMinder Data Store in a SQL Server Database (see page 113).

3. Open the Policy Server User Interface's SiteMinder ODBC Query Scheme dialog and modify the policy store's SQL query scheme by placing an **N** before every %s reference in any = %s statement.

   Example: the following sample query scheme statements:

   select Name, 'User' from SmUser where Name = '%s' Union select Name, 'Group' from SmGroup where Name = '%s'

   should become:

   select Name, 'User' from SmUser where Name = **N**'%s' Union select Name, 'Group' from SmGroup where Name = **N**'%s'

4. Stop and restart the Policy Server.

   The user store configuration is complete and now supports multi-byte characters.

Configure a Japanese User Store in Oracle

Using the smsampleusers_oracle.sql file installed with the Policy Server, you can configure a user store in an Oracle database. This file is installed in the <*siteminder_installation*>\db\SQL directory.

To configure a Japanese user store in Oracle

1. Create a database for the user data that supports Oracle's UTF-8 NLS_CHARACTERSET encoding.
2. Using Oracle's SQL-Plus, import the smsampleusers_oracle.sql file.

   Note: More information on importing the smssampleusers_oracle.sql file exists in How to Configure a SiteMinder Data Store in an Oracle Database (see page 119). Be aware that if you are inserting Japanese characters, import the file from a Japanese operating system.

   The user store configuration is complete.

Appendix D: Modified Environment Variables

This section contains the following topics:

Modified Windows Environment Variables

The Policy Server installation adds and modifies the following environment variables in a Windows environment:

- NETE_PS_ROOT = $INSTALL_PATH$
- NETE_PS_PATH = $INSTALL_PATH$$/$bin; $INSTALL_PATH$$/bin/$thirdparty;$INSTALL_PATH$$/$lib
- NETEGRITY_LICENSE_FILE = %NETE_PS_ROOT%$/$license$/$license.dat
- NETE_JVM_OPTION_FILE = %NETE_PS_ROOT%$/$config$/$JVMOptions.txt
- NETE_DOC_ROOT=$INSTALL_PATH$$/$netegrity_documents
- NETE_JRE_ROOT = HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Runtime Environment\1.6 in JAVAHOME value
- NETE_JDK_ROOT = HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Development Kit\1.6 in JAVAHOME value
- NETE_SHORTCUTS = C:\Documents and Settings\All Users\Start Menu\Programs\SiteMinder

  Note: This is the default location.

Modified UNIX Environment Variables

The Policy Server installation adds and modifies the following environment variables in a UNIX environment:

- NETE_PS_ROOT = $INSTALL_PATH$
- NETE_PS_PATH = $INSTALL_PATH$$/$bin; $INSTALL_PATH$$/bin/$thirdparty;$INSTALL_PATH$$/$lib
- NETEGRITY_LICENSE_FILE = %NETE_PS_ROOT%$/$license$/$license.dat
- NETE_JVM_OPTION_FILE = %NETE_PS_ROOT%$/$config$/$JVMOptions.txt
- NETE_DOC_ROOT=$INSTALL_PATH$$/$netegrity_documents
- NETE_JDK_ROOT = JDK_PATH
- NETE_JRE_ROOT = JRE_PATH

Index

A

B

C

D

E

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W