CA SiteMinder®

Directory Configuration Guide

r12.0 SP3

Fourth Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA SiteMinder®
- CA SiteMinder® Federation Security Services

Contact CA Technologies

Contact CA Support

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

- 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

Providing Feedback About Product Documentation

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

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: About this Guide

This section contains the following topics:

Directory Configuration Overview

The *Directory Configuration Guide* documents the configuration of the following directory servers and relational databases as user or policy stores:

- Critical Path inJoin Directory Server v4.2
- IBM DB2 Database
- IBM Directory Server
- MySQL Server
- Novell eDirectory
- Oracle Internet Directory Server
- OpenLDAP Server
- Red Hat Directory Server 7.1
- Siemens DirX 6.0 D00 Directory Server
- Siemens DirX EE 2.0 Directory Server

For information about other supported directory servers and relational databases, such as Microsoft ADAM and Sun Java System, see the following guides:

- *Policy Server Configuration Guide*
- *Policy Server Installation Guide*
- *Upgrade Guide*

Chapter 2: Critical Path inJoin Directory Server

This section contains the following topics:

Point the Policy Server to the Policy Store

You point the Policy Server to the policy store so the Policy Server can access the policy store.

Follow these steps:

1. Open the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut with Administrator permissions. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the Data tab.

3. Select the following value from the Database list:

   `Policy Store`

4. Select the following value from the Storage list:

   LDAP

5. Configure the following settings in the LDAP Policy Store group box.

   - LDAP IP Address
   - Admin Username
   - Password

- Confirm Password
- DN

Note: You can click Help for a description of fields, controls, and their respective requirements.

6. Click Apply.
7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.
8. Select the following value from the Database list:

   `Key Store`
9. Select the following value from the Storage list:

   LDAP
10. Select the following option:

    `Use Policy Store database`
11. Click OK.

Configure an inJoin Directory Server as a Policy Store

You can configure a Critical Path inJoin Directory Server (IDS) as a policy store using the Critical Path's iCon GUI.

Follow these steps:

1. Start the DSA.
2. Log in to the Policy Server host system.
3. Navigate to *siteminder_home*\bin.

   siteminder_home

   Specifies the Policy Server installation path.
4. Run the following command:

   `ldapmodify -h`*`host`* `-p`*`port`* `-d`*`AdminDN`* `-w`*`AdminPW`* `-c -f`*`siteminder_home`*`\db\tier2\CriticalPathIDS\IDS_Add_Schema_R12sp3.ldif`

   -h*host*

   Specifies the IP address of the LDAP server.

   -p*port*

   Specifies the port number of the LDAP server.

-d*AdminDN*

Specifies the name of an LDAP user with privileges to create a new LDAP schema on the LDAP directory server.

Example: cn=manager

-w*AdminPW*

Specifies the password of the LDAP user with privileges to create a new LDAP schema on the LDAP directory server.

-c

Specifies continuous mode (do not stop on errors).

-f*siteminder_home*

Specifies the Policy Server installation path.

5. Reload the schema, or verify that the schema has been updated.
6. Run the following command:

   `ldapmodify -h`*`host`* `-p`*`port`* `-d`*`AdminDN`* `-w`*`AdminPW`* `-c -f`*`siteminder_home`*`\xps\db\tier2\criticalpath\CriticalPath.ldif`
7. Reload the schema, or verify that the schema has been updated.
8. Go to dsa, comms, LDAP, change the "paging mode" option to "always", and restart the DSA.

   The policy store schema is created for r12.0 SP3.
9. Manually create the following root nodes using Critical Path's iCon DIT administrator interface:
   - ou=Netegrity
   - ou=SiteMinder
   - ou=PolicySvr4
   - ou=XPS
10. Copy the smreg utility to *policy_server_home*\bin.

    policy_server_home

    Specifies the Policy Server installation path.
11. Run the following command:

    `smreg -su `*`password`*

    password

    Specifies the password for the default SiteMinder administrator.

Limits:

- The password must contain at least six (6) characters and cannot exceed 24 characters.
- The password cannot include an ampersand (&) or an asterisk (*).
- If the password contains a space, enclose the passphrase with quotation marks.

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

12. Delete the smreg utility from *policy_server_home*\bin. Deleting smreg prevents someone from changing the password without knowing the previous one.

    The password for the default SiteMinder administrator account is set.

13. Run the following command:

    ```
    smobjimport -ipolicy_server_home/db/smdif/smpolicy.smdif
    -dsiteminder_super_user_name -wsiteminder_super_user_password -v
    ```

    -i

    Specifies the path and name of the import file.

    -v

    Turns on tracing and outputs error, warning, and comment messages.

    The base policy store data is imported from the file smpolicy.smdif.

14. Run the following command:

    ```
    smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
    -dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
    ```

    -i

    Specifies the path and name of the import file.

    -d*siteminder_super_user_name*

    Specifies the name of the SiteMinder Super User account.

    -w*siteminder_super_user_password*

    Specifies the password for the SiteMinder Super User account.

    -f

    Overrides duplicate objects

    -v

    Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

    Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

smobjimport imports the policy store objects. These objects are automatically imported to the appropriate locations.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for more information on licensing.

The Critical Path inJoin Directory Server (IDS) is configured as a policy store.

Note: You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.

3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the SiteMinder environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually.

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   Specifies the password for the default SiteMinder super user account (siteminder).

   Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

-adminui–setup

Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

-t *timeout*

(Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect SiteMinder administrator credentials when logging into the Administrative UI for the first–time

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

Enable LDAP Tracing in IDS

To enable LDAP tracing in IDS

1. Stop the DSA.
2. Open the exec file located in the DSA directory (c:\ids\icon\dsa1) with a text editor.
3. Add the switch on the odsldap3 process.

   Example:

   1r odsldap3 -ldap:1708 -ldaps:0 -http:0 -https:0 -diag:5

   -diag:n 0 is OFF; higher values give more output:

   1=FATAL, 2=SEVERE, 3=ERROR, 4=WARNING,5=INFO, 6=ENTRY/EXIT

4. Start the DSA, using iCon.

   The log file will be available within iCon.

5. Select the DSA.
6. Select the comms option across the top menu.
7. Select the LDAP process.
8. Click on the file labeled odsldap3.out.000.

Sample User Directory Settings--Critical Path InJoin Directory Server

The following are sample user directory settings:

Directory Setup

- Namespace: LDAP
- Server: 123.456.7.8
- Root: o=companyname, c=us
- DN Lookup Start: (cn=
- DN Lookup End:)

Credentials and Connection

- Admin Username: cn=manager
- Admin Password: ********

User Attributes

- Universal ID (R): cn
- Disabled Flag (RW): description
- Password Attribute (RW): userpassword
- Password Data (RW): audio
- Challenge/Response (RW): jpegPhoto

Note: User attribute names in DMS are or are not case-sensitive on an attribute-by-attribute basis.

Sample Policy Server Settings--Critical Path InJoin Directory Server

The following are sample Policy Server settings:

LDAP

- LDAP IP Address: 12.3.4.5
- Admin Username: cn=manager
- Admin Password: ********
- Confirm Password: ********
- Root DN: o=companyname, c=us
- Use Policy Store: [checked]
- Netscape Certificate Database File: pathname

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.0 SP3 policy store. You can upgrade an existing policy store to r12.0 SP3.

Complete the following procedures to upgrade the policy store:

1. Extend the policy store schema.

   Note: The existing r6.x policy store schema has not changed. The r12.0 SP3 migration requires that you extend the policy store schema for policy store for objects that r12.0 SP3 requires.

2. Import the base policy store objects.
3. Import the Policy Store Data Definitions.

Note: If you are upgrading a directory server or database that is listed in the Support Matrix, but not in this guide, see the *SiteMinder Upgrade Guide.*

Extend the inJoin Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.0 SP3 using the Critical Path's iCon GUI. There are no changes to the existing 6.x policy store schema.

Follow these steps:

1. Start the DSA.
2. Navigate to *siteminder_home*\bin.

   siteminder_home

   Specifies the Policy Server installation path.
3. Run the following command:

   ```
   ldapmodify -hhost -pport -dAdminDN -wAdminPW -c
   -fsiteminder_home\xps\db\tier2\criticalpath\CriticalPath.ldif
   ```

   -h*host*

   Specifies the IP address of the LDAP server.

   -p*port*

   Specifies the port number of the LDAP server.

   -d*AdminDN*

   Specifies the name of an LDAP user with privileges to create a new LDAP schema on the LDAP directory server.

   Example: cn=manager

   -w*AdminPW*

   Specifies the password of the LDAP user with privileges to create a new LDAP schema on the LDAP directory server.

   -c

   Specifies continuous mode (do not stop on errors).

   Note: ldapmodify requires version 4.2 of the Critical Path inJoin Directory Server.
4. Reload the schema, or verify that the schema has been updated.
5. Go to dsa, comms, LDAP, change the "paging mode" option to "always", and restart the DSA.

   The policy store schema is extended to include the objects introduced by r12.0 SP3.

Import the Base Policy Store Objects

Importing the default SiteMinder objects upgrades the policy store for use with the Administrative UI. The default SiteMinder objects are required to store policy information in the 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.

To import the base policy store objects

1. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

Specifies the Policy Server installation path.

upgrade_smdif_file_name

Specifies the name of the import file:

- **r6.0 to r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r6.0 SP1 to r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r6.0 SP2 to r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r6.0 SP3 to r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r6.0 SP4 to r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r6.0 SP5 to r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r6.0 SP6 to r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.0 SP3.

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

Windows example: smobjimport
`-i"C:\Program Files\CA\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

The base policy store objects are imported.

2. Run the following command:

Important! Do not re-import ampolicy.smdif if it has been previously imported into the policy store.

`smobjimport -i`*`policy_server_home`*`\db\smdif\ampolicy.smdif -d`*`siteminder_super_user_name`* `-w`*`siteminder_super_user_password`* `-f -v -l -c`

-policy_server_home

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for licensing information.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

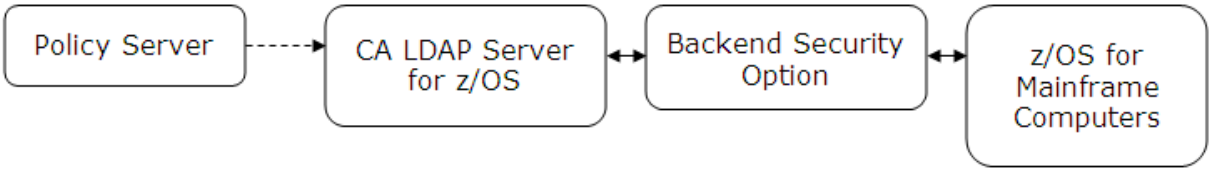
   You have imported all required policy store data definitions.

Chapter 3: CA LDAP Server for z/OS

This section contains the following topics:

CA LDAP Server for z/OS Overview

You can configure a CA LDAP Server for z/OS as a user store by configuring a connection from the Policy Server to the LDAP Server. How you configure the connection from the Policy Server to the LDAP Server depends on the backend option that you are using to secure the LDAP Server:



CA supports the following backend security options for CA LDAP Server:

- CA Top Secret r12 (TSS)
- CA LDAP Server r15 for z/OS (RACF)
- CA LDAP Server r15 for z/OS (ACF2)

Become familiar with the objectclass hierarchy for these backend security options before configuring the connection from the Policy Server to the LDAP Server. Also, add the backend-related objectclasses to the Policy Server registries in the LDAP namespace.

Note: z/OS is an IBM operating system for mainframe computers.

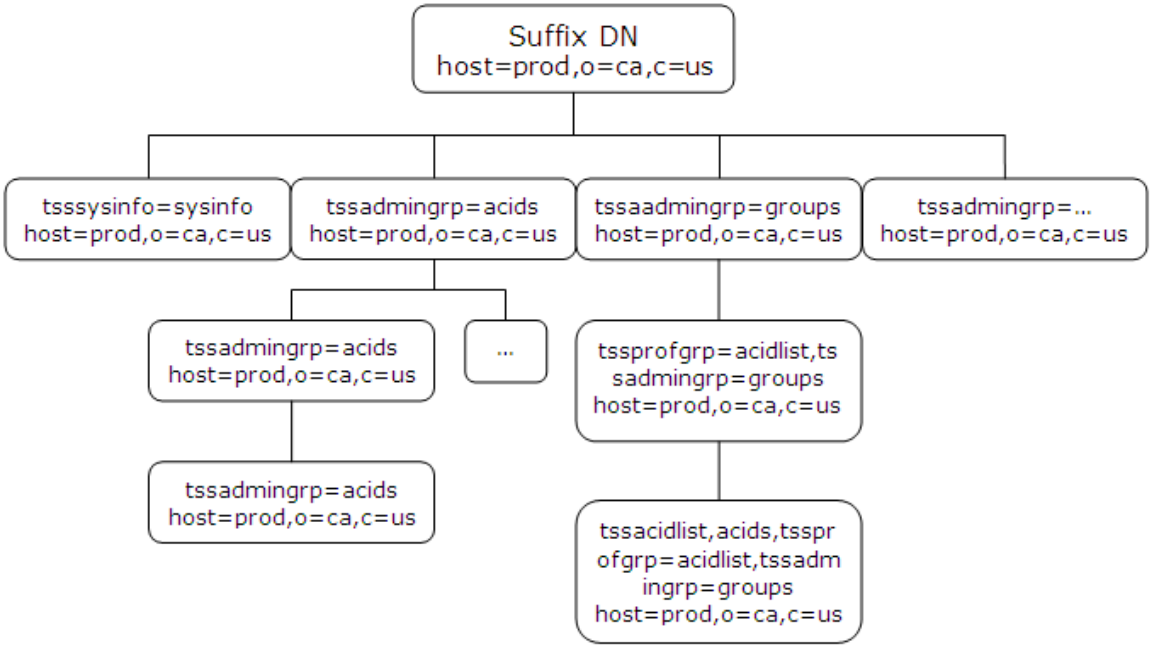
CA Top Secret r12 (TSS) Backend Security Option

When you are using TSS to secure the CA LDAP Server for z/OS, complete the following steps before configuring the connection from the Policy Server to the CA LDAP Server:

1. Become familiar with the TSS objectclass hierarchy.
2. Add the TSS objectclasses to the Policy Server registries in the LDAP namespace.

TSS Objectclass Hierarchy

The following diagram shows the hierarchy of objectclass entries in the CA Top Secret Directory Information Tree (DIT). Below the diagram is a description of each objectclass.



Objectclass host

Object class used to start access to the objectclass hierarchy for a CA Top Secret database.

Objectclass tsssysinfo

Object class used to create branches in the objectclass hierarchy below the host.

Objectclass tssadmingrp

Object class used to create branches in the objectclass hierarchy below the host.

Values:

- acids
- profiles
- groups
- departments
- divisions
- zones

Objectclass tssacid

Object class used to access the ACID record fields of all user types.

Objectclass tssacidgrp

Object class used to create the branches in the objectclass hierarchy below an acid.

Configure Policy Server Registry Entries for TSS

The CA LDAP Server for z/OS contains different object classes than other LDAP servers. Before configuring a connection from the Policy Server to the CA LDAP Server, add the TSS objectclasses to certain Policy Server registry entries in the LDAP namespace. Substitute the replacement values for the default values of the following Policy Server registry entries:

registry_entry_home

Specifies the following registry entry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds.

default_value

Specifies the default value of the registry entry.

replacement_value

Specifies a new value containing the TSS objectclasses for the registry entry.

- registry_entry_home\ClassFilters

  class_filters_default_value:

  organization,organizationalUnit,groupOfNames,groupOfUniqueNames,group

  class_filters_replacement_value:

  class_filters_default_value,eTTSSAcidName,tssacidgrp,tssadmingrp

- registry_entry_home\GroupClassFilters

  group_class_filters_default_value:

  groupOfNames,groupOfUniqueNames,group

  group_class_filters_replacement_value:

  group_class_filters_default_value,eTTSSAcidName,tssacidgrp,tssadmingrp

- registry_entry_home\PolicyClassFilters

  policy_class_filters_default_value:

  organizationalPerson,inetOrgPerson,organization,organizationalUnit, groupOfNames,groupOfUniqueNames,group

  policy_class_filters_replacement_value:

  policy_class_filters_default_value,eTTSSAcidName,tssacidgrp,tssadmingrp

- registry_entry_home\PolicyResolution

Add the following TSS object classes to this registry entry:

TSS Objectclass	Registry Key Type	Data
eTTSSAcidName	REG_DWORD	0x00000001(1)
tssacid	REG_DWORD	0x00000001(1)
tssacidgrp	REG_DWORD	0x00000002(2)
tssadmingrp	REG_DWORD	0x00000003(3)

Note: Some LDAP queries that the Policy Server issues (such as a full list of users) can take up to 60 seconds to complete. Under these conditions most of the queries from the Policy Server-side timeout. To improve connectivity, you can adjust this registry key entry as follows:

[HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Debug]
LDAPPingTimeout = 300; REG_DWORD

Configure a Connection from the Policy Server to CA LDAP Server for z/OS

To configure a connection from the Policy Server to the CA LDAP Server for z/OS, create a new user directory object in the Administrative UI.

To configure a connection from the Policy Server to the CA LDAP Server

1. Click Infrastructure, Directory, User Directory, Create User Directory.

   The Create User Directory pane opens.

   Note: You can click Help for a description of fields, controls, and their respective requirements.

2. Type the name and a description of the new User Directory object in the fields on the General group box.

3. Select LDAP from the Namespace list, and type the IP address and port number in the Server field on the Directory Setup group box.

   Note: Load balancing and failover are not supported for this LDAP server.

4. Select the Require Credentials check box, type the full DN and password of the administrator in the fields on the Administrator Credentials group box, and specify whether the directory connection uses SSL.

   Note: This step is required, because TSS does not allow anonymous binds to the user store.

5. Type the values in the fields on the LDAP Search group box, specifying a value of 100 seconds in the Max Time field.

   Note: This value is required, because the Policy Server takes more time when retrieving data from this LDAP Server.

6. Type the values in the fields on the LDAP UserDN Lookup group box.

7. (Optional) Specify the user directory profile attributes that are reserved for SiteMinder's use in the fields on the User Attributes group box.

8. (Optional) Click Create on the Attribute Mapping List group box.

   The Create Attribute Mapping pane opens.

9. Click Submit.

   The Create User Directory task is submitted for processing.

SiteMinder Features Not Supported by CA LDAP Server for z/OS

CA LDAP Server for z/OS does not support the following SiteMinder features:

Anonymous Binds

When configuring a CA Top Secret LDAP Server as a user store, you must provide values in the fields on the Administrator Credentials group box on the Create User Directory pane.

Characters Not Supported in User Names

The following characters are not supported in user names:

- space
- single quote
- opening parenthesis
- closing parenthesis
- comma
- backslash

Load Balancing and Failover

Load balancing and failover is not supported.

Password Services

Password Services is not supported.

User Groups and Policies

Adding a user group to a policy and attempting to authorize a user in that group fails.

CA LDAP Server r15 for z/OS (RACF) Backend Security Option

This section describes the settings that are required to configure the CA LDAP Server r15 for z/OS (RACF) as a user store with the Policy Server.

Configure Policy Server Registry Entries for RACF

The CA LDAP Server r15 for z/OS (RACF) contains a different set of objectclasses than other LDAP servers. Before configuring a user directory connection from the Policy Server to the CA LDAP Server, add the RACF objectclasses to certain Policy Server registry entries in the LDAP namespace. Substitute the replacement values for the default values of the following Policy Server registry entries:

registry_entry_home

Specifies the following registry entry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds.

default_value

Specifies the default value of the registry entry.

replacement_value

Specifies a new value containing the RACF objectclasses for the registry entry.

- registry_entry_home\ClassFilters

  class_filters_default_value:

  organization,organizationalUnit,groupOfNames,groupOfUniqueNames,group

  class_filters_replacement_value:

  class_filters_default_value,*

- registry_entry_home\GroupClassFilters

  group_class_filters_default_value:

  groupOfNames,groupOfUniqueNames,group

  group_class_filters_replacement_value:

  group_class_filters_default_value,*

- registry_entry_home\PolicyClassFilters

  policy_class_filters_default_value:

  organizationalPerson,inetOrgPerson,organization,organizationalUnit,groupOfNames,groupOfUniqueNames,group

  policy_class_filters_replacement_value:

  policy_class_filters_default_value,*

- registry_entry_home\PolicyResolution

  Add the following RACF objectclasses to this registry entry:

RACF Objectclass	Registry Key Type	Data
eTRACUserid	REG_DWORD	0x00000001(1)
eTRACAdminGrp	REG_DWORD	0x00000002(2)

- registry_entry_home\Debug

  In UNIX, add the following RACF objectclass to this registry entry:

RACF Objectclass	Registry Key Type	Data
LDAPPingTimeout=	REG_DWORD	300;

Note: The value of this registry key can be changed based on the response time of the CA LDAP Server r15 for z/OS (RACF).

Configure a Connection from the Policy Server to CA LDAP Server for z/OS (RACF)

To configure a directory connection from the Policy Server to the CA LDAP Server for z/OS, open an existing user directory object in the Administrative UI.

To configure a directory connection from the Policy Server to the CA LDAP Server

1. Open the User Directory Dialog.
2. In Directory Setup, select LDAP as the namespace.
3. Enter the connection information for your LDAP directory.

   Note: For more information, see the topic LDAP Namespace Directory Setup Tab in the *Policy Design Reference Guide*.

   Note: Failover is not supported for this LDAP Server.
4. In the LDAP Search box, in the Max Time field, specify a value of 300 seconds.

   Note: A greater timeout value is required, because the Policy Server takes more time to retrieve data from this LDAP Server.
5. In Credentials and Connection, specify administrator credentials that the Policy Server will use to connect to this LDAP Server.

   Important! Specifying administrator credentials is mandatory as anonymous binds to the user store are not allowed with CA LDAP Server r15 for z/OS (RACF).

SiteMinder Features Not Supported by CA LDAP Server for z/OS (RACF)

CA LDAP Server for z/OS (RACF) does not support the following SiteMinder features:

Password Services

Password Services is not supported.

Anonymous Binds

When configuring a CA LDAP Server r15 for z/OS (RACF) as a user store, provide values for the Administrator Credentials in the Create User Directory page.

Characters Not Supported in User Names

The following characters are not supported in user names:

- space
- single quote
- opening parenthesis
- closing parenthesis
- comma
- backslash

User Groups and Policies

Adding a user group to a policy and attempting to authorize a user in that group fails.

LDAP Failover and Replication

LDAP Failover and Replication is not supported.

CA LDAP Server r15 for z/OS (ACF2) Backend Security Option

This section describes the settings that are required to configure the CA LDAP Server r15 for z/OS (ACF2) as a user store with the Policy Server.

Configure Policy Server Registry Entries for ACF2

The CA LDAP Server r15 for z/OS (ACF2) contains a different set of objectclasses than other LDAP servers. Before configuring a user directory connection from the Policy Server to the CA LDAP Server, add the ACF2 objectclasses to certain Policy Server registry entries in the LDAP namespace. Substitute the replacement values for the default values of the following Policy Server registry entries:

registry_entry_home

Specifies the following registry entry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds.

default_value

Specifies the default value of the registry entry.

replacement_value

Specifies a new value containing the ACF2 objectclasses for the registry entry.

- registry_entry_home\ClassFilters

  class_filters_default_value:

  organization,organizationalUnit,groupOfNames,groupOfUniqueNames,group

  class_filters_replacement_value:

  class_filters_default_value,*

- registry_entry_home\GroupClassFilters

  group_class_filters_default_value:

  groupOfNames,groupOfUniqueNames,group

  group_class_filters_replacement_value:

  group_class_filters_default_value,*

- registry_entry_home\PolicyClassFilters

  policy_class_filters_default_value:

  organizationalPerson,inetOrgPerson,organization,organizationalUnit,groupOfNames,groupOfUniqueNames,group

  policy_class_filters_replacement_value:

  policy_class_filters_default_value,*

- registry_entry_home\PolicyResolution

  Add the following ACF2 objectclasses to this registry entry:

ACF2 Objectclass	Registry Key Type	Data
acf2lid	REG_DWORD	0x00000001(1)
acf2admingrp	REG_DWORD	0x00000002(2)
eTACFLidName	REG_DWORD	0x00000001(1)

- registry_entry_home\Debug

  In UNIX, add the following ACF2 objectclass to this registry entry:

ACF2 Objectclass	Registry Key Type	Data
LDAPPingTimeout=	REG_DWORD	300;

Note: The value of this registry key can be changed based on the response time of the CA LDAP Server r15 for z/OS (ACF2).

Configure a Connection from the Policy Server to CA LDAP Server for z/OS

To configure a directory connection from the Policy Server to the CA LDAP Server for z/OS (RACF) or CA LDAP Server for z/OS (ACF2), open an existing user directory object in the Administrative UI.

Follow these steps:

1. Open the User Directory Dialog.
2. In Directory Setup, select LDAP as the namespace.
3. Enter the connection information for your LDAP directory.

   Note: For more information, see the topic LDAP Namespace Directory Setup Tab in the *Policy Design Reference Guide*.

   Note: Failover is not supported for this LDAP Server.
4. In the LDAP Search section, in the Max Time field, specify a value of 300 seconds.

   Note: A greater timeout value is required, because the Policy Server takes more time to retrieve data from this LDAP Server.
5. In Credentials and Connection, specify administrator credentials that the Policy Server uses to connect to this LDAP Server.

   Important! Specifying administrator credentials is mandatory as anonymous binds to the user store are not allowed with CA LDAP Server r15 for z/OS (RACF) and CA LDAP Server r15 for z/OS (ACF2).

SiteMinder Features Not Supported by CA LDAP Server for z/OS (ACF2)

The SiteMinder features not supported by CA LDAP Server for z/OS (ACF2) are the same as specified for CA LDAP Server for z/OS (RACF).

Chapter 4: IBM DB2

This section contains the following topics:

How to Configure an IBM DB2 Database as a Data Store

SiteMinder provides schema files that you can use to create the schema for storing policies, keys, audit data, and session data in an IBM DB2 Database.

Complete the following tasks to configure an IBM DB2 database as a data store:

1. Create a DB2 database with SiteMinder schema.
2. Configure a DB2 Data Source for SiteMinder.
3. Point the Policy Server to the database.
4. Set the SiteMinder super user password.
5. Import the default policy store objects.
6. Import the policy store data definitions.
7. Prepare for the Administrative UI registration.

Create a DB2 Database with SiteMinder Schema

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to *siteminder_home*\db\tier2\DB2.

   siteminder_home

   Specifies the Policy Server installation path.
3. Open the following file in a text editor and copy the contents of the entire file:

   sm_db2_ps.sql

   Specifies the schema for a policy or key store in a DB2 database.
4. Paste the file contents into a query and execute the query.

   The policy or key store schema is created in the DB2 database.

5. (Optional) Repeat steps two and three to create the audit log, session server, or sample users schema in the DB2 database:

   sm_db2_logs.sql

   Specifies the schema for an audit log store in a DB2 database.

   sm_db2_ss.sql

   Specifies the schema for a session server in a DB2 database.

   smsampleusers_db2.sql

   Specifies the schema for sample users in a DB2 database and populates the database with the sample users.

   The corresponding SiteMinder schema is created in the DB2 database.

   Note: You can create multiple SiteMinder schema to a single DB2 database or create each schema in a separate database, optionally creating the following stores:

   - policy store
   - key store
   - audit logging store
   - session store
   - sample users store

6. Copy the following XPS schema file to the DB2 host system:

   siteminder_home\xps\db\tier2\db2\DB2.sql

7. Open a command prompt and run the following command:

   `db2 -td@ [-v] -f path\DB2.sql`

   path

   Specifies the path to the DB2 schema file.

   The policy store schema is created.

Configure a DB2 Data Source for SiteMinder

If you are using ODBC, you need to configure a data source for the DB2 wire protocol driver.

Create a DB2 Data Source on Windows Systems

When using ODBC, you can create a DB2 data source for the DB2 wire protocol driver.

Follow these steps:

1. Complete one of the following steps:
   - If you are using a supported 32–bit Windows operating system, click Start and select Programs, Administrative Tools, ODBC Data Sources.
   - If you are using a supported 64–bit Windows operating system:
     a. Navigate to the *install_home*\Windows\SysWOW64.
     b. Double–click odbcad32.exe

   The ODBC Data Source Administrator appears.
2. Click the System DSN tab and click Add.
3. Scroll down and select SiteMinder DB2 Wire Protocol and click Finish.
4. In the ODBC DB2 Wire Protocol Driver Setup dialog, under the General tab, complete the following steps:
   a. In the Data Source Name field, enter any name.

      Example:

      ```
      SiteMinder DB2 Wire Data Source
      ```

   b. (Optional) In the Description field, enter a description of the DB2 wire protocol data source.
   c. In the IP Address field, enter the IP Address where the DB2 database is installed.
   d. In the Tcp Port field, enter the port number where DB2 is listening on the system.
   e. Click Test Connect.

      The connection is tested.
5. Click OK.

   The ODBC DB2 Wire Protocol Driver Setup dialog closes, the selections are saved, and the DB2 data source is created on a Windows System.

Note: You can now configure SiteMinder to use the data source that you created.

Create a DB2 Data Source on UNIX Systems

The SiteMinder ODBC data sources are configured using a system_odbc.ini file, which you can create by renaming db2wire.ini, located in policy_server_home/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.

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 DB2 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 DB2 driver under [SiteMinder Data Source].

Again, to configure a DB2 data source, you must first create a system_odbc.ini file in the policy_server_home/db directory. To do this, you need to rename db2wire.ini, located in policy_server_home/db, to system_odbc.ini.

Note: policy_server_home specifies the Policy Server installation path.

Configure the DB2 Wire Protocol Driver

The following table contains configuration parameters for DB2 data sources. You can edit these parameters to configure data sources for separate key, audit log, session, and sample users databases.

Parameter	Description	How to Edit
Data Source Name	Name of the data source.	Enter the data source name inside the square brackets.
Driver	Full path to the SiteMinder DB2 Wire Protocol driver.	Replace "nete_ps_root" with the SiteMinder installation directory.
Description	Description of the data source.	Enter any desired description.

Database	Name of the DB2 UDB database.	Replace “nete_database” with the name of the database configured on the DB2 UDB server.
LogonID	Username required for accessing the database.	Replace “uid” with the username of the DB2 UDB administrator.
Password	Password required for accessing the database.	Replace “pwd” with the password of the DB2 UDB administrator.
IPAddress	IP address or hostname of the DB2 UDB server.	Replace “nete_server_ip” with the IP address or the hostname of the DB2 UDB server.
TcpPort	TCP port number of the DB2 UDB server.	Replace the default value of 50000 with the actual TCP port number of the DB2 UDB server.
Package	The name of the package to process dynamic SQL.	Replace “nete_package” with the name of the package you want to create.
PackageOwner	(Optional) The AuthID assigned to the package.	Empty by default. This DB2 AuthID must have authority to execute all SQLs in the package.
GrantAuthid	The AuthID granted execute privileges for the package.	“PUBLIC” by default. Specify the desired AuthID if you wish to restrict the execute privileges for the package.
GrantExecute	Specifies whether to grant execute privileges to the AuthID listed in GrantAuthid.	Can be either 1 or 0. Set to 0 by default.
IsolationLevel	The method by which locks are acquired and released by the system.	CURSOR_STABILITY by default.
DynamicSections	The number of statements that the DB2 Wire Protocol driver package can prepare for a single user.	100 by default. Enter the desired number of statements.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can access the SiteMinder data in the policy store.

Follow these steps:

1. Open the Policy Server Management Console and click the Data tab.
2. Select the following value from the Storage list:

   ODBC
3. Select the following value from the Database list:

   `Policy Store`
4. Enter the name of the data source in the Data Source Information field.
   - (Windows) The entry must match the name that you entered in the Data Source Name field when you created the data source.
   - (UNIX) The entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure to enter the correct value.
5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
6. Specify the maximum number of database connections that are allocated to SiteMinder.

   Note: We recommend retaining the 25 connection default for best performance.
7. Click Apply to save the settings.
8. Select the following value from the Database list:

   `Key Store`
9. Select the following value from the Storage list:

   ODBC
10. Select the following option:

    `Use the Policy Store database`
11. Select the following value from the Database list:

    `Audit Logs`
12. Select the following value from the Storage list:

    ODBC
13. Select the following option:

    `Use the Policy Store database`
14. Click Apply to save the settings.

15. Click Test Connection to verify that the Policy Server can access the policy store.
16. Click OK.

    The Policy Server is configured to use the database as a policy store, key store, and logging database.

Set the SiteMinder Super User Password

The default SiteMinder administrator account is named siteminder. This account has maximum permissions. Set the password for this account so it can be used to manage the SiteMinder user interfaces and utilities until additional SiteMinder administrators can be created.

Note: The smreg utility is located at the top level of the Policy Server installation kit.

To set the super user password

1. Copy the smreg utility to *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   smreg -su 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.

   password

   Specifies the password for the default SiteMinder administrator.

   Limits:

   - The password must contain at least six (6) characters and cannot exceed 24 characters.
   - The password cannot include an ampersand (&) or an asterisk (*).
   - If the password contains a space, enclose the passphrase with quotation marks.

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

3. Delete the smreg utility from *policy_server_home*\bin. Deleting smreg prevents someone from changing the password without knowing the previous one.

   The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day–to–day operations. Use the default super user to:

- Import the default policy store objects.
- Access the FSS Administrative UI and Administrative UI for the first–time. We recommend creating another administrator with super user permissions.

More information:

Locate the Installation Media (see page 213)

Import the Default Policy Store Objects

Importing the default policy store objects sets up the policy store for use with the Administrative UI. The default policy store objects are required to store policy information in the policy store.

Note: If you have installed the Policy Server in FIPS-only mode, ensure you use the -cf argument when importing the default policy store objects.

To import the default policy store objects

1. Run the following command:

   ```
   smobjimport -ipolicy_server_home\db\smdif\smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

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

   Windows example: smobjimport
   ```
   -i"C:\Program Files\CA\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
   ```

   policy_server_home

   Specifies the Policy Server installation path.

   -d*siteminder_super_user_name*

   Specifies the name of the SiteMinder super user account.

   Default: siteminder

   -w*siteminder_super_user_password*

   Specifies the password for the SiteMinder super user account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-cf

(Optional) Imports sensitive data using FIPS-compatible cryptography.

Note: This argument is only required if the Policy Server is operating in FIPS-only mode.

smobjimport imports the policy store objects. The objects are automatically imported to the appropriate locations.

2. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder super user account.

Default: siteminder

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

smobjimport imports the policy store objects. These objects are automatically imported to the appropriate locations.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for more information about licensing.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the SiteMinder environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually.

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   Specifies the password for the default SiteMinder super user account (siteminder).

   Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

   -adminui–setup

   Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

-t *timeout*

(Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect SiteMinder administrator credentials when logging into the Administrative UI for the first–time

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

Upgrade a 6.x Session Server

If you have a 6.x Session Server installed, you can upgrade it to take advantage of the features in r12.0 SP3.

Note: The r12.0 SP3 session server schema has not changed from r6.0 SP5. If you have an r6.0 SP5 session server or later, you do not have to upgrade the schema.

Import one of the following SQL schema scripts into the existing session store database:

6.0, 6.0 SP1 or 6.0 SP2 to r12.0 SP3

dir_config_home\ibmdb2\sm_db2_ss_upgrade_60_60sp1or2_to_R12sp3.sql

6.0 SP3 or 6.0 SP4 to r12.0 SP3

dir_config_home\ibmdb2\sm_db2_ss_upgrade_60sp3or4_to_R12sp3.sql

dir_config_home

Specifies the Directory Configuration installation path.

A DB2 database session store is upgraded from 6.x to r12.0 SP3, and a new Expiry Data table is added to the session store.

Note: More information on importing a SQL script into a session store database exists in the *Policy Server Installation Guide*.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.0 SP3 policy store. You can upgrade an existing policy store to r12.0 SP3.

Complete the following procedures to upgrade the policy store:

1. Extend the policy store schema.

   Note: The existing r6.x policy store schema has not changed. The r12.0 SP3 migration requires that you extend the policy store schema for policy store for objects that r12.0 SP3 requires.

2. Import the base policy store objects.
3. Import the Policy Store Data Definitions.

Note: If you are upgrading a directory server or database that is listed in the Support Matrix, but not in this guide, see the *SiteMinder Upgrade Guide.*

Extend the IBM DB2 Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.0 SP3. There are no changes to the existing 6.x policy store schema.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to the following location:

   siteminder_home\xps\db\tier2\db2

   siteminder_home

   Specifies the Policy Server installation path.
3. Copy the following schema file:

   DB2.sql
4. Log in to the DB2 host system and save the schema file locally.
5. Open a command prompt and run the following command:

   `db2 -td@ [-v] -f path\DB2.sql`

   path

   Specifies the path to the DB2 schema file.

   The policy store schema is extended.

Import the Base Policy Store Objects

Importing the default SiteMinder objects upgrades the policy store for use with the Administrative UI. The default SiteMinder objects are required to store policy information in the 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.

To import the base policy store objects

1. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

Specifies the Policy Server installation path.

upgrade_smdif_file_name

Specifies the name of the import file:

- **r6.0 to r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r6.0 SP1 to r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r6.0 SP2 to r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r6.0 SP3 to r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r6.0 SP4 to r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r6.0 SP5 to r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r6.0 SP6 to r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.0 SP3.

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

Windows example: smobjimport
`-i"C:\Program Files\CA\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

The base policy store objects are imported.

2. Run the following command:

Important! Do not re-import ampolicy.smdif if it has been previously imported into the policy store.

`smobjimport -i`*`policy_server_home`*`\db\smdif\ampolicy.smdif -d`*`siteminder_super_user_name`* `-w`*`siteminder_super_user_password`* `-f -v -l -c`

-policy_server_home

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for licensing information.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Chapter 5: IBM Directory Server

This section contains the following topics:

IBM Directory Server as a Policy Store

Policy Servers installed on either Windows or UNIX systems can use an IBM Secureway/Directory Server as a policy store.

The following sections detail how to configure your directory server as a policy store.

IBM Directory Server

Before you configure an IBM Directory Server as a policy store, be sure that you have met the following prerequisites:

1. Edit the SiteMinder policy store schema file.

   Note: If applicable, create or load a server suffix using the IBM directory server configuration tool.

2. Create a directory entry and root nodes.

Edit the V3 Matching Rules File

Edit the V3 matching rules (V3.matchingrules) file before you import the policy store schema and the default policy store objects.

To edit the file

1. Open the V3 matching rules file.

   Note: For more information about the V3 matching rules file, see your vendor–specific documentation.

2. Add the following line:

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

3. Save the file.

   The V3 matching rules file is edited.

Create a Directory Entry and Root Nodes

You use the IBM Tivoli Directory Server Web Administration Tool to create a directory entry and root nodes.

Note: If applicable, create or load a server suffix using the IBM Tivoli Directory Server Configuration Tool.

Follow these steps:

1. Create a directory entry for the root DN of the policy server data.

   Example:

   `ou=Nete`

2. Create the following root nodes under the root DN:

   Example:

   `ou=Netegrity,ou=SiteMinder,ou=PolicySvr4,ou=XPS`

Gather Directory Server Information

Configuring an LDAP directory server as a policy store or upgrading an existing policy store requires specific directory server information. Gather the following information before beginning. You can use the Policy Store Worksheets to record your values.

Note: Policy and data store worksheets are provided to help you gather and record information before configuring or upgrading a SiteMinder data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

Specifies the fully-qualified host name or the IP Address of the directory server.

Port information

(Optional) Specifies a non-standard port.

Default values: 636 (SSL) and 389 (non-SSL)

Administrative DN

Specifies the LDAP user name of a user who has privileges to create, read, modify, and delete objects in the LDAP tree underneath the policy store root object.

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

Specifies the distinguished name of the node in the LDAP tree where policy store objects are to be defined.

SSL client certificate

Specifies the pathname of the directory where the SSL client certificate database file resides.

Limit: SSL only

How to Configure the Policy Store

To configure an IBM Directory Server as a policy store, complete the following steps:

1. Verify that you have met the IBM Directory Server prerequisites.
2. Verify that you have gathered the necessary information.
3. Point the Policy Server to the policy store.
4. Create the policy store schema.
5. Set the SiteMinder super user password.
6. Import the default policy store objects.
7. Import the policy store data definitions.
8. Restart the Policy Server.
9. Prepare for the Administrative UI registration.

Point the Policy Server to the Policy Store

You point the Policy Server to the policy store so the Policy Server can access the policy store.

Follow these steps:

1. Open the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut with Administrator permissions. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the Data tab.
3. Select the following value from the Database list:

   ```
   Policy Store
   ```

4. Select the following value from the Storage list:

   LDAP

5. Configure the following settings in the LDAP Policy Store group box.

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

   Note: You can click Help for a description of fields, controls, and their respective requirements.

6. Click Apply.
7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.
8. Select the following value from the Database list:

   `Key Store`

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    `Use Policy Store database`

11. Click OK.

Create the Policy Store Schema

You create the policy store schema so the directory server can function as a policy store and store SiteMinder objects.

To create the policy store schema

1. Access the directory server using the IBM directory server configuration tool.
2. Navigate to *policy_server_home*\IBMDirectoryServer.

   policy_server_home

   Specifies the Policy Server installation path.

3. Use the IBM directory server configuration tool to add the V3.siteminder*release* schema file to the Manage Schema Files section of the schema configuration.

   release

   Specifies the SiteMinder release.

4. Navigate to *policy_server_home*\xps\db.
5. Locate the following file:

   IBMDirectoryServer.ldif
6. Use the IBM directory server configuration tool to add the file to the Manage Schema Files section of the schema configuration.
7. Restart the directory server.

   The policy store schema is created.

Set the SiteMinder Super User Password

The default SiteMinder administrator account is named siteminder. This account has maximum permissions. Set the password for this account so it can be used to manage the SiteMinder user interfaces and utilities until additional SiteMinder administrators can be created.

Note: The smreg utility is located at the top level of the Policy Server installation kit.

To set the super user password

1. Copy the smreg utility to *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   `smreg -su 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.

   password

   Specifies the password for the default SiteMinder administrator.

   Limits:

   - The password must contain at least six (6) characters and cannot exceed 24 characters.
   - The password cannot include an ampersand (&) or an asterisk (*).
   - If the password contains a space, enclose the passphrase with quotation marks.

   Note: The password is not case sensitive, except when the password is stored in an Oracle policy store.
3. Delete the smreg utility from *policy_server_home*\bin. Deleting smreg prevents someone from changing the password without knowing the previous one.

   The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day–to–day operations. Use the default super user to:

- Import the default policy store objects.
- Access the FSS Administrative UI and Administrative UI for the first–time. We recommend creating another administrator with super user permissions.

More information:

Locate the Installation Media (see page 213)

Import the Default Policy Store Objects

Importing the default policy store objects sets up the policy store for use with the Administrative UI. The default policy store objects are required to store policy information in the policy store.

Note: If you have installed the Policy Server in FIPS-only mode, ensure you use the -cf argument when importing the default policy store objects.

To import the default policy store objects

1. Run the following command:

   ```
   smobjimport -ipolicy_server_home\db\smdif\smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

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

   Windows example: smobjimport

   ```
   -i"C:\Program Files\CA\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
   ```

   policy_server_home

   Specifies the Policy Server installation path.

   -d*siteminder_super_user_name*

   Specifies the name of the SiteMinder super user account.

   Default: siteminder

   -w*siteminder_super_user_password*

   Specifies the password for the SiteMinder super user account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-cf

(Optional) Imports sensitive data using FIPS-compatible cryptography.

Note: This argument is only required if the Policy Server is operating in FIPS-only mode.

smobjimport imports the policy store objects. The objects are automatically imported to the appropriate locations.

2. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder super user account.

Default: siteminder

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

smobjimport imports the policy store objects. These objects are automatically imported to the appropriate locations.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for more information about licensing.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.

3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the SiteMinder environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually.

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   Specifies the password for the default SiteMinder super user account (siteminder).

   Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

   -adminui–setup

   Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

   -t *timeout*

   (Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

   Unit of measurement: minutes

   Default: 240 (4 hours)

   Minimum Limit: 15

   Maximum Limit: 1440 (24 hours)

   -r *retries*

   (Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect SiteMinder administrator credentials when logging into the Administrative UI for the first–time

   Default: 1

   Maximum Limit: 5

   -c *comment*

   (Optional) Inserts the specified comments into the registration log file for informational purposes.

   Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.0 SP3 policy store. You can upgrade an existing policy store to r12.0 SP3.

Complete the following procedures to upgrade the policy store:

1. Extend the policy store schema.

   Note: The existing r6.x policy store schema has not changed. The r12.0 SP3 migration requires that you extend the policy store schema for policy store for objects that r12.0 SP3 requires.

2. Import the base policy store objects.
3. Import the Policy Store Data Definitions.

Note: If you are upgrading a directory server or database that is listed in the Support Matrix, but not in this guide, see the *SiteMinder Upgrade Guide.*

Extend the IBM Directory Server Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.0 SP3. There are no changes to the existing 6.x policy store schema.

To extend the IBM Directory Server policy store schema

1. Use the IBM Tivoli Directory Server Web Administration Tool to update the policy store root nodes.Create the following root node under ou=PolicySvr4:

   ou=XPS

2. Navigate to *siteminder_home*\xps\db, locate the following file, and add it to the Manage Schema Files section of the schema configuration using the IBM Directory Server Configuration Tool:

   IBMDirectoryServer.ldif

   siteminder_home

   Specifies the Policy Server installation path.

3. Restart the IBM Directory Server.

   The policy store schema is extended to include the objects introduced by r12.0 SP3.

Import the Base Policy Store Objects

Importing the default SiteMinder objects upgrades the policy store for use with the Administrative UI. The default SiteMinder objects are required to store policy information in the 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.

To import the base policy store objects

1. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

Specifies the Policy Server installation path.

upgrade_smdif_file_name

Specifies the name of the import file:

- **r6.0 to r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r6.0 SP1 to r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r6.0 SP2 to r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r6.0 SP3 to r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r6.0 SP4 to r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r6.0 SP5 to r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r6.0 SP6 to r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.0 SP3.

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

Windows example: smobjimport
`-i"C:\Program Files\CA\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

The base policy store objects are imported.

2. Run the following command:

Important! Do not re-import ampolicy.smdif if it has been previously imported into the policy store.

`smobjimport -i`*`policy_server_home`*`\db\smdif\ampolicy.smdif -d`*`siteminder_super_user_name`* `-w`*`siteminder_super_user_password`* `-f -v -l -c`

-policy_server_home

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for licensing information.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Chapter 6: MySQL Server

This section contains the following topics:

Configure a MySQL Policy Store

A MySQL policy store can also function as:

- A key store
- An audit logging database

  Note: SiteMinder session information should be stored in a separate database. You should not use the policy store to store session information.

Using a single database simplifies administration tasks. The following sections provide instruction on how to configure a single database server to store SiteMinder data.

Gather Database Information

Configuring a single MySQL Server database to function as a policy store or any other type of SiteMinder data store requires specific database information.

Gather the following information before configuring the policy store or any other type of SiteMinder data store.

- **Database host**—Identify the name of the database host system.
- **Database name**—Identify the name of the database instance that is to function as the policy store or data store.
- **Database port**—Identify the port on which the database is listening.
- **Administrator account**—Identify the login ID of an administrator account that has permission to create, read, modify, and delete objects in the database.
- **Administrator password** —Identify the password for the administrator account.

How to Configure the Policy Store

Complete the following procedures to configure a MySQL Server database as a policy store.

Note: Be sure that you have gathered the required database information before beginning. Some of the following procedures require this information.

1. Be sure that MySQL is installed using the default character set (Latin1). If MySQL was not installed using the default character set, reinstall MySQL before configuring the SiteMinder data store.
2. Be sure that the MySQL database that is to function as the policy store is accessible from the Policy Server host system.
3. Use the vendor–specific user interface to create the database instance for the SiteMinder data store.
4. Create the SiteMinder schema.
5. Configure a MySQL data source for SiteMinder.
   - (Windows) Create a MySQL data source.
   - (UNIX) Create a MySQL data source on UNIX systems.
   - (UNIX) Configure the MySQL wire protocol driver.
6. Point the Policy Server to the database.
7. Set the SiteMinder super user password.
8. Import the default SiteMinder objects.
9. Import the policy store data definitions.
10. Restart the Policy Server.
11. Prepare for the Administrative UI registration.

Create the SiteMinder Schema

You create the SiteMinder schema so that the MySQL database can store policy, key, and audit logging information.

Follow these steps:

1. Navigate to *siteminder_home*\db\tier2\MySQL.

   siteminder_home

   Specifies the Policy Server installation path.

2. Open the following file in a text editor:

   sm_mysql_ps.sql

3. Locate the following lines:

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

4. Replace each instance of 'databaseName' with the name of the database functioning as the policy store.

   Example: If the name of the database is smpolicystore, the required update appears as follows:

```
DROP FUNCTION IF EXISTS `smpolicystore`.`getdate` $$
CREATE FUNCTION `smpolicystore`.`getdate` () RETURNS DATE
```

5. Copy the contents of the entire file.
6. Paste the file contents in to a query and execute the query.

   Note: You can also use this schema file to create a seperate key store.

7. (Optional) If the policy store is to store audit logs:

   Note: You can use a separate database to function as this type of SiteMinder data store.

   a. Open the following file in a text editor:

      sm_mysql_logs.sql

   b. Locate the following lines:

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

   c. Replace each instance of 'databaseName' with the name of the database functioning as the audit store.

   d. Copy the contents of the entire file.

   e. Paste the file contents into a query and execute the query.

      The audit store schema is created.

8. (Optional) If the policy store is to function as a SiteMinder sample user store:

   Note: You can use a separate database to function as this type of SiteMinder data store.

   a. Open the following file in a text editor:

      smsampleusers_mysql.sql

   b. Locate the following lines:

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

   c. Replace each instance of 'databaseName' with the name of the database functioning as the SiteMinder sample user store.

d. Copy the contents of the entire file.

e. Paste the file contents into a query and execute the query.

The SiteMinder sample user store schema is created.

9. Navigate to *siteminder_home*\xps\db\tier2\MySQL

siteminder_home

Specifies the Policy Server installation path.

10. Open the following file in a text editor and copy the contents of the entire file:

MySQL.sql

11. Paste the file contents into a query.

12. Use the MySQL command line tool to exectute the query.

The policy store schema is created.

Configure a MySQL Data Source for SiteMinder

You configure a data source to let the Policy Server communicate with the SiteMinder data store.

More information:

How to Configure a MySQL User Store (see page 97)

Create a MySQL Data Source on Windows

You create a MySQL data source for the MySQL wire protocol driver.

Follow these steps:

1. Log in to the Policy Server host system.
2. Do one of the following steps:
   - If you are using a supported 32–bit Windows operating system, click Start and select Programs, Administrative Tools, ODBC Data Sources.
   - If you are using a supported 64–bit Windows operating system:
     a. Navigate to the *install_home*\Windows\SysWOW64.
     b. Double–click odbcad32.exe.

   The ODBC Data Source Administrator appears.
3. Click System DSN.

   System Data Sources lists all available data sources.

4. Click Add.

   The Create New Data Source dialog appears.

5. Scroll down and select SiteMinder MySQL Wire Protocol and click Finish.

   The ODBC MySQL Wire Protocol Driver Setup dialog appears.

6. Complete the following steps in the General tab:

   a. Enter a data source name in the Data Source Name field.

      Example:

      ```
      SiteMinder MySQL Wire Data Source
      ```

   b. Enter the name of the MySQL database host system in the Host Name field.

   c. Enter the port on which the MySQL database is listening in the Port Number field.

   d. Enter the name of the MySQL database in the Database Name field.

7. Click Test Connect.

   The connection settings are tested. If the settings are valid, a prompt states that the connection is successful.

8. Click OK.

   The data source is created and appears in the System Data Sources list.

Note: You can now point the Policy Server to the SiteMinder data store.

Create a MySQL Data Source on UNIX Systems

The SiteMinder ODBC data sources are configured using a system_odbc.ini file, which you create by renaming mysqlwire.ini to system_odbc.ini. The mysqlwire.ini file is located in *siteminder_home*/db.

siteminder_home

Specifies the Policy Server installation path.

This system_odbc.ini file contains all of the names of the available ODBC data sources and 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 value. The value is required when you configure the 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 that is loaded when SiteMinder uses this data source. The remaining attributes are specific to the driver.

Adding a MySQL Server Data source involves:

- Adding a new data source name in the [ODBC Data Sources] section of the file.
- Adding a section that describes the data source using the same name as the data source.

If you create a new service name or want to use a different driver, update the system_odbc.ini file. You should have entries for the MySQL driver under [SiteMinder Data Source].

Again, to configure a MySQL Server data source, you create the system_odbc.ini file by renaming mysqlwire.ini to system_odbc.ini.

Create the MySQL Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder uses to connect to the database.

Note: This procedure only applies if the Policy Server is installed on a UNIX system. If you have not already done so, copy one of the following files and rename it system_odbc.ini. The file you rename depends on the database vendor you are configuring as a SiteMinder data store.

- sqlserverwire.ini
- oraclewire.ini
- mysqlwire.ini

These files are located in *siteminder_home*/db

The system_odbc.ini file contains the following sections. The data source that you are configuring determine the section or sections that you edit:

[SiteMinder Data Source]

Specifies the settings SiteMinder is to use to connect to the database functioning as the policy store.

[SiteMinder Logs Data Source]

Specifies the settings SiteMinder is to use to connect to the database functioning as the audit log database.

[SiteMinder Keys Data Source]

Specifies the settings SiteMinder is to connect to the database functioning as the key store.

[SiteMinder Session Data Source]

Specifies the settings SiteMinder is to connect to the database functioning as the session store.

[SmSampleUsers Data Source]

Specifies the settings SiteMinder is to connect to the database functioning as the sample user data store.

Follow these steps:

1. Open the system_odbc.ini file.
2. Enter the following under [ODBC Data Sources]:

   ```
   SiteMinder Data Source=DataDirect 6.0 MySQL Wire Protocol.
   ```

3. Depending on the data source you are configuring, edit the one or more of the data source sections with the following information:

   ```
   Driver=nete_ps_root/odbc/lib/NSmysql24.so
   Description=DataDirect 6.0 MySQL Wire Protocol
   Database=database_name
   HostName=host_name
   LogonID=root_user
   Password=root_user_password
   PortNumber=mysql_port
   ```

   Note: When editing data source information, do not use the pound sign (#). Entering a pound sign comments the information, which truncates the value. The truncated value can cause ODBC connections to fail.

   nete_ps_root

   Specifies the Policy Server installation path. Enter this value as an explicit path, rather than one with an environment variable.

   Example: /export/smuser/siteminder

   database_name

   Specifies the name of the MySQL database that is to function as the SiteMinder data store.

   host_name

   Specifies the name of the MySQL database host system.

   root_user

   Specifies the login ID of the MySQL root user.

root_user_password

Specifies the password for the MySQL root user.

mysql_port

Specifies the port on which the MySQL database is listening.

4. Save the file.

   The wire protocol driver is configured.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can access the SiteMinder data in the policy store.

Follow these steps:

1. Open the Policy Server Management Console and click the Data tab.
2. Select the following value from the Storage list:

   ODBC

3. Select the following value from the Database list:

   `Policy Store`

4. Enter the name of the data source in the Data Source Information field.
   - (Windows) The entry must match the name that you entered in the Data Source Name field when you created the data source.
   - (UNIX) The entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure to enter the correct value.
5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
6. Specify the maximum number of database connections that are allocated to SiteMinder.

   Note: We recommend retaining the 25 connection default for best performance.

7. Click Apply to save the settings.
8. Select the following value from the Database list:

   `Key Store`

9. Select the following value from the Storage list:

   ODBC

10. Select the following option:

    `Use the Policy Store database`

11. Select the following value from the Database list:

    `Audit Logs`

12. Select the following value from the Storage list:

    ODBC

13. Select the following option:

    `Use the Policy Store database`

14. Click Apply to save the settings.
15. Click Test Connection to verify that the Policy Server can access the policy store.
16. Click OK.

    The Policy Server is configured to use the database as a policy store, key store, and logging database.

Set the SiteMinder Super User Password

The default SiteMinder administrator account is named siteminder. This account has maximum permissions. Set the password for this account so it can be used to manage the SiteMinder user interfaces and utilities until additional SiteMinder administrators can be created.

Note: The smreg utility is located at the top level of the Policy Server installation kit.

To set the super user password

1. Copy the smreg utility to *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   `smreg -su` *`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.

   password

   Specifies the password for the default SiteMinder administrator.

Limits:

- The password must contain at least six (6) characters and cannot exceed 24 characters.
- The password cannot include an ampersand (&) or an asterisk (*).
- If the password contains a space, enclose the passphrase with quotation marks.

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

3. Delete the smreg utility from *policy_server_home*\bin. Deleting smreg prevents someone from changing the password without knowing the previous one.

   The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day–to–day operations. Use the default super user to:

- Import the default policy store objects.
- Access the FSS Administrative UI and Administrative UI for the first–time. We recommend creating another administrator with super user permissions.

More information:

Locate the Installation Media (see page 213)

Import the Default Policy Store Objects

Importing the default policy store objects sets up the policy store for use with the Administrative UI. The default policy store objects are required to store policy information in the policy store.

Note: If you have installed the Policy Server in FIPS-only mode, ensure you use the -cf argument when importing the default policy store objects.

To import the default policy store objects

1. Run the following command:

   ```
   smobjimport -ipolicy_server_home\db\smdif\smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

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

   Windows example: smobjimport
   ```
   -i"C:\Program Files\CA\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
   ```

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder super user account.

Default: siteminder

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder super user account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-cf

(Optional) Imports sensitive data using FIPS-compatible cryptography.

Note: This argument is only required if the Policy Server is operating in FIPS-only mode.

smobjimport imports the policy store objects. The objects are automatically imported to the appropriate locations.

2. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder super user account.

Default: siteminder

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

smobjimport imports the policy store objects. These objects are automatically imported to the appropriate locations.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for more information about licensing.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.

3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the SiteMinder environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually.

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   Specifies the password for the default SiteMinder super user account (siteminder).

   Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

   -adminui–setup

   Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

   -t *timeout*

   (Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

   Unit of measurement: minutes

   Default: 240 (4 hours)

   Minimum Limit: 15

   Maximum Limit: 1440 (24 hours)

   -r *retries*

   (Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect SiteMinder administrator credentials when logging into the Administrative UI for the first–time

   Default: 1

   Maximum Limit: 5

   -c *comment*

   (Optional) Inserts the specified comments into the registration log file for informational purposes.

   Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

Configure MySQL Data Stores

SiteMinder keys and SiteMinder audit information can each be stored in a separate database.

Consider the following:

- 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 Administration Guide*.
- SiteMinder session information must be stored in a separate database. You cannot use the policy store to store session information.

The following sections detail how to configure individual data stores.

How to Store Key Information in MySQL

Complete the following procedures to configure MySQL as a standalone key store:

1. Be sure that MySQL is installed using the default character set (Latin1). If MySQL was not installed using the default character set, reinstall MySQL before configuring the SiteMinder data store.
2. Gather database information.
3. Create the key store schema.
4. Configure a MySQL data source for SiteMinder.
5. Point the Policy Server to the database.
6. Restart the Policy Server.

More information:

Gather Database Information (see page 75)
Configure a MySQL Data Source for SiteMinder (see page 78)

Create the Key Store Schema

You create the key store schema so the MySQL database can store key information.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to the following location:

   siteminder_home\db\tier2\MySQL.

   siteminder_home

   Specifies the Policy Server installation path.
3. Open the following file in a text editor:

   sm_mysql_ps.sql
4. Locate the following lines:

   ```
   DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
   CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
   ```
5. Replace each instance of 'databaseName' with the name of the database functioning as the key store.
6. Copy the contents of the entire file.
7. Paste the file contents into a query and execute the query.

   The key store schema is created.

Point the Policy Server to Database

You point the Policy Server to the database so the Policy Server can read and store key information.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.
2. Select ODBC from the Storage list.

   ODBC settings appear.
3. Select Key Store from the Database list and clear the Use Policy Store database check box.

   Data source settings become active.

4. Enter the name of the data source in the Data Source Information field.
   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.
5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
6. Specify the maximum number of database connections allocated to SiteMinder.

   Note: We recommend retaining the default for best performance.
7. Click Apply.

   The settings are saved.
8. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.
9. Click OK.

   The Policy Server is configured to use the database as a key store

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Audit Logs in MySQL

Complete the following procedures to configure MySQL as a standalone audit log store:

1. Be sure that MySQL is installed using the default character set (Latin1). If MySQL was not installed using the default character set, reinstall MySQL before configuring the SiteMinder data store.

2. Gather database information.
3. Create the audit log schema.
4. Configure a MySQL data source for SiteMinder.
5. Point the Policy Server to the database.
6. Restart the Policy Server.

More information:

Gather Database Information (see page 75)

Create the Audit Log Schema

You create the audit log schema so the MySQL database can store audit logs.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to the following location:

   siteminder_home\db\tier2\MySQL.

   siteminder_home

   Specifies the Policy Server installation path.
3. Open the following file in a text editor:

   sm_mysql_logs.sql
4. Locate the following lines:

   ```
   DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
   CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
   ```
5. Replace each instance of 'databaseName' with the name of the database functioning as the audit store.
6. Copy the contents of the entire file.
7. Paste the file contents into a query and execute the query.

   The audit store schema is created.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can read and store audit logs.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select ODBC from the Storage list.

   ODBC settings appear.

3. Select Audit Logs from the Database list.

4. Select ODBC from the Storage list.

   Data source settings become active.

5. Enter the name of the data source in the Data Source Information field.

   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.

6. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.

7. Specify the maximum number of database connections allocated to SiteMinder.

   Note: We recommend retaining the default for best performance.

8. Click Apply.

   The settings are saved.

9. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

10. Click OK.

    The Policy Server is configured to use the database as an audit logging database.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Session Information in MySQL

Complete the following procedures to configure MySQL as a standalone session store:

1. Be sure that MySQL is installed using the default character set (Latin1). If MySQL was not installed using the default character set, reinstall MySQL before configuring the SiteMinder data store.
2. Gather database information.
3. Create the session store schema.
4. Configure a MySQL data source for SiteMinder.
5. Point the Policy Server to the database.
6. Restart the Policy Server.

More information:

Gather Database Information (see page 75)

Create the Session Store Schema

You create the session store schema so the MySQL database can store the session information.

Follow these steps:

1. Log in to the Policy Server host system.

2. Navigate to the following location:

   siteminder_home\db\tier2\MySQL.

   siteminder_home

   Specifies the Policy Server installation path.

3. Open the following file in a text editor:

   sm_mysql_ss.sql

4. Locate the following lines:

   ```
   DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
   CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
   ```

5. Replace each instance of 'databaseName' with the name of the database functioning as the session store.

6. Copy the contents of the entire file.

7. Paste the file contents into a query and execute the query.

   The session store schema is created.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can read and store session information.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select Session Server from the Database list.

   Data source settings become active.

3. Enter the name of the data source in the Data Source Information field.

   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.

4. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.

5. Specify the maximum number of database connections allocated to SiteMinder.

   Note: We recommend retaining the default for best performance.

6. Click Apply.

   The settings are saved.

7. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

8. Click OK.

   The Policy Server is configured to use the database as a session store.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.

3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Configure a MySQL User Store

Complete the following procedures to configure MySQL as a user store:

1. (Optional) Import the SiteMinder sample users.
2. Create a MySQL data source for SiteMinder
3. Configure the user directory connection.

More information:

Configure a MySQL Data Source for SiteMinder (see page 78)

Import the SiteMinder Sample Users

You configure a sample user directory to populate a database with sample users.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to *siteminder_home*\db\tier2\MySQL.

   siteminder_home

   Specifies the Policy Server installation path.
3. Open the following file in a text editor:

   smsampleusers_mysql.sql
4. Locate the following lines:

   ```
   DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
   CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
   ```
5. Replace each instance of 'databaseName' with the name of the database functioning as the sample user store.

   Example: If the name of the database is smsampleuserstore, the required update appears as follows:

   ```
   DROP FUNCTION IF EXISTS `smsampleuserstore`.`getdate` $$
   CREATE FUNCTION `smsampleuserstore`.`getdate` () RETURNS DATE
   ```
6. Copy the contents of the entire file.
7. Paste the file contents into a query and execute the query.

   Note: For more information about executing a query, see the MySQL documentation.

   The user store is populated with the sample users.

Configure MySQL Server Directory Connections

To configure a connection from the Policy Server to a MySQL Server user store, create a new User Directory object.

To configure a connection from the Policy Server to a MySQL Server user store

1. Click Infrastructure, Directory.
2. Click User Directory, Create User Directory.

   The Create User Directory pane opens.

   Note: You can specify user directory properties on this pane. For more information on the fields, settings, and options, click Help.

3. Type the name and a description of the new User Directory object in the fields on the General group box.
4. Select ODBC from the Namespace list, and type the data source name in the Data Source field on the Directory Setup group box.
5. Select the Require Credentials check box, and type the full DN and password of the administrator in the fields on the Administrator Credentials group box.
6. Select a scheme from the SQL Query Scheme list on the SQL Query Scheme group box.
7. (Optional) Complete the fields on the User Attributes group box.
   a. Type the Universal ID in the Universal ID field.

      Attribute type: string

   b. Type the flag that tracks disabled users in the Disabled Flag field.

      Attribute type: string

   c. Type the location of user passwords in the Password field.

      Attribute type: binary

   d. Type the location of user password history in the Password Data field.

      Attribute type: binary

      Note: This attribute is required by Password Services.

   e. Type the user's anonymous ID in the Anonymous ID field.

      Attribute type: string

   f. Leave the Email field blank.

      Note: The email feature is not implemented in the current version of SiteMinder.

   g. Type a response in the Challenge/Response field.

      Attribute type: string

      Note: This string is sent to the user after each challenge.
8. (Optional) Click Create on the Attribute Mapping List group box.

   The Create Attribute Mapping pane opens.

   Note: For more information about user attribute mapping, see the *Policy Configuration Guide*.
9. Click Submit.

   The Create User Directory task is submitted for processing.

Chapter 7: Novell eDirectory

This section contains the following topics:

Novell eDirectory as a Policy Store

Policy Servers installed on either Windows or UNIX systems can use Novell eDirectory as a policy store.

Before you begin, ensure that you have the following installed:

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

The following sections detail how to configure your directory server as a policy store.

Limitations of Policy Store Objects in Novell eDirectory

Consider the following items when working with Policy Store objects in a Novell eDirectory:

- Use a policy store root DN no longer than 15 characters.

  A Novell eDirectory DN cannot exceed 256 characters. Some SiteMinder objects can reach 241 characters. If your root DN is longer than 15 characters, some objects can exceed the 256–byte limit.

- When the policy store resides in Novell eDirectory, policy store objects cannot have names longer than 64 characters. eDirectory does not allow an attribute to be set to a value longer than 64. The limitation affects Certificate Maps particularly because they routinely have long names by design.

- The Policy Server does not support LDAP referrals for policy stores residing in Novell eDirectory.

Gather Directory Server Information

Configuring an LDAP directory server as a policy store or upgrading an existing policy store requires specific directory server information. Gather the following information before beginning. You can use the Policy Store Worksheets to record your values.

Note: Policy and data store worksheets are provided to help you gather and record information before configuring or upgrading a SiteMinder data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

Specifies the fully-qualified host name or the IP Address of the directory server.

Port information

(Optional) Specifies a non-standard port.

Default values: 636 (SSL) and 389 (non-SSL)

Administrative DN

Specifies the LDAP user name of a user who has privileges to create, read, modify, and delete objects in the LDAP tree underneath the policy store root object.

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

Specifies the distinguished name of the node in the LDAP tree where policy store objects are to be defined.

SSL client certificate

Specifies the pathname of the directory where the SSL client certificate database file resides.

Limit: SSL only

How to Configure the Policy Store

To configure Novell eDirectory as a policy store, complete the following procedures:

1. Edit the Policy Store Schema File
2. Edit the Novell XPS Schema File
3. Point the Policy Server to the Policy Store
4. Set the SiteMinder Super User Password

   Note: You do not have to complete this procedure if you already have a SiteMinder super user password.

5. Create the Policy Store Schema
6. Import the Default Policy Store Objects
7. Import the Policy Store Data Definitions
8. Refresh the LDAP Server
9. Restart the Policy Server
10. Prepare for the Administrative UI Registration

Edit the Policy Store Schema File

Edit the Novell policy store schema file to be sure that it contains your Novell server DN information. You edit the Novell policy store schema file from the Novell Client.

To edit the policy store schema file

1. Navigate to *policy_server_home*\bin on the Policy Server host system.

   policy_server_home

   Specifies the policy server installation path.

2. Run the following command:

   ```
   ldapsearch -hhost -pport -bcontainer -ssub -dAdminDN -wAdminPW
   objectclass=ncpServer dn
   ```

   Example:

   ```
   ldapsearch -h192.168.1.47 -p389 -bo=nwqa47container -ssub
   -dcn=admin,o=nwqa47container -wpassword objectclass=ncpServer dn
   ```

   The Novell server DN opens.

3. Open the Novell policy store schema file:

   policy_server_home\novell\Novell_ADD_SMR12sp3.ldif

4. Manually edit the open LDIF file by replacing every NCP_Server variable with the value that you found in step 2 for your Novell server DN.

   Example: If your Novell server DN value is cn=servername,o=servercontainer, replace every instance of NCP_Server with cn=servername,o=servercontainer.

5. Save and close the LDIF file.

   The Novell policy store schema file contains your Novell server DN information.

Edit the Novell XPS Schema File

Edit the Novell XPS schema file Novell.ldif so that it contains the correct information for your Novell server DN. You edit the Novell XPS schema file from the Novell Client.

To edit the Novell XPS schema file

1. Navigate to *policy_server_home*\bin or *policy_server_home*/bin on the machine where the Policy Server is installed.

   policy_server_home

   Specifies the policy server installation path.

2. Run the following command:

   ```
   ldapsearch -hhost -pport -bcontainer -ssub -dAdminDN -wAdminPW
   objectclass=ncpServer dn
   ```

   Example:

   ```
   ldapsearch -h192.168.1.47 -p389 -bo=nwqa47container -ssub
   -dcn=admin,o=nwqa47container -wpassword objectclass=ncpServer dn
   ```

   The Novell server DN opens.

3. Open the Novell XPS schema file:

   policy_server_home\xps\db\Novell.ldif

4. Manually edit the open XPS file by replacing every NCP_Server variable with the value that you found in step 2 for your Novell server DN.

   Example: If your Novell server DN value is cn=servername,o=servercontainer, replace every instance of NCP_Server with cn=servername,o=servercontainer.

5. Save and close the XPS file.

   The Novell XPS schema file contains your Novell server DN information.

Point the Policy Server to the Policy Store

You point the Policy Server to the policy store so the Policy Server can access the policy store.

Follow these steps:

1. Open the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut with Administrator permissions. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the Data tab.

3. Select the following value from the Database list:

   `Policy Store`

4. Select the following value from the Storage list:

   LDAP

5. Configure the following settings in the LDAP Policy Store group box.

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

   Note: You can click Help for a description of fields, controls, and their respective requirements.

6. Click Apply.
7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.
8. Select the following value from the Database list:

   `Key Store`

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    `Use Policy Store database`

11. Click OK.

Create the Policy Store Schema

You create the policy store schema so the directory server can function as a policy store and store SiteMinder objects. You use the smldapsetup tool to add the policy store schema.

To create the policy store schema

1. Open a command prompt and navigate to *policy_server_home*\bin or *policy_server_home*/bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   smldapsetup ldmod -v
   -fpolicy_server_home/novell/Novell_Add_SMR12sp3.ldif
   ```

   -v

   Turns on tracing and outputs error, warning, and comment messages.

   -f

   Specifies the name of the schema file that is supplied with r12.0 SP3.

3. Run the following command:

   ```
   smldapsetup ldmod -v -fpolicy_server_home\xps\db\Novell.ldif
   ```

   -f

   Specifies the path and name of the XPS schema file that is supplied with r12.0 SP3.

   The policy store schema is created for r12.0 SP3.

Set the SiteMinder Super User Password

The default SiteMinder administrator account is named siteminder. This account has maximum permissions. Set the password for this account so it can be used to manage the SiteMinder user interfaces and utilities until additional SiteMinder administrators can be created.

Note: The smreg utility is located at the top level of the Policy Server installation kit.

To set the super user password

1. Copy the smreg utility to *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   smreg -su 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.

   password

   Specifies the password for the default SiteMinder administrator.

Limits:

- The password must contain at least six (6) characters and cannot exceed 24 characters.
- The password cannot include an ampersand (&) or an asterisk (*).
- If the password contains a space, enclose the passphrase with quotation marks.

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

3. Delete the smreg utility from *policy_server_home*\bin. Deleting smreg prevents someone from changing the password without knowing the previous one.

   The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day–to–day operations. Use the default super user to:

- Import the default policy store objects.
- Access the FSS Administrative UI and Administrative UI for the first–time. We recommend creating another administrator with super user permissions.

More information:

Locate the Installation Media (see page 213)

Import the Default Policy Store Objects

Importing the default policy store objects sets up the policy store for use with the Administrative UI. The default policy store objects are required to store policy information in the policy store.

Note: If you have installed the Policy Server in FIPS-only mode, ensure you use the -cf argument when importing the default policy store objects.

To import the default policy store objects

1. Run the following command:

   ```
   smobjimport -ipolicy_server_home\db\smdif\smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

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

   Windows example: smobjimport
   ```
   -i"C:\Program Files\CA\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
   ```

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder super user account.

Default: siteminder

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder super user account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-cf

(Optional) Imports sensitive data using FIPS-compatible cryptography.

Note: This argument is only required if the Policy Server is operating in FIPS-only mode.

smobjimport imports the policy store objects. The objects are automatically imported to the appropriate locations.

2. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder super user account.

Default: siteminder

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

smobjimport imports the policy store objects. These objects are automatically imported to the appropriate locations.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for more information about licensing.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Refresh the LDAP Server

You refresh the LDAP server to help ensure that the changes take effect on Novell eDirectory. You use the Novell Client to refresh the LDAP server.

To refresh the LDAP Server

1. Open ConsoleOne.
2. Double-click LDAP server from the directory tree.
3. Click Refresh LDAP Server Now.

   The LDAP server is refreshed.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.

3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the SiteMinder environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually.

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   Specifies the password for the default SiteMinder super user account (siteminder).

   Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

   -adminui–setup

   Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

-t *timeout*

(Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect SiteMinder administrator credentials when logging into the Administrative UI for the first–time

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.0 SP3 policy store. You can upgrade an existing policy store to r12.0 SP3.

Complete the following procedures to upgrade a supported LDAP or relational database policy store:

1. Edit the Novell XPS Schema File.
2. Extend the Policy Store Schema.

   Note: The existing r6.x policy store schema has not changed. The r12.0 SP3 migration requires that you extend the policy store schema for policy store for objects that r12.0 SP3 requires.

3. Import the Base Policy Store Objects.
4. Import the Policy Store Data Definitions.

Note: If you are upgrading a directory server or database that is listed in the Support Matrix, but not in this guide, see one of the following guides:

- *Policy Server Configuration Guide*
- *Policy Server Installation Guide*
- *Upgrade Guide*

Edit the Novell XPS Schema File

Edit the Novell XPS schema file Novell.ldif so that it contains the correct information for your Novell server DN. You edit the Novell XPS schema file from the Novell Client.

To edit the Novell XPS schema file

1. Navigate to *policy_server_home*\bin or *policy_server_home*/bin on the machine where the Policy Server is installed.

   policy_server_home

   Specifies the policy server installation path.

2. Run the following command:

   ```
   ldapsearch -hhost -pport -bcontainer -ssub -dAdminDN -wAdminPW
   objectclass=ncpServer dn
   ```

   Example:

   ```
   ldapsearch -h192.168.1.47 -p389 -bo=nwqa47container -ssub
   -dcn=admin,o=nwqa47container -wpassword objectclass=ncpServer dn
   ```

   The Novell server DN opens.

3. Open the Novell XPS schema file:

   policy_server_home\xps\db\Novell.ldif

4. Manually edit the open XPS file by replacing every NCP_Server variable with the value that you found in step 2 for your Novell server DN.

   Example: If your Novell server DN value is cn=servername,o=servercontainer, replace every instance of NCP_Server with cn=servername,o=servercontainer.

5. Save and close the XPS file.

   The Novell XPS schema file contains your Novell server DN information.

Extend the Novell Policy Store Schema

You can extend a Novell 6.0 policy store schema to include the objects introduced by r12.0 SP3. There are no changes to the existing 6.0 policy store schema or data.

To extend the Novell policy store schema

Run the following command:

```
smldapsetup ldmod -fpolicy_server_home/xps/db/Novell.ldif
```

-f

Specifies the path and name of the XPS schema file that is supplied with r12.0 SP3.

policy_server_home

Specifies the Policy Server installation path.

The policy store schema is extended to include the objects introduced by r12.0 SP3.

Note: You can now import the policy store data definitions.

Import the Base Policy Store Objects

Importing the default SiteMinder objects upgrades the policy store for use with the Administrative UI. The default SiteMinder objects are required to store policy information in the 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.

To import the base policy store objects

1. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

Specifies the Policy Server installation path.

upgrade_smdif_file_name

Specifies the name of the import file:

- **r6.0 to r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r6.0 SP1 to r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r6.0 SP2 to r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r6.0 SP3 to r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r6.0 SP4 to r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r6.0 SP5 to r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r6.0 SP6 to r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-dsiteminder_super_user_name

Specifies the name of the SiteMinder administrator account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder administrator account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.0 SP3.

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

Windows example: smobjimport

```
-i"C:\Program Files\CA\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

The base policy store objects are imported.

2. Run the following command:

Important! Do not re-import ampolicy.smdif if it has been previously imported into the policy store.

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-policy_server_home

Specifies the path and name of the import file.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder administrator account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder administrator account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for licensing information.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Chapter 8: Oracle Internet Directory Server

This section contains the following topics:

Oracle Internet Directory as a Policy Store

Policy Servers installed on Windows and UNIX systems can use an Oracle Internet Directory (OID) as a policy store. The following sections detail how to configure an OID as a policy store.

Gather Directory Server Information

Configuring an LDAP directory server as a policy store or upgrading an existing policy store requires specific directory server information. Gather the following information before beginning. You can use the Policy Store Worksheets to record your values.

Note: Policy and data store worksheets are provided to help you gather and record information before configuring or upgrading a SiteMinder data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

Specifies the fully-qualified host name or the IP Address of the directory server.

Port information

(Optional) Specifies a non-standard port.

Default values: 636 (SSL) and 389 (non-SSL)

Administrative DN

Specifies the LDAP user name of a user who has privileges to create, read, modify, and delete objects in the LDAP tree underneath the policy store root object.

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

Specifies the distinguished name of the node in the LDAP tree where policy store objects are to be defined.

SSL client certificate

Specifies the pathname of the directory where the SSL client certificate database file resides.

Limit: SSL only

How to Configure the Policy Server

To configure OID as a policy store, complete the following procedures:

1. Configure a domain in Oracle Internet Directory.
2. Point the Policy Server to the directory server.
3. Create the policy store schema.
4. Set the SiteMinder super user password.

   Note: You do not have to complete this procedure if you already have a SiteMinder super user password.
5. Import the default policy store objects.
6. Import the policy store data definitions.
7. Restart the Policy Server.
8. Prepare for the Administrative UI registration.

Configure a Domain in Oracle Internet Directory

To configure an OID as a policy store, first create a domain in OID.

To configure a domain in Oracle Internet Directory

1. Open Oracle Data Manager (ODM).
2. Right-click Entry Management, and select Create.

   The Distinguished Name dialog opens.
3. Enter **dc=dcbok** for the Distinguished Name value.
4. Enter **dc** for the dc value.
5. Create an organizational unit.
6. Select an organizational unit.

7. Enter **ou=bok,dc=dcbok** for the Distinguished Name value.
8. Enter **bok** for the ou value.

   The OID domain is configured.

Point the Policy Server to the Directory Server

You point the Policy Server to the LDAP directory server so that the Policy Server has the necessary system information and administrative privileges to read and write information to the policy store.

To point the Policy Server to the directory server

1. Run the following command from the Policy Server host system:

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

   -h*host*

   Specifies the IP Address of the LDAP server host system.

   -p*port*

   Specifies the port on which the LDAP server is listening.

   -d*AdminDN*

   Specifies the name of an LDAP user with privileges to create LDAP schema in the LDAP directory server.

   ADAM or 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}

   -w*AdminPW*

   Specifies the password for an LDAP user with privileges to create LDAP schema in the LDAP directory server.

   -r*root*

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

   ADAM or AD LDS: Specifies the existing root DN location of the application partition in the ADAM or AD LDS server where you want to put the policy store schema data.

   -ssl1|0

   Specifies an SSL connection.

   Limits: 0=no | 1=yes

   Default: 0

-c*cert*

(Only required if the ssl value is 1) Specifies the path to the directory where the SSL client certificate database file, cert7.db, exists.

The correct configuration of the LDAP policy store connection parameters is verified.

2. Run the following command:

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

The connection to the LDAP directory server is tested and the server is configured as a SiteMinder policy store.

Create the Policy Store Schema

You can create the policy store schema to include the objects introduced by r12.0 SP3.

To create the policy store schema

1. Run the following command:

```
smldapsetup ldgen -ffile_name.ldif
```

-f*file_name*

Specifies the name of the schema file that you are creating.

2. Run the following command:

```
smldapsetup ldmod -ffile_name.ldif
```

-f*file_name*

Specifies the name of the schema file that you created.

3. Run the following command:

```
ldapmodify -hhost -pport -dAdminDN -wAdminPW
```

```
-c -fsiteminder_home/xps/db/tier2/oid_10g/OID_10g.ldif
-Z -Pcert
```

Note: Although the schema file is version–specific, you can use this file to import the policy store schema for all supported versions of OID.

-h*host*

Specifies the IP address of the LDAP directory server.

Example: 123.123.12.12

-p*port*

Specifies the port number of the LDAP directory server.

Example: 3500

-d*AdminDN*

Specifies the name of the LDAP user who has the privileges needed to create a new LDAP schema in the LDAP directory server.

-w*AdminPW*

Specifies the password of the administrator specified by the -d option.

-c

Specifies continuous mode (do not stop on errors).

-f*siteminder_home*

Specifies the Policy Server installation path.

-Z

Specifies an SSL-encrypted connection.

-P*cert*

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

Example:

If cert7.db exists in app/siteminder/ssl, specify:

```
-Papp/siteminder/ssl
```

The policy store schema is created for r12.0 SP3.

Set the SiteMinder Super User Password

The default SiteMinder administrator account is named siteminder. This account has maximum permissions. Set the password for this account so it can be used to manage the SiteMinder user interfaces and utilities until additional SiteMinder administrators can be created.

Note: The smreg utility is located at the top level of the Policy Server installation kit.

To set the super user password

1. Copy the smreg utility to *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   `smreg -su 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.

   password

   Specifies the password for the default SiteMinder administrator.

   Limits:

   - The password must contain at least six (6) characters and cannot exceed 24 characters.
   - The password cannot include an ampersand (&) or an asterisk (*).
   - If the password contains a space, enclose the passphrase with quotation marks.

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

3. Delete the smreg utility from *policy_server_home*\bin. Deleting smreg prevents someone from changing the password without knowing the previous one.

   The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day–to–day operations. Use the default super user to:

- Import the default policy store objects.
- Access the FSS Administrative UI and Administrative UI for the first–time. We recommend creating another administrator with super user permissions.

More information:

Locate the Installation Media (see page 213)

Import the Default Policy Store Objects

Importing the default policy store objects sets up the policy store for use with the Administrative UI. The default policy store objects are required to store policy information in the policy store.

Note: If you have installed the Policy Server in FIPS-only mode, ensure you use the -cf argument when importing the default policy store objects.

To import the default policy store objects

1. Run the following command:

   ```
   smobjimport -ipolicy_server_home\db\smdif\smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

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

   Windows example: smobjimport
   ```
   -i"C:\Program Files\CA\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
   ```

   policy_server_home

   Specifies the Policy Server installation path.

   -d*siteminder_super_user_name*

   Specifies the name of the SiteMinder super user account.

   Default: siteminder

   -w*siteminder_super_user_password*

   Specifies the password for the SiteMinder super user account.

   -v

   Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

   Default value: stdout

   -cf

   (Optional) Imports sensitive data using FIPS-compatible cryptography.

   Note: This argument is only required if the Policy Server is operating in FIPS-only mode.

   smobjimport imports the policy store objects. The objects are automatically imported to the appropriate locations.

2. Run the following command:

   ```
   smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
   ```

   policy_server_home

   Specifies the Policy Server installation path.

   -d*siteminder_super_user_name*

   Specifies the name of the SiteMinder super user account.

   Default: siteminder

   -w*siteminder_super_user_password*

   Specifies the password for the SiteMinder super user account.

   -f

   Overrides duplicate objects.

   -v

   Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

   Default value: stdout

   -l

   Creates a log file.

   -c

   Indicates that the smdif input file contains unencrypted data.

   smobjimport imports the policy store objects. These objects are automatically imported to the appropriate locations.

   Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for more information about licensing.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.
4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.
5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the SiteMinder environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually.

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

passphrase

Specifies the password for the default SiteMinder super user account (siteminder).

Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

-adminui–setup

Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

-t *timeout*

(Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect SiteMinder administrator credentials when logging into the Administrative UI for the first–time

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.0 SP3 policy store. You can upgrade an existing policy store to r12.0 SP3.

Complete the following procedures to upgrade the policy store:

1. Extend the policy store schema.

   Note: The existing r6.x policy store schema has not changed. The r12.0 SP3 migration requires that you extend the policy store schema for policy store for objects that r12.0 SP3 requires.

2. Import the base policy store objects.
3. Import the Policy Store Data Definitions.

Note: If you are upgrading a directory server or database that is listed in the Support Matrix, but not in this guide, see the *SiteMinder Upgrade Guide.*

Extend the Oracle Internet Directory Policy Store Schema

You can extend a 6.x policy store schema to include the objects introduced by r12.0 SP3. There are no changes to the existing 6.x policy store schema.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command:

```
ldapmodify -hhost -pport -dAdminDN -wAdminPW
-c -fsiteminder_home/xps/db/tier2/oid_10g/OID_10g.ldif
-Z -Pcert
```

-h*host*

Specifies the IP address of the LDAP directory server.

Example: 123.123.12.12

-p*port*

Specifies the port number of the LDAP directory server.

Example: 3500

-d*AdminDN*

Specifies the name of the LDAP user who has the privileges needed to create a new LDAP schema in the LDAP directory server.

-w*AdminPW*

Specifies the password of the administrator specified by the -d option.

-c

Specifies continuous mode (do not stop on errors).

-f*siteminder_home*

Specifies the Policy Server installation path.

-Z

Specifies an SSL-encrypted connection.

-P*cert*

Specifies 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:

```
-Papp/siteminder/ssl
```

The policy store schema is extended to include the objects introduced by r12.0 SP3.

Import the Base Policy Store Objects

Importing the default SiteMinder objects upgrades the policy store for use with the Administrative UI. The default SiteMinder objects are required to store policy information in the 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.

To import the base policy store objects

1. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

Specifies the Policy Server installation path.

upgrade_smdif_file_name

Specifies the name of the import file:

- **r6.0 to r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r6.0 SP1 to r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r6.0 SP2 to r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r6.0 SP3 to r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r6.0 SP4 to r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r6.0 SP5 to r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r6.0 SP6 to r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.0 SP3.

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

Windows example: smobjimport
`-i"C:\Program Files\CA\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

The base policy store objects are imported.

2. Run the following command:

Important! Do not re-import ampolicy.smdif if it has been previously imported into the policy store.

`smobjimport -i`*`policy_server_home`*`\db\smdif\ampolicy.smdif -d`*`siteminder_super_user_name`* `-w`*`siteminder_super_user_password`* `-f -v -l -c`

-policy_server_home

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for licensing information.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Chapter 9: OpenLDAP Server

This section contains the following topics:

How to Configure the Slapd Configuration File

An OpenLDAP directory server requires additional configuration before you can use it as a policy store. The following process lists the configuration steps:

1. Specify the SiteMinder schema files.
2. Specify policy store indexing.
3. Enable user authentication.
4. Specify database directives.
5. Support Client-Side Sorting
6. Test the configuration file.
7. Restart the OpenLDAP server.

Specify the SiteMinder Schema Files

Specifying the schema files in the include section of the slapd configuration file (slapd.conf) ensures that the slapd process (the LDAP Directory Server daemon) reads the additional configuration information. The included files must follow the correct slapd configuration file format.

To specify the schema files

1. Copy the following schema files to the schema folder in the OpenLDAP installation directory:
   - *siteminder_home*/db/tier2/OpenLDAP/openldap_attribute.schema
   - *siteminder_home*/db/tier2/OpenLDAP/openldap_object.schema

- *siteminder_home*/xps/db/tier2/openldap/openldap_attribute_XPS.schema
- *siteminder_home*/xps/db/tier2/openldap/openldap_object_XPS.schema

siteminder_home

Specifies the Policy Server installation path.

2. Type the following in the include section of the slapd configuration file:

```
....
.....
include /usr/local/etc/openldap/schema/openldap_attribute.schema
include /usr/local/etc/openldap/schema/openldap_object.schema
include /usr/local/etc/openldap/schema/openldap_attribute_XPS.schema
include /usr/local/etc/openldap/schema/openldap_object_XPS.schema
```

Note: This procedure assumes that the OpenLDAP server is located at /usr/local/etc/openldap and that the schema files are located in the schema subdirectory.

The policy store schema is created for r12.0 SP3.

Specify Policy Store Indexing

Specify indexing in the slapd.conf file to use OpenLDAP as a policy store.

Follow these steps:

1. Stop the slapd instance.
2. Open the slapd.conf file with a text editor.
3. Locate the following lines:

```
# Indices to maintain
index   objectClass     eq
```

4. Insert a new line in the file, and then add the following lines:

```
index smAdminOID4 pres,eq
index smAuthDirOID4 pres,eq
index smAzDirOID4 pres,eq
index smcertmapOID4 pres,eq
index smIsRadius4 pres,eq
index smIsAffiliate4 pres,eq
index smParentRealmOID4 pres,eq
index smPasswordPolicyOID4 pres,eq
index smAgentGroupOID4 pres,eq
index smKeyManagementOID4 pres,eq
index smAgentOID4 pres,eq
index smAgentKeyOID4 pres,eq
index smRootConfigOID4 pres,eq
index smAGAgents4 pres,eq
index smDomainAdminOIDs4 pres,eq
index smDomainOID4 pres,eq
index smvariableoid5 pres,eq
index smNestedVariableOIDs5 pres,eq
index smvariabletypeoid5 pres,eq
index smActiveExprOID5 pres,eq
index smDomainUDs4 pres,eq
index smVariableOIDs5 pres,eq
index smusractiveexproid5 pres,eq
index smPropertyOID5 pres,eq
index smPropertySectionOID5 pres,eq
index smPropertyCollectionOID5 pres,eq
index smFilterClass4 pres,eq
index smTaggedStringOID5 pres,eq
index smNoMatch5 pres,eq
index smTrustedHostOID5 pres,eq
index smIs4xTrustedHost5 pres,eq
index smDomainMode5 pres,eq
# index smImsEnvironmentOIDs5 pres,eq
index smSecretRolloverEnabled6 pres,eq
index smSecretGenTime6 pres,eq
```

```
index smSecretUsedTime6 pres,eq
index smSharedSecretPolicyOID6 pres,eq
index smFilterPath4 pres,eq
index smPolicyLinkOID4 pres,eq
index smIPAddress4 pres,eq
index smRealmOID4 pres,eq
index smSelfRegOID4 pres,eq
index smAzUserDirOID4 pres,eq
index smResourceType4  pres,eq
index smResponseAttrOID4 pres,eq
index smResponseGroupOID4  pres,eq
index smResponseOID4     pres,eq
index smRGResponses4 pres,eq
index smRGRules4     pres,eq
index smRuleGroupOID4 pres,eq
index smRuleOID4   pres,eq
index smSchemeOID4 pres,eq
index smisTemplate4  pres,eq
index smisUsedbyAdmin4 pres,eq
index smSchemeType4   pres,eq
index smUserDirectoryOID4 pres,eq
index smODBCQueryOID4 pres,eq
index smUserPolicyOID4 pres,eq
index smAgentTypeAttrOID4 pres,eq
index smAgentTypeOID4 pres,eq
index smAgentTyperfcid4 pres,eq
index smAgentTypeType4 pres,eq
index smAgentCommandOID4 pres,eq
index smTimeStamp4     pres,eq
index smServerCommandOID4 pres,eq
index smAuthAzMapOID4 pres,eq
index xpsParameter pres,eq
index xpsValue  pres,eq
index xpsNumber pres,eq
index xpsCategory pres,eq
index xpsGUID pres,eq
index xpsSortKey pres,eq
index xpsIndexedObject pres,eq
```

5. Save the file and close the text editor.
6. Run the following command:

   ```
   slapindex -f slapd.conf
   ```

7. Restart the slapd instance.

   The policy store indexing for OpenLDAP is specified.

Enable User Authentication

Enabling user authentication ensures that you can protect resources with a supported authentication scheme.

To enable user authentication, add the following to the slapd configuration file:

```
access to attrs=userpassword
by self write
by anonymous auth
by * none
```

Specify Database Directives

The slapd configuration file requires values for additional database directives.

To specify the directives, edit the following:

database

Specify any supported backend type.

Example: bdb

suffix

Specify the database suffix.

Example: dc=example,dc=com

rootdn

Specify the DN of root.

Example: cn=Manager,dc=example,dc=com

rootpw

Specify the password to root.

directory

Specify the path of the database directory.

Example: /usr/local/var/openldap-data

Note: The database directory must exist prior to running slapd and should only be accessible to the slapd process.

Support Client-Side Sorting

OpenLDAP is the only supported LDAP directory that does not support server-side sorting. Instead, OpenLDAP requires that all sorting be performed on the client side. To accomplish this, all XPS objects are retrieved at start-up using server-side paging.

To support client-side sorting, the OpenLDAP directory administrator must configure the following settings in the slapd.conf file:

- Enable reading of the Root DSE.

  This setting allows the XPS client to read the OpenLDAP directory's type and capabilities.

- Set the maximum number of entries that can be returned from a search operation >= 500.

  This setting accommodates XPS objects which are retrieved in increments of 500 by server-side paging.

- Allow a simple V2 bind.

  This setting allows smconsole to test the LDAP connection using a simple V2 bind.

To support client-side sorting

1. Add the following lines to the slapd.conf file:

   ```
   access to *
   by users read
   by anonymous read
   access to dn.base=ACL by users read
   ```

   ACL

   Specifies an access control list or list of permissions.

   Note: For more information on how to specify the ACL, see http://www.openldap.org/doc/admin24/access-control.html.

2. Verify that the value specified by the sizelimit directive in the slapd.conf file >= 500:

   ```
   sizelimit 500
   ```

   Note: The default sizelimit value is 500. For more information, see http://www.openldap.org/doc/admin24/slapdconfig.html.

3. Add the following line to the slapd.conf file:

   ```
   allow bind_v2
   ```

The slapd.conf file is configured to support client-side sorting.

Test the Configuration File

Testing the configuration file ensures that it is correctly formatted.

To test the configuration file

1. Change the directory to the OpenLDAP server directory.
2. Run the following command:

   ```
   ./slapd
   ```

   Note: Unless you specified a debugging level, including level 0, slapd automatically forks, detaches itself from its controlling terminal, and runs in the background.
3. Run the following command:

   ```
   ./slapd -Tt
   ```

   The slapd configuration file is tested.

Restart the OpenLDAP Server

Restarting the OpenLDAP directory server loads the SiteMinder schema. The Policy Server requires that the SiteMinder schema is loaded before you can use the directory server as a policy store.

To restart the directory server

1. Stop the directory server using the following command:

   ```
   kill -INT 'cat path_of_var/run_directory/slapd.pid`
   ```

   path_of_var/run_directory

   Specifies the path of the database directory.

   Example: kill -INT `cat /usr/local/var/run/slapd.pid`
2. Start the directory server using the following command:

   ```
   ./slapd
   ```

How to Create the Database

The following process lists the steps for creating the directory server database for the policy store:

1. Create the base tree structure.
2. Add entries.

Create the Base Tree Structure

You can create a base tree structure in the policy store.

Specify the following under the root DN:

```
ou=Netegrity,ou=SiteMinder,ou=PolicySvr4,ou=XPS
```

The base tree structure is created in the policy store.

Add Entries

Add entries to the directory server so that SiteMinder has the necessary organization and organizational role information.

To add database entries

1. Create an LDIF file.

   Example: The following example contains an organization entry and an organizational role entry for the entries.ldif.

```
# CA, example.com
dn: ou=Netegrity,dc= example,dc=com
ou: CA
objectClass: organizationalUnit
objectClass: top


# SiteMinder, CA, example.com
dn: ou=SiteMinder,ou=CA,dc= example,dc=com
ou: SiteMinder
objectClass: organizationalUnit
objectClass: top


# PolicySvr4, SiteMinder, CA, example.com
dn: ou=PolicySvr4,ou=SiteMinder,ou=CA,dc= example,dc=com
ou: PolicySvr4
objectClass: organizationalUnit
objectClass: top


# XPS, policysvr4, siteminder, ca, example.com
dn: ou=XPS,ou=policysvr4,ou=siteminder,ou=ca,dc= example,dc=com
ou: XPS
objectClass: organizationalUnit
objectClass: top
```

2. Use the following command to add the entries.

```
ldapadd -f <file_name.ldif> -D "cn=Manager,dc=example,dc=com"
-w<password>
```

How to Configure the Directory Server as a Policy Store

You can use the Policy Server Management Console and the Administrative UI to configure the directory server as a policy store. The following process lists the steps for using the directory server as a policy store:

1. Create the Policy Store
2. Connect to the Policy Store

Point the Policy Server to the Directory Server

You point the Policy Server to the LDAP directory server so that the Policy Server has the necessary system information and administrative privileges to read and write information to the policy store.

To point the Policy Server to the directory server

1. Run the following command from the Policy Server host system:

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

-h*host*

Specifies the IP Address of the LDAP server host system.

-p*port*

Specifies the port on which the LDAP server is listening.

-d*AdminDN*

Specifies the name of an LDAP user with privileges to create LDAP schema in the LDAP directory server.

ADAM or 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}

-w*AdminPW*

Specifies the password for an LDAP user with privileges to create LDAP schema in the LDAP directory server.

-rroot

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

ADAM or AD LDS: Specifies the existing root DN location of the application partition in the ADAM or AD LDS server where you want to put the policy store schema data.

-ssl1|0

Specifies an SSL connection.

Limits: 0=no | 1=yes

Default: 0

-ccert

(Only required if the ssl value is 1) Specifies the path to the directory where the SSL client certificate database file, cert7.db, exists.

The correct configuration of the LDAP policy store connection parameters is verified.

2. Run the following command:

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

The connection to the LDAP directory server is tested and the server is configured as a SiteMinder policy store.

Create the Policy Store

To configure an OpenLDAP directory server as a policy store, import the base policy store data.

To create the policy store

1. Start the Policy Server Management Console.
2. Click the Data tab.
3. Type the root DN in the Root DN field, and click OK.

   The root DN is saved.
4. Go to policy_server_home/bin.

   policy_server_home

   Specifies the Policy Server installation path.
5. Run the following command:

```
smreg -su adminPW
```

The administrator's password is saved.

6. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\smpolicy.smdif
-dsiteminder_super_user_name  -wsiteminder_super_user_password -v
```

-i

Specifies the name of the import file.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder Super User account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder Super User account.

-v

Turns on tracing and outputs error, warning, and comment messages.

The base policy store data is imported from the file smpolicy.smdif.

7. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder Super User account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder Super User account.

-f

Overrides duplicate objects

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

smobjimport imports the policy store objects. These objects are automatically imported to the appropriate locations.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for more information on licensing.

Note: You can now import policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the SiteMinder environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually.

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   Specifies the password for the default SiteMinder super user account (siteminder).

   Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

   -adminui–setup

   Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

-t *timeout*

(Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect SiteMinder administrator credentials when logging into the Administrative UI for the first–time

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

How to Configure the Directory Sever as a User Store

You can use the OpenLDAP directory server as a user store. The following process lists the steps for using the directory server as a user store:

1. Create a User Store
2. Connect to the User Store

Create a User Store

You can use an OpenLDAP directory server as a user store

To create a user store

1. Use an LDIF file to create ou=People under the root DN.
2. Create users under the organizational unit.

Configure a Connection from the Policy Server to an OpenLDAP User Store

To configure a connection from the Policy Server to an OpenLDAP user store, create a new User Directory object.

To configure a connection from the Policy Server to an OpenLDAP user store

1. Click Infrastructure, Directory.

2. Click User Directory, Create User Directory.

   The Create User Directory pane opens.

   Note: You can specify user directory properties on this pane. For more information on the fields, settings, and options, click Help.

3. Type the name and a description of the new User Directory object in the fields on the General group box.

4. Verify that LDAP is selected from the Namespace list, and type the IP address and port number in the Server field on the Directory Setup group box.

   Note: When the Policy Server is operating in FIPs mode and the User Directory connection is a secure SSL connection, the certificates used by the Policy Server and the user store must be FIPs compliant.

5. Select the Require Credentials check box, and type the full DN and password of the administrator in the fields on the Administrator Credentials group box.

6. Type the root node and search parameters in the fields on the LDAP Search group box.

7. Type a beginning text string and an ending text string in the fields on the LDAP User DN Lookup group box.

   Note: The beginning text string, username, and ending text string are combined to create a string that is used for searching the User Directory tree.

8. (Optional) Complete the fields on the User Attributes group box.

   a. Type the Universal ID in the Universal ID field.

      Attribute type: string

   b. Type the flag that tracks disabled users in the Disabled Flag field.

      Attribute type: string

   c. Type the location of user passwords in the Password field.

      Attribute type: binary

   d. Type the location of user password history in the Password Data field.

      Attribute type: binary

      Note: This attribute is required by Password Services.

   e. Type the user's anonymous ID in the Anonymous ID field.

      Attribute type: string

   f. Leave the Email field blank.

      Note: The email feature is not implemented in the current version of SiteMinder.

g. Type a response in the Challenge/Response field.

Attribute type: string

Note: This string is sent to the user after each challenge.

9. (Optional) Click Create on the Attribute Mapping List group box.

The Create Attribute Mapping pane opens.

Note: For more information about user attribute mapping, see the *Policy Server Configuration Guide*.

10. Click Submit.

The Create User Directory task is submitted for processing.

More information:

How to Configure an LDAP User Directory Connection over SSL (see page 203)

Configure SSL for a Policy Store

Policy stores support Secure Socket Layers (SSL). You configure the policy store for SSL from the Policy Server Management Console.

The following procedure assumes:

- The OpenLDAP environment is configured for SSL.
- The certificate Authority's (CA) root certificate (cacert.pem) is installed on the Netscape cert7.db database on each machine that will use SSL to communicate with the directory server.
- A key3.db file has been created.

  Note: SiteMinder requires that the root certificate adheres to the Netscape file format. You cannot use Microsoft IE to install the certificate.

To configure SSL for a policy store

1. Start the Policy Server Management Console.
2. Click the Data tab.

   The Data tab opens.
3. Select Use SSL.

4. Enter the absolute path to cert7.db in the Netscape Certificate Database File field.

   Note: Consider the following:

   - A known limitation requires that the file name be included in the path. You can resolve this issue after providing a complete absolute path. Fix the path by removing the last substring (cert7.db) in the CertDbPath variable in the registry.
   - The key3.db file must also be in the same directory as the cert7.db file.

5. Click OK.

   SSL is enabled for the policy store.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.0 SP3 policy store. You can upgrade an existing policy store to r12.0 SP3.

Complete the following procedures to upgrade the policy store:

1. Extend the policy store schema.

   Note: The existing r6.x policy store schema has not changed. The r12.0 SP3 migration requires that you extend the policy store schema for policy store for objects that r12.0 SP3 requires.

2. Import the base policy store objects.
3. Import the Policy Store Data Definitions.

Note: If you are upgrading a directory server or database that is listed in the Support Matrix, but not in this guide, see the *SiteMinder Upgrade Guide.*

Extend the OpenLDAP Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.0 SP3 by specifying the schema files in the include section of the slapd configuration file (slapd.conf). This ensures that the slapd process (the LDAP Directory Server daemon) reads the additional configuration information. The included files must follow the correct slapd configuration file format. There are no changes to the existing 6.x policy store schema.

Follow these steps:

1. Add the following root node under ou=Netegrity,ou=SiteMinder,ou=PolicySvr4:

   ou=XPS

2. Log in to the Policy Server host system.

3. Navigate to *siteminder_home*/xps/db/tier2/openldap.

   siteminder_home

   Specifies the Policy Server installation path.

4. Copy the following schema files to the schema folder in the OpenLDAP installation directory:

   - openldap_attribute_XPS.schema
   - openldap_object_XPS.schema

5. Type the following in the include section of the slapd configuration file:

```
....
.....
include /usr/local/etc/openldap/schema/openldap_attribute_XPS.schema
include /usr/local/etc/openldap/schema/openldap_object_XPS.schema
```

   Note: This procedure assumes that the OpenLDAP server is located at /usr/local/etc/openldap and that the schema files are located in the schema subdirectory.

   The policy store schema is extended to include the objects introduced by r12.0 SP3.

Import the Base Policy Store Objects

Importing the default SiteMinder objects upgrades the policy store for use with the Administrative UI. The default SiteMinder objects are required to store policy information in the 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.

To import the base policy store objects

1. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

   policy_server_home

   Specifies the Policy Server installation path.

   upgrade_smdif_file_name

   Specifies the name of the import file:

   - **r6.0 to r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
   - **r6.0 SP1 to r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif

- **r6.0 SP2 to r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r6.0 SP3 to r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r6.0 SP4 to r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r6.0 SP5 to r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r6.0 SP6 to r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.0 SP3.

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

Windows example: smobjimport

```
-i"C:\Program Files\CA\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

The base policy store objects are imported.

2. Run the following command:

Important! Do not re-import ampolicy.smdif if it has been previously imported into the policy store.

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-policy_server_home

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for licensing information.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.

3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Troubleshooting OpenLDAP

For information on troubleshooting OpenLDAP, see the following topics:

- Cyrus SASL Installation
- Berkeley Database Version Mismatch Errors
- Building and Installing openSSL

Cyrus SASL Installation

Symptom:

When I install Cyrus SASL, I am experiencing compiling problems.

Solution:

More information on troubleshooting Cyrus SASL installation problems can be found at:

http://marc.theaimsgroup.com/?l=cyrus-sasl&m=111835942621184&w=2

Berkeley Database Version Mismatch Errors

Symptom:

I am receiving Berkeley database version mismatch errors.

Solution:

More information on troubleshooting Berkeley database version mismatch errors can be found at:

http://www.openldap.org/faq/data/cache/1113.html

Building and Installing openSSL

Symptom:

I am having problems building and installing openSSL.

Solution:

More information on building and installing openSSL can be found at:

http://www.proscrutiny.com/howtos/OpenLDAP.html#confssl-co

Chapter 10: Red Hat Directory Server

This section contains the following topics:

Configure a Connection from the Policy Server to a Red Hat User Store

To configure a connection from the Policy Server to a Red Hat user store, create a User Directory object in the SiteMinder Administrative UI.

To configure a connection from the Policy Server to a Red Hat user store

1. Click Infrastructure, Directory.
2. Click User Directory, Create User Directory.

   The Create User Directory pane opens.

   Note: You can specify user directory properties on this pane. For more information about the fields, settings, and options, click Help.
3. Type the name and a description of the new User Directory object in the fields on the General group box.
4. Verify that LDAP is selected from the Namespace list, and type the IP address and port number in the Server field on the Directory Setup group box.
5. Select the Require Credentials check box, and type the full DN and password of the administrator in the fields on the Administrator Credentials group box.
6. Type the root node and search parameters in the fields on the LDAP Search group box.
7. Type a beginning text string and an ending text string in the fields on the LDAP User DN Lookup group box.

   Note: The beginning text string, username, and ending text string are concatenated to create a string that is used for searching the User Directory tree.
8. (Optional) Complete the fields on the User Attributes group box.
   a. Type the Universal ID in the Universal ID field.

      Attribute type: string

b. Type the flag that tracks disabled users in the Disabled Flag field.

Attribute type: string

c. Type the location of user passwords in the Password field.

Attribute type: binary

d. Type the location of user password history in the Password Data field.

Attribute type: binary

Note: Password Services requires this information.

e. Type the anonymous ID of the user in the Anonymous ID field.

Attribute type: string

f. Leave the Email field blank.

Note: The email feature is not implemented in the current version of SiteMinder.

g. Type a response in the Challenge/Response field.

Attribute type: string

Note: This string is sent to the user after each challenge.

9. (Optional) Click Create on the Attribute Mapping List group box.

The Create Attribute Mapping pane opens.

Note: For more information about user attribute mapping, see the *Policy Server Configuration Guide*.

10. Click Submit.

The Create User Directory task is submitted for processing.

How to Configure a Red Hat Directory Server as a Policy Store

Complete the following tasks to configure Red Hat Directory Server as a policy store:

1. Point the Policy Server to the policy store (Red Hat Directory Server).
2. Create the policy store schema in a Red Hat Directory Server.
3. Set the SiteMinder superuser password.
4. Import the default policy store objects.
5. Import the policy store data definitions.
6. Restart the Policy Server.
7. Prepare for the Administrative UI registration.

Point the Policy Server to the Policy Store

You point the Policy Server to the policy store so the Policy Server can access the policy store.

Follow these steps:

1. Open the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut with Administrator permissions. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the Data tab.
3. Select the following value from the Database list:

   `Policy Store`

4. Select the following value from the Storage list:

   LDAP

5. Configure the following settings in the LDAP Policy Store group box.
   - LDAP IP Address
   - Admin Username
   - Password
   - Confirm Password
   - DN

   Note: You can click Help for a description of fields, controls, and their respective requirements.

6. Click Apply.
7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.
8. Select the following value from the Database list:

   `Key Store`

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    `Use Policy Store database`

11. Click OK.

Create the Policy Store Schema in a Red Hat Directory Server

You can create the policy store schema in a Red Hat Directory Server.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command:
   `smldapsetup ldgen -f`*`schema_file`*

   schema_file

   Specifies the name of the LDIF file you are creating.

   An LDIF file is created using the policy store schema.
3. Run the following command:
   `smldapsetup ldmod -f`*`schema_file`*

   schema_file

   Specifies the name of the LDIF file you created.

   The policy store schema is imported.
4. Do the following:
   a. Restart the directory server. Restarting the directory server is required to save the policy store schema correctly.
   b. Repeat step 3. Restarting the directory server removed the policy store root. Importing the policy store schema again is required to create the policy store root.
5. Run the following command:

   `smldapsetup ldmod`
   `-f`*`siteminder_home`*`/xps/db/tier2/redhat/RedHat_7_1.ldif`

   siteminder_home

   Specifies the Policy Server installation path.

   The policy store schema is extended for XPS.

The policy store schema is created.

Set the SiteMinder Super User Password

The default SiteMinder administrator account is named siteminder. This account has maximum permissions. Set the password for this account so it can be used to manage the SiteMinder user interfaces and utilities until additional SiteMinder administrators can be created.

Note: The smreg utility is located at the top level of the Policy Server installation kit.

To set the super user password

1. Copy the smreg utility to *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   smreg -su 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.

   password

   Specifies the password for the default SiteMinder administrator.

   Limits:

   - The password must contain at least six (6) characters and cannot exceed 24 characters.
   - The password cannot include an ampersand (&) or an asterisk (*).
   - If the password contains a space, enclose the passphrase with quotation marks.

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

3. Delete the smreg utility from *policy_server_home*\bin. Deleting smreg prevents someone from changing the password without knowing the previous one.

   The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day–to–day operations. Use the default super user to:

- Import the default policy store objects.
- Access the FSS Administrative UI and Administrative UI for the first–time. We recommend creating another administrator with super user permissions.

More information:

Locate the Installation Media (see page 213)

Import the Default Policy Store Objects

Importing the default policy store objects sets up the policy store for use with the Administrative UI. The default policy store objects are required to store policy information in the policy store.

Note: If you have installed the Policy Server in FIPS-only mode, ensure you use the -cf argument when importing the default policy store objects.

To import the default policy store objects

1. Run the following command:

   ```
   smobjimport -ipolicy_server_home\db\smdif\smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

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

   Windows example: smobjimport
   ```
   -i"C:\Program Files\CA\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
   ```

   policy_server_home

   Specifies the Policy Server installation path.

   -d*siteminder_super_user_name*

   Specifies the name of the SiteMinder super user account.

   Default: siteminder

   -w*siteminder_super_user_password*

   Specifies the password for the SiteMinder super user account.

   -v

   Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

   Default value: stdout

-cf

(Optional) Imports sensitive data using FIPS-compatible cryptography.

Note: This argument is only required if the Policy Server is operating in FIPS-only mode.

smobjimport imports the policy store objects. The objects are automatically imported to the appropriate locations.

2. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder super user account.

Default: siteminder

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

smobjimport imports the policy store objects. These objects are automatically imported to the appropriate locations.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for more information about licensing.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.
4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.
5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the SiteMinder environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually.

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

passphrase

Specifies the password for the default SiteMinder super user account (siteminder).

Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

-adminui–setup

Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

-t *timeout*

(Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect SiteMinder administrator credentials when logging into the Administrative UI for the first–time

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

How to Configure a Secure Connection to a Red Hat Directory Server

You can configure a secure connection from the Policy Server to a Red Hat user store or policy store.

Configure a Secure Connection from the Policy Server to a Red Hat User Store

You can configure a secure connection from the Policy Server to a Red Hat user store.

Note: When the Policy Server is operating in FIPS mode and the directory connection is a secure SSL connection, the certificates used by the Policy Server and the directory server must be FIPS-compliant.

To configure a secure connection from the Policy Server to a Red Hat user store

1. Install the root certificate of the Certificate Authority in the Netscape cert7.db database on each computer that uses SSL to communicate with the Red Hat user store.

   Note: The Policy Server requires the root certificate to be in the Netscape cert7.db format. Do not use Microsoft Internet Explorer to install the certificate.

2. In the SiteMinder Administrative UI, click Infrastructure, Directory.
3. Click User Directory, Modify User Directory.

   The Modify User Directory pane opens.

4. Specify search criteria, and click Search.

   A list of user directories that match the search criteria opens.

   Note: To view all user directories, leave the search field blank and click Search.

5. Select the Red Hat user directory from the list, and click OK.

   The Modify User Directory: Name pane opens.

6. Select the Secure Connection check box on the Directory Setup group box, and click Submit.

A secure connection is configured from the Policy Server to the Red Hat user store.

Configure a Secure Connection from the Policy Server to a Red Hat Policy Store

You can configure a secure connection from the Policy Server to a Red Hat policy store.

Note: When the Policy Server is operating in FIPS mode and the directory connection is a secure SSL connection, the certificates used by the Policy Server and the directory server must be FIPS-compliant.

To configure a secure connection from the Policy Server to a Red Hat policy store

1. Install the root certificate of the Certificate Authority in the Netscape cert7.db database on each computer that uses SSL to communicate with the Red Hat policy store.

   Note: The Policy Server requires the root certificate to be in the Netscape cert7.db format. Do not use Microsoft Internet Explorer to install the certificate.

2. On the server where the Policy Server is installed, open the Policy Server Management Console, and select the Data tab.

3. On the Data tab, perform the following steps:

   a. Select the check box Use SSL.

   b. Type the path to the cert7.db file in the Netscape Certificate Database File field.

4. Click Apply.

A secure connection is configured from the Policy Server to a Red Hat policy store.

Chapter 11: Siemens DirX 6.0 D00 Directory Server

This section contains the following topics:

Configure a DirX 6.0 D00 Directory Server as a Policy Store

You can configure a Siemens DirX 6.0 D00 Directory Server as a SiteMinder r12.0 SP3 policy store.

Follow these steps:

1. Install DirX 6.0 D00, and accept all of the defaults during installation.

   Note: If you do not have an existing database, install the sample database.

2. Log in to the Policy Server host system.

3. Copy the following files from *siteminder_home*\db\tier2\SiemensDirx to

   DirX_install_path\scripts\security\Netegrity\SiteMinder:

   - dirxabbr-ext.SiteMinderR12sp3
   - schema_ext_for_SiteMinderR12sp3.adm
   - subschema_ext_for_SiteMinderR12sp3.cp
   - bind.tcl
   - l-bind.cp
   - _setup.bat
   - setup.bat
   - GlobalVar.tcl

   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.

siteminder_home

Specifies the Policy Server installation path.

DirX_install_path

Specifies the DirX installation path.

Example: C:\program files\siemens\dirx

4. Copy the following files from *siteminder_home*\xps\db\tier2\dirx to *DirX_install_path*\scripts\security\Netegrity\SiteMinder:
   - dirxabbr-ext.XPS
   - schema_ext_for_XPS.adm
   - subschema_ext_for_XPS.cp
5. Rename the following files:
   - schema_ext_for_SiteMinderR12sp3.adm to schema_ext_for_SiteMinder.adm
   - subschema_ext_for_SiteMinderR12sp3.cp to subschema_ext_for_SiteMinder.cp
6. Copy the following files to *DirX_install_path*\client\conf:
   - dirxabbr-ext.SiteMinderR12sp3
   - dirxabbr-ext.XPS
7. Rename dirxabbr-ext.SiteMinderR12sp3 to dirxabbr-ext.SiteMinder.
8. Stop and restart the DirX service.
9. Edit GlobalVar.tcl to update the global variables that the DirX scripts reference.

   Default values:
   - LDAP port: 389
   - Root DN: o=pqr
   - Admin username: cn=admin,o=pqr
   - Admin password: dirx
10. Run setup.bat, and check the resulting log file, setup.log, for errors.
11. Rebind to the DSA using the DirXmanage tool.

    Note: Watch for errors.

12. Create the base tree structure using the DirXmanage tool:
    a. Under o=PQR, create ou=Netegrity.
    b. Under ou=Netegrity, create ou=SiteMinder.
    c. Under ou=SiteMinder, create ou=PolicySvr4.
    d. Under ou=PolicySvr4, create ou=XPS

    The policy store schema is created for r12.0 SP3.
13. Point the Policy Server to the DirX Directory Server by using the Data tab on the Policy Server Management Console.

    Sample values:

    - LDAP IP Address: 123.456.7.8
    - Root DN: o=pqr
    - Admin username: cn=admin,o=pqr
    - Admin password: ********
14. Run the following command:

    ```
    smreg -su password
    ```

    The SiteMinder super user password is set.
15. Navigate to *policy_server_home*\bin.

    policy_server_home

    Specifies the Policy Server installation path.
16. Run the following command:

    ```
    smobjimport -ipolicy_server_home\db\smdif\smpolicy.smdif -v
    -dsiteminder_super_user_name -wsiteminder_super_user_password
    ```

    -i

    Specifies the path and name of the import file.

    -v

    Turns on tracing and outputs error, warning, and comment messages.

    Note: You can output to a log file and check for errors.

    The base policy store data is imported from the file smpolicy.smdif.
17. Run the following command:

    ```
    smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
    -dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
    ```

    -i

    Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder Super User account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder Super User account.

-f

Overrides duplicate objects

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

smobjimport imports the policy store objects. These objects are automatically imported to the appropriate locations.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for more information on licensing.

The DirX Directory Server is configured as a policy store.

Note: You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.
4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.
5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the SiteMinder environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually.

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   `XPSRegClient siteminder[:`*`passphrase`*`] -adminui-setup -t `*`timeout`*` -r `*`retries`*` -c `*`comment`*` -cp -l `*`log_path`*` -e `*`error_path`*` -vT -vI -vW -vE -vF`

   passphrase

   Specifies the password for the default SiteMinder super user account (siteminder).

   Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

   -adminui–setup

   Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

-t *timeout*

(Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect SiteMinder administrator credentials when logging into the Administrative UI for the first–time

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

Sample User Directory Settings--Siemens DirX 6.0

Following are sample user directory settings:

Directory Setup

- Namespace: LDAP
- Server: 123.456.7.8
- Root: o=pqr
- DN Lookup Start: (cn=
- DN Lookup End:)

Credentials and Connection

- Admin Username: cn=admin,o=pqr
- Admin Password: dirx

User Attributes

- Universal ID(R): cn
- Disabled Flag (RW): description
- Password Attribute (RW): userpassword
- Password Data (RW): audio
- Challenge/Response (RW): jpegPhoto

Note: The user attributes above are available without adding any attributes to the user object in DirX.

Note: User attribute names in DMS are or are not case-sensitive on an attribute-by-attribute basis.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.0 SP3 policy store. You can upgrade an existing policy store to r12.0 SP3.

Complete the following procedures to upgrade the policy store:

1. Extend the policy store schema.

   Note: The existing r6.x policy store schema has not changed. The r12.0 SP3 migration requires that you extend the policy store schema for policy store for objects that r12.0 SP3 requires.

2. Import the base policy store objects.
3. Import the Policy Store Data Definitions.

Note: If you are upgrading a directory server or database that is listed in the Support Matrix, but not in this guide, see the *SiteMinder Upgrade Guide.*

Extend the Siemens DirX Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.0 SP3. There are no changes to the existing 6.x policy store schema.

Follow these steps:

1. Update the base tree structure using the DirXmanage tool. Under ou=PolicySvr4, create ou=XPS.
2. Copy the following files from *siteminder_home*\xps\db\tier2\dirx

   to *DirX_install_path*\scripts\security\Netegrity\SiteMinder:

   - _setup.bat
   - bind.tcl
   - dirxabbr-ext.XPS
   - GlobalVar.tcl
   - l-bind.cp
   - schema_ext_for_XPS.adm
   - setup.bat
   - subschema_ext_for_XPS.cp

   siteminder_home

   Specifies the Policy Server installation path.

   DirX_install_path

   Specifies the DirX installation path.

   Example: C:\program files\siemens\dirx
3. Copy dirxabbr-ext.XPS to *DirX_install_path*\client\conf.
4. Stop and restart the DirX service.
5. Edit GlobalVar.tcl to update the global variables that the DirX scripts reference.

   Default values:

   - LDAP port: 389
   - Root DN: o=pqr
   - Admin username: cn=admin,o=pqr
   - Admin password: dirx

6. Run setup.bat, and check the resulting log file, setup.log, for errors.
7. Rebind to the DSA using the DirXmanage tool.

   Note: Watch for errors.

The policy store schema is extended to include the objects introduced by r12.0 SP3.

Import the Base Policy Store Objects

Importing the default SiteMinder objects upgrades the policy store for use with the Administrative UI. The default SiteMinder objects are required to store policy information in the 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.

To import the base policy store objects

1. Run the following command:

   ```
   smobjimport -ipolicy_server_home\db\smdif\upgrade_smdif_file_name
   -dsiteminder_super_user_name -wsiteminder_super_user_password
   -v -f
   ```

   policy_server_home

   Specifies the Policy Server installation path.

   upgrade_smdif_file_name

   Specifies the name of the import file:

   - **r6.0 to r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
   - **r6.0 SP1 to r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
   - **r6.0 SP2 to r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
   - **r6.0 SP3 to r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
   - **r6.0 SP4 to r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
   - **r6.0 SP5 to r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
   - **r6.0 SP6 to r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

   -dsiteminder_super_user_name

   Specifies the name of the SiteMinder administrator account.

   -wsiteminder_super_user_password

   Specifies the password for the SiteMinder administrator account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.0 SP3.

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

Windows example: smobjimport

```
-i"C:\Program Files\CA\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

The base policy store objects are imported.

2. Run the following command:

Important! Do not re-import ampolicy.smdif if it has been previously imported into the policy store.

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-policy_server_home

Specifies the path and name of the import file.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder administrator account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder administrator account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for licensing information.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Chapter 12: Siemens DirX EE 2.0 Directory Server

This section contains the following topics:

How to Configure a Siemens DirX EE 2.0 Policy Store

To configure a Siemens DirX EE 2.0 Directory Server as a r12.0 SP3 policy store, complete the following procedures:

1. Configure a DirX EE 2.0 Directory Server as a policy store.
2. Import the policy store data definitions.
3. Prepare for the Administrative UI registration.

Configure a DirX EE 2.0 Directory Server as a r12.0 SP3 Policy Store

Follow these steps:

1. Install DirX EE 2.0.
2. Open the DirX EE Manager and create the following base tree structure to hold the policy store data:
   a. Under o=MyCompany, create ou=netegrity.
   b. Under ou=netegrity, create ou=Siteminder.
   c. Under ou=Siteminder, create ou=PolicySvr4.
   d. Under ou=PolicySvr4, create ou=XPS.

3. Log in to the Policy Server host system.
4. Copy the following files from *siteminder_home*\db\tier2\SiemensDirXEE20

   to *DirX_EE_install_path*\scripts\stand_alone\extensions:

   - DirXEE20_SMR12sp3_Schema.ldif
   - add_PS_Indexes.adm

   siteminder_home

   Specifies the Policy Server installation path.

   DirX_EE_install_path

   Specifies the DirX EE installation path.
5. Copy the following files from *siteminder_home*\xps\db\tier2\dirxee20 to *DirX_EE_install_path*\scripts\stand_alone\extensions:

   - XPS_SchemaExt.ldif
   - add_XPS_Indexes.adm
6. From a command prompt on the directory server host system, change to the following directory:

   DirX_EE_install_path\scripts\stand_alone\extensions
7. Run the following command:

   dirxmodify -f DirXEE20_SMR12sp3_Schema.ldif -D cn=admin,o=MyCompany -w dirx

   -f

   Specifies the name of the LDIF file.

   -D

   Specifies the bind DN.

   Example: cn=admin,o=MyCompany

   -w

   Specifies the password.

   Example: dirx

   -h

   (Optional) Specifies the host.

   Default: localhost

   -p

   (Optional) Specifies the port number.

   Default: 389

8. Run the following command:

   dirxadm add_PS_Indexes.adm

9. Run the following command:

   dirxmodify -f XPS_SchemaExt.ldif -D cn=admin,o=MyCompany -w dirx

10. Run the following command:

    dirxadm add_XPS_Indexes.adm

    The XPS schema is created.

11. Open the Policy Server Management Console, click the Data tab, and specify the following information in the fields on the tab:

    - LDAP IP Address

      Specifies the IP address of the policy store.

    - Root DN

      Example: o=MyCompany

    - Admin Username

      Example: cn=admin,o=MyCompany

    - Password

      Example: dirx

    The Policy Server points to the DirX EE policy store.

12. Run the following command:

    smreg –su *password*

    The SiteMinder administrator password is set.

13. Run the following command:

    smobjimport –i*policy_server_home*\db\smdif\smpolicy.smdif –v

    -d*siteminder_super_user_name* -w*siteminder_super_user_password*

    policy_server_home

    Specifies the Policy Server installation path.

    -i

    Specifies the path and name of the import file.

-v

Turns on tracing and outputs error, warning, and comment messages.

Note: You can output to a log file and check for errors.

The base policy store data is imported from the file smpolicy.smdif to the DirX EE policy store.

14. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-i

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder superuser account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder superuser account.

-f

Overrides duplicate objects

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.
4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.
5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the SiteMinder environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually.

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   Specifies the password for the default SiteMinder super user account (siteminder).

   Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

   -adminui–setup

   Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

-t *timeout*

(Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect SiteMinder administrator credentials when logging into the Administrative UI for the first–time

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.0 SP3 policy store. You can upgrade an existing policy store to r12.0 SP3.

Complete the following procedures to upgrade the policy store:

1. Extend the policy store schema.

   Note: The existing r6.x policy store schema has not changed. The r12.0 SP3 migration requires that you extend the policy store schema for policy store for objects that r12.0 SP3 requires.

2. Import the base policy store objects.
3. Import the Policy Store Data Definitions.

Note: If you are upgrading a directory server or database that is listed in the Support Matrix, but not in this guide, see the *SiteMinder Upgrade Guide.*

Upgrade a DirX EE 2.0 Policy Store from 6.x to r12.0 SP3

To upgrade a Siemens DirX EE 2.0 Directory Server from a 6.x policy store to a r12.0 SP3 policy store, create the XPS schema in the policy store.

Follow these steps:

1. Open the DirX EE Manager and update the base tree structure. Under ou=PolicySvr4, create ou=XPS.
2. Log in to the Policy Server host system.

3. Copy the following file from *siteminder_home*\db\tier2\SiemensDirXEE20 to *DirX_EE_install_path*\scripts\stand_alone\extensions:

   add_PS_Indexes.adm

   siteminder_home

   Specifies the Policy Server installation path.

   DirX_EE_install_path

   Specifies the DirX EE installation path.

4. Copy the following files from *siteminder_home*\xps\db\tier2\dirxee20 to *DirX_EE_install_path*\scripts\stand_alone\extensions:

   - XPS_SchemaExt.ldif
   - add_XPS_Indexes.adm

5. From the command prompt on the directory server host system, change to the following directory:

   DirX_EE_install_path\scripts\stand_alone\extensions

6. Run the following command:

   dirxadm add_PS_Indexes.adm

7. Run the following command:

   dirxmodify -f XPS_SchemaExt.ldif -D cn=admin,o=MyCompany -w dirx

   -f

   Specifies the name of the LDIF file.

   -D

   Specifies the bind DN.

   Example: cn=admin,o=MyCompany

   -w

   Specifies the password.

   Example: dirx

   -h

   (Optional) Specifies the host.

   Default: localhost

   -p

   (Optional) Specifies the port number.

   Default: 389

8. Run the following command:

   dirxadm add_XPS_Indexes.adm

The XPS schema is created. You can now import the policy store data definitions.

Import the Base Policy Store Objects

Importing the default SiteMinder objects upgrades the policy store for use with the Administrative UI. The default SiteMinder objects are required to store policy information in the 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.

To import the base policy store objects

1. Run the following command:

   ```
   smobjimport -ipolicy_server_home\db\smdif\upgrade_smdif_file_name
   -dsiteminder_super_user_name -wsiteminder_super_user_password
   -v -f
   ```

   policy_server_home

   Specifies the Policy Server installation path.

   upgrade_smdif_file_name

   Specifies the name of the import file:

   - **r6.0 to r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
   - **r6.0 SP1 to r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
   - **r6.0 SP2 to r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
   - **r6.0 SP3 to r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
   - **r6.0 SP4 to r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
   - **r6.0 SP5 to r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
   - **r6.0 SP6 to r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

   -d*siteminder_super_user_name*

   Specifies the name of the SiteMinder administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SiteMinder administrator account.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.0 SP3.

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

Windows example: smobjimport

```
-i"C:\Program Files\CA\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

The base policy store objects are imported.

2. Run the following command:

Important! Do not re-import ampolicy.smdif if it has been previously imported into the policy store.

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-policy_server_home

Specifies the path and name of the import file.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder administrator account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder administrator account.

-f

Overrides duplicate objects.

-v

Turns on tracing and outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

Note: Importing ampolicy.smdif makes available Federation Security Services, Web Service Variables, and eTelligent Rules functionality that is separately licensed from SiteMinder. If you intend on using the latter functionality, contact your CA account representative for licensing information.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

Importing the policy store data definitions is required to use the policy store with the Administrative UI. The base definitions describe the policy store data.

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.

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:
   - **Windows**—*policy_server_home*\xps\dd
   - **UNIX**—*policy_server_home*/xps/dd

   policy_server_home

   Specifies the Policy Server installation path.
2. Run the following command:

   Important! Run the XPSDDInstall tool with the data definition files in the following order or the imports fail.

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

   Note: If you are importing this file for the first time, a warning states that no policy data can be found. This is expected behavior and does not affect the import.
3. Run the following command:

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   You have imported all required policy store data definitions.

Appendix A: Configuring SiteMinder Connections over SSL

This section contains the following topics:

How to Configure an LDAP User Directory Connection over SSL

Configuring an LDAP user directory connection over SSL requires that you configure SiteMinder to use your certificate database files.

Complete the following steps to configure the connection over SSL:

1. Before you configure a connection over SSL.
2. Install the NSS utility.
3. Create the certificate database files.
4. Add the root Certificate Authority (CA) to the certificate database.
5. Add the server certificate to the certificate database.
6. List the certifications in the certificate database.
7. Configure the user directory connection for SSL.
8. Point the Policy Server to the certificate database.
9. Verify the SSL connection.

Before You Configure a Connection over SSL

Review the following before configuring an LDAP user directory connection over SSL:

- Ensure your directory server is SSL-enabled.

  Note: For more information on configuring your directory server to communicate over SSL, refer to the vendor-specific documentation.

- SiteMinder uses a Netscape LDAP SDK to communicate with LDAP directories. As a result, SiteMinder requires that the database files be in a Netscape version file format (cert7.db).

  Important! Do not use Microsoft Internet Explorer to install certificates into your cert7.db database file.

- A third-party certificate utility, which is compatible with Netscape, is required to manage your SSL certificates. We recommend the Mozilla® Network Security Services (NSS) utility, version 3.2.2.

  Note: Version 3.2.2 is required to support the cert7.db format. Do not use later versions.

- (Active Directory) Considering the following:
  - If the SiteMinder user directory connection was configured with the AD namespace, the following process does not apply. The AD namespace uses the native Windows certificate repository when establishing an SSL connection. When configuring the AD namespace to communicate over SSL:
    - Ensure that the SiteMinder user directory connection is configured for a secure connection. For more information, refer to Configure the User Directory Connection for SSL (see page 210).
    - On the machine hosting the Active Directory instance, ensure that the root CA certificate and the server certificate are added to the services' certificate store.

    Note: For more information on configuring Active Directory to communicate over SSL, refer to the Microsoft documentation.
  - If the SiteMinder user directory connection was configured with the LDAP namespace, complete the following process to configure the connection over SSL.

Install the NSS Utility

You install the NSS utility to manage your certificate database files.

Note: Install the utility on a system to which the Netscape Portable Runtime (NSPR) or the Policy Server is installed. Installing the utility to a system with either component ensures that the necessary DLLs or shared objects are available.

To install the NSS utility

1. Access the Mozilla NSS 3.2.2 FTP site.
2. Download the respective zip or tar for your operating system.

   Note: A zip is not available for Windows Server 2003. Download the zip for Windows NT.
3. Extract the NSS utility to a temporary location on the system to which you are managing your certificate database files.

Create the Certificate Database Files

The Policy Server requires that the certificate database files be in the Netscape version file format (cert7.db). You may use the NSS utility to create the certificate database files.

Note: The following procedure details the specific options and arguments to complete the task. For a complete list of the NSS utility options and arguments, refer to the Mozilla documentation on the NSS project page.

To create the certificate database files

1. From a command prompt, navigate to the bin directory in the location to which you extracted the NSS utility.

   Example: C:\nss\bin

   Note: Windows has a native certutil utility. Verify that you are working from the bin directory of the NSS utility, or you can inadvertently run the Windows certutil utility.

2. Enter the following command:

   `certutil -N -d certificate_database_directory`

   -N

   Creates the cert7.db, key3.db, and secmod.db certificate database files.

   -d *certificate_database_directory*

   Specifies the directory to which the NSS utility is to create the certificate database files.

   Note: If the file path contains spaces, bracket the path in quotes.

   The utility prompts for a password to encrypt the database key.

3. Enter and confirm the password.

   NSS creates the required certificate database files:

   - cert7.db
   - key3.db
   - secmod.db

Example: Create the Certificate Database Files

```
certutil -N -d C:\certdatabase
```

Add the Root Certificate Authority to the Certificate Database

You add the root Certificate Authority (CA) to make it available for communication over SSL.

Note: The following procedure details the specific options and arguments to complete the task. For a complete list of the NSS utility options and arguments, refer to the Mozilla documentation on the NSS project page.

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.

To add the root CA certificate to the certificate database

1. From a command prompt, navigate to the bin directory in the location to which you extracted the NSS utility.

   Example: C:\nss\bin

   Note: Windows has a native certutil utility. Verify that you are working from the bin directory of the NSS utility, or you can inadvertently run the Windows certutil utility.

2. Run the following command to add the root CA to the database file:

   `certutil -A -n alias -t trust_arguments -i root_CA_path -d certificate_database_directory`

   -A

   Adds a certificate to the certificate database.

   -n *alias*

   Specifies an alias for the certificate.

   Note: If the alias contains spaces, bracket the alias with quotes.

   -t *trust_arguments*

   Specify the trust attributes to apply to the certificate when adding it to the certificate database. There are three available trust categories for each certificate, which are expressed in this order: "SSL, email, object signing". Specify the appropriate trust arguments so that the root CA is trusted to issue SSL certificates. In each category position, you may use zero or more of the following attribute arguments.

   p

   Valid peer.

   P

   Trusted peer. This argument implies p.

c

Valid CA.

T

Trusted CA to issue client certificates. This argument implies c.

C

Trusted CA to issue server certificates (SSL only). This argument implies c.

Important! This is a required argument for the SSL trust category.

u

Certificate can be used for authentication or signing.

-i *root_CA_path*

Specifies the path to the root CA file. Consider the following:

- The path must include the certificate name.
- Valid extensions for a certificate include .cert, .cer, and .pem.

Note: If the file path contains spaces, bracket the path in quotes.

-d *certificate_database_directory*

Specifies the path to the directory that contains the certificate database.

Note: If the file path contains spaces, bracket the path in quotes.

NSS adds the root CA to the certificate database.

Example: Adding a Root CA to the Certificate Database

```
certutil -A -n "My Root CA"  -t "C,," -i C:\certificates\cacert.cer -d C:\certdatabase
```

Add the Server Certificate to the Certificate Database

You add the server certificate to the certificate database to make it available for communication over SSL.

Note: The following procedure details the specific options and arguments to complete the task. For a complete list of the NSS utility options and arguments, refer to the Mozilla documentation on the NSS project page.

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.

To add the server certificate to the certificate database

1. From a command prompt, navigate to the bin directory in the location to which you extracted the NSS utility.

   Example: C:\nss\bin

   Note: Windows has a native certutil utility. Verify that you are working from the bin directory of the NSS utility, or you can inadvertently run the Windows certutil utility.

2. Run the following command to add the root certificate to the database file:

   `certutil -A -n alias -t trust_arguments -i server_certificate_path -d certificate_database_directory`

   -A

   Adds a certificate to the certificate database.

   -n *alias*

   Specifies an alias for the certificate.

   Note: If the alias contains spaces, bracket the alias with quotes.

   -t *trust_arguments*

   Specify the trust attributes to apply to the certificate when adding it to the certificate database. There are three available trust categories for each certificate, which are expressed in this order: "SSL, email, object signing". Specify the appropriate trust arguments so that the certificate is trusted. In each category position, you may use zero or more of the following attribute arguments:

   p

   Valid peer.

   P

   Trusted peer. This argument implies p.

   Important! This is a required argument for the SSL trust category.

   -i *server_certificate_path*

   Specifies the path to the server certificate. Consider the following:

   - The path must include the certificate name.
   - Valid extensions for a certificate include .cert, .cer, and .pem.

   Note: If the file path contains spaces, bracket the path in quotes.

-d *certificate_database_directory*

Specifies the path to the directory that contains the certificate database.

Note: If the file path contains spaces, bracket the path in quotes.

NSS adds the server certificate to the certificate database.

Example: Adding a Server Certificate to the Certificate Database

```
certutil -A -n "My Server Certificate" -t "P,," -i C:\certificates\servercert.cer -d
C:\certdatabase
```

List the Certificates in the Certificate Database

You list the certifications to verify that they were added to the certificate database.

Note: The following procedure details the specific options and arguments to complete the task. For a complete list of the NSS utility options and arguments, refer to the Mozilla documentation on the NSS project page.

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.

To list the certifications in the certificate database

1. From a command prompt, navigate to the bin directory in the location to which you extracted the NSS utility.

   Example: C:\nss\bin

   Note: Windows has a native certutil utility. Verify that you are working from the bin directory of the NSS utility, or you can inadvertently run the Windows certutil utility.

2. Run the following command:

   ```
   certutil -L -d certificate_database_directory
   ```

   -L

   Lists all of the certificates in the certificate database.

   -d *certificate_database_directory*

   Specifies the path to the directory that contains the certificate database.

   Note: If the file path contains spaces, bracket the path in quotes.

NSS displays the root CA alias, the server certificate alias, and the trust attributes you specified when adding the certificates to the certificate database.

Example: List the Certificates in the Certificate Database

```
certutil -L -d C:\certdatabase
```

Configure the User Directory Connection for SSL

You configure the user store connection to ensure that an SSL connection is used when the Policy Server and user store communicate.

Note: When you create or modify a Policy Server object in the FSS Administrative UI, use ASCII characters. Object creation or modification with non-ASCII characters is not supported.

To configure the user store connection for SSL

1. Log in to the Administrative UI.
2. Click Infrastructure, Directory.
3. Click User Directory, Modify User Directory.

   The Modify User Directory pane appears with a list of existing user directory connections.
4. Select the user directory connection you want, and click Select.

   User directory settings appear.
5. Select the Secure Connection check-box, and click Submit.

   The user directory connection is configured to communicate over SSL.

Point the Policy Server to the Certificate Database

You point the Policy Server to the certificate database to configure the Policy Server to communicate with the user directory over SSL.

Note: When you create or modify a Policy Server object in the FSS Administrative UI, use ASCII characters. Object creation or modification with non-ASCII characters is not supported.

To point the Policy Server to the certificate database

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the Data tab.
3. Enter the path to the Netscape certificate database file in the Netscape Certificate Database File field.

   Example: C:\certdatabase\cert7.db

   Note: The key3.db file must also be in the same directory as the cert7.db file.

4. Restart the Policy Server.

The Policy Server is configured to communicate with the user directory over SSL.

Verify the SSL Connection

You verify the SSL connection to ensure the user directory and the Policy Server are communicating over SSL.

Note: When you create or modify a Policy Server object in the FSS Administrative UI, use ASCII characters. Object creation or modification with non-ASCII characters is not supported.

To verify the SSL connection

1. Log in to the Administrative UI.
2. Click Infrastructure, Directory.
3. Click User Directory, View User Directory.

   The View User Directory pane appears with a list of existing user directory connections.

4. Select the connection you want, and click Select.

   User directory settings appear.

5. Click View contents.

   If SSL is properly configured, the Directory Content pane appears and lists the contents of the user directory.

Chapter 13: Platform Support and Installation Media

Locate the Platform Support Matrix

Use the Platform Support Matrix to verify that the operating environment and other required third-party components are supported.

Follow these steps:

1. Log in to the CA Support site.
2. Locate the Technical Support section.
3. Enter SiteMinder in the Product Finder field.

   The SiteMinder product page appears.
4. Click Product Status, SiteMinder Family of Products Platform Support Matrices.

Note: You can download the latest JDK and JRE versions at the Oracle Developer Network.

Locate the Bookshelf

The SiteMinder bookshelf is available on the Technical Support site.

Follow these steps:

1. Go to the Technical Support site.

   Note: You do not have to log in.
2. (Optional) If the Get Support tab is not pulled to the front, click Get Support.
3. Under Find Product News and Support, click Product Pages.

   The Support by Product page appears.
4. Enter SiteMinder in the Select a Product Page field and press Enter.

   The SiteMinder product page appears.
5. Click Bookshelves.
6. Click the link for the release that you require.

   The SiteMinder bookshelf main page appears.

Locate the Installation Media

You can find the installation media on the Technical Support site.

Follow these steps:

1. Log in to the CA Support site.
2. Locate the Technical Support section.
3. Click Download Center.
4. Locate the Support by Product section.
5. Type **SiteMinder** in the Select a Product Page field, and then press Enter.
6. Click Downloads.

   The Download Center screen appears.
7. Enter **SiteMinder** in the Select a Product field.
8. Select a release from the Select a Release drop-down list.
9. Select a Service Pack from the Select a Gen Level drop-down list.
10. Click Go.

    The Product Downloads screen appears. All SiteMinder installation executables are listed.

Index

G

H

I

L

M

N

O

P

R

S

T

U

V