CA SiteMinder®

Directory Configuration Guide

r6.0 SP6

Second Edition

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

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

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

CA Product References

This document references the following CA products:

CA SiteMinder®

Contact CA

Contact CA Support

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

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

Provide Feedback

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

If you would like to provide feedback about CA 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:

Overview

The Policy Server can connect to a number of different directory servers. The most common directories used as SiteMinder policy stores are discussed in the *Policy Server Installation Guide*.

Additional directories servers are supported as policy stores, user stores, or both, but must be manually configured to communicate with the Policy Server. This guide provides the configuration instructions for the following directories:

- Active Directory Global Catalog
- CA LDAP Server for z/OS r12
- Critical Path inJoin Directory Server v4.2
- Domino Directory Server
- IBM DB2
- Oracle Internet Directory Server
- Openwave Directory Server 6.0.1
- Siemens DirX 6.0 D00 Directory Server
- Siemens DirX EE 1.0 Directory Server

Chapter 2: Active Directory Global Catalog

This section contains the following topics:

Configure a Connection from the Policy Server to an Active Directory Global Catalog User Store

You use the SiteMinder User Directory dialog box to set up the parameters necessary to connect the Policy Server to an Active Directory Global Catalog user store.

To configure the Policy Server for the Global Catalog

1. In the Policy Server User Interface, select Edit, System Configuration, Create User Directory from the menu bar.

   The system displays the SiteMinder User Directory dialog box.

2. In the Directory Setup tab of the SiteMinder User Directory dialog box, do the following:

   a. In the Name field, enter the name of the user directory.

      Example: adgc_user_dir

   b. Make sure LDAP is selected from the Namespace drop-down menu.

   c. In the Server field, enter the IP Address and port number of the Active Directory Global Catalog.

      Example: 172.25.135.180:3269

   d. In the Root field, enter the search base that covers all the domains in the global catalog.

      Example: dc=com

   e. In the Start field, enter the starting LDAP user DN search criteria.

      Example: (&(cn=

   f. In the End field, enter the ending LDAP user DN search criteria.

      Example:)(objectclass=*))

   g. Click the Credentials and Connections tab.

3. In the Credentials and Connections tab, do the following:
   a. Check Require Credentials.
   b. In the Username field, enter the full DN of the Active Directory Global Catalog administrator.

      Example: cn=user1,cn=users,dc=universal,dc=com
   c. Enter and reconfirm the password.
   d. Check Secure Connection if you are using an SSL connection.

Configure a Global Catalog User Store With an SSL Connection

To configure an SSL connection

1. Install the Certificate Authority's (CA) root certificate into the Netscape cert7.db database on each machine that expects to use SSL to communicate with the Global Catalog user directory.

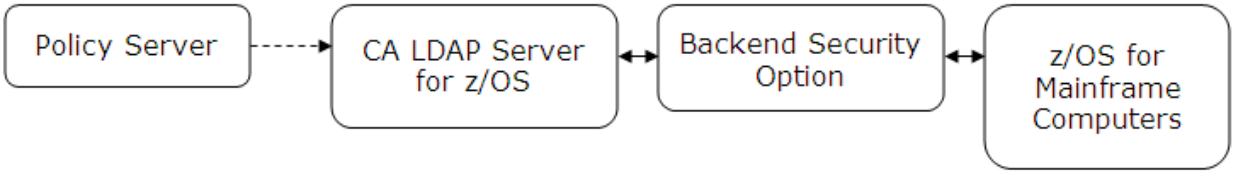
   Note: SiteMinder requires the certificate to be in a Netscape version file format (cert7.db), so do not use Microsoft Internet Explorer to install the certificate.
2. In the Netscape Certificate Database File field on the Data tab on the Policy Server Management Console, configure the Policy Server to use SSL by specifying the path to the cert7.db file.

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 r12 for z/OS (RACF)

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

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

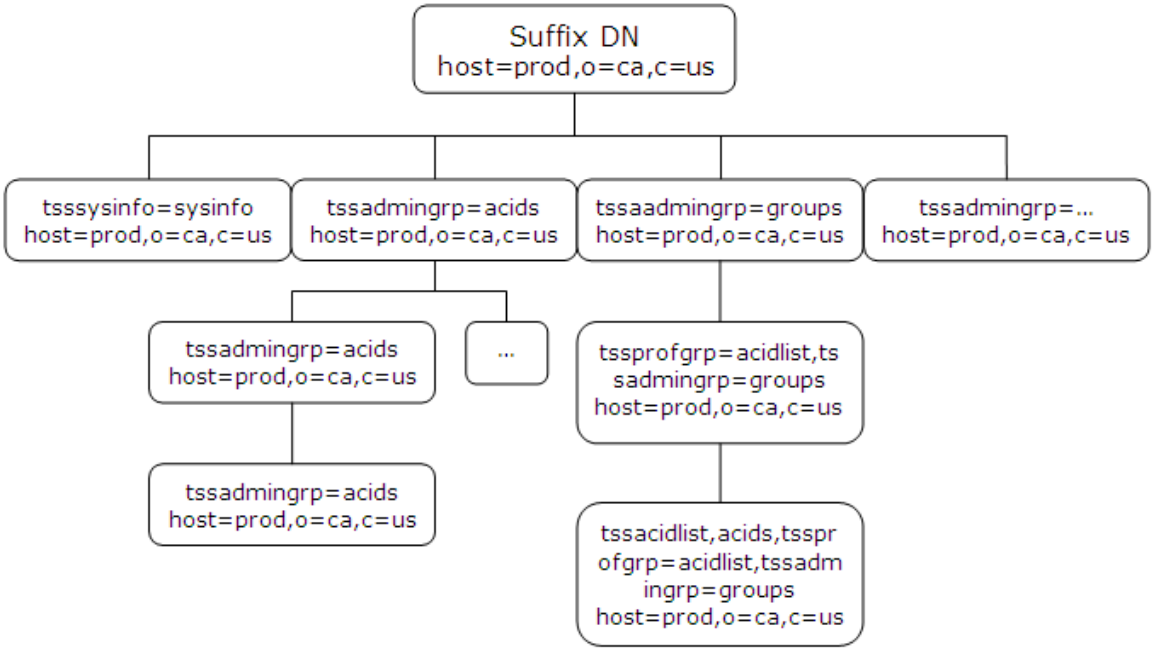
CA Top Secret r12 (TSS) Backend Security Option

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 the following Policy Server registry entries in the LDAP namespace by substituting the replacement values for the default values below.

registry_entry_home

Specifies the following registry entry location:

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

default_value

Specifies the registry entry's default value.

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 objectclasses to this registry entry:

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

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 Policy Server User Interface.

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 R12 for z/OS (RACF) Backend Security Option

This section describes the settings required to configure the CA LDAP Server R12 for z/OS (RACF) as a user store with the Policy Server.

Configure Policy Server Registry Entries for RACF

The CA LDAP Server R12 for z/OS (RACF) contains a different set of objectclasses as compared to other LDAP servers. Before configuring a user directory connection from the Policy Server to the CA LDAP Server, add the RACF objectclasses to the following Policy Server registry entries in the LDAP namespace by substituting the replacement values for the default values below:

registry_entry_home

Specifies the following registry entry location:

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

default_value

Specifies the registry entry's default value.

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:

RACT Objectclasses	Registry Key Type	Data
eTRACUserid	REG_DWORD	0x00000001(1)
eTRACAdminGrp	REG_DWORD	0x00000002(2)

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, open an existing user directory object in the Policy Server User Interface.

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 *CA SiteMinder 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 and specify whether the connection to the directory will use SSL.

   Important! Specifying administrator credentials is mandatory as anonymous binds to the user store are not allowed with CA LDAP Server R12 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 R12 for z/OS (RACF) as a user store, you must provide values in the fields on the Administrator Credentials group box on 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.

Chapter 4: Critical Path inJoin Directory Server

This section contains the following topics:

Policy Store Schema Considerations

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

- smpolicy.smdif
- smpolicy-secure.smdif

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

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

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

Parameter Name	Value in smpolicy.smdif	Value in smpolicy-secure.smdif
BadCssChars	No value	<, >, ', ;,), (, &, +, %00
BadQueryChars	No value	<, >, ', ;,), (, &, +, %00
BadUrlChars	//, ./, /., /*, *., ~, \, %00-%1f, %7f-%ff, %25	smpolicy.smdif values plus: <, >, ', ;,), (, &, +

IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	smpolicy.smdif values plus .jsp
ValidTargetDomain	Note: This parameter does not exist in smpolicy.smdif.	Provide a valid redirection domain as follows: validtargetdomain=".example.com"

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

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

Create a SiteMinder 5.5 or 6.0 Policy Store in InJoin Directory Server v4.2

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

To create the required SiteMinder 5.5 or 6.0 policy store schema in InJoin Directory Server (IDS)

1. Start the DSA, using Critical Path's iCon GUI.
2. Perform an LDAP modify, using the supplied IDS_Add_Schema_55.ldif or IDS_Add_Schema_60.ldif file.

   6.0 example:

   ```
   ldapmodify -h <server_IP> -p <port_number> -D "cn=manager" -w <password> -c -f
   "IDS_Add_Schema_60.ldif"
   ```

   Note: ldapmodify requires version 4.2 of the Critical Path InJoin Directory Server.
3. Use the iCon GUI to reload the schema or verify that the schema has been updated.
4. Go to dsa, comms, LDAP and modify the option "paging mode" to always. Restart the DSA.

5. Manually create the root nodes (ou=PolicySvr4, ou=SiteMinder, ou=Netegrity) via iCon's DIT admin interface.
6. Import the base policy store data from the file smpolicy.smdif.

   Example: smobjimport -i<siteminder_installation>\db\smdif\smpolicy.smdif -v

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

   - smpolicy.smdif
   - smpolicy–secure.smdif

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

Connect to an IDS Policy Store

To connect to the IDS Policy Store, follow the instructions in the *Policy Server Installation Guide*.

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.

Configure SSL

To configure SSL

1. Install the SSL version of IDS. The CD is entitled "InJoin Directory Server Secure Sockets Layer Option for Microsoft Windows NT."

   Note: Despite the name, Solaris support is included.

   To check on whether or not you have the SSL-enabled version installed:

   a. Go to the DSA directory (c:\ids\icon\dsa1).

   b. Run the command odsadmin.

   c. Bind to the directory by typing "bman", then the password.

   d. Type m_read_lkey.

      You should see the following, including "SSL enabled":

      admin>m_read_lkey

      read:

      read result:

      Entry information:

      Name: root

      Attribute type = licenceKey

      Maximum number of entries: 20000

      Demonstration expiry time: 06 August 2002

      Instance: 8192

      Options:

      Shadowing enabled

      Enterprise iCon enabled

      SSL enabled

      Result = OK

2. Go to the SSL directory of iDS (c:\ids\icon\dsa1\ssl). Create a file containing a random key (such as ds43jr58vndn3). The new file name is used in Step 3. (The example uses the name "random.")

3. Generate a CSR (Certificate Signing Request) file containing one line with a string made up of random characters and numbers. For example:

   "odscertreq -rnd random -str 1024 -alg rsa -enc pem -prv pkfile.p8 -pass password -req test.req -dn cn=server.icarus.com"

   In this example:

   - random is the name of the file that we created in Step 2.
   - pkfile.p8 is the name of the file that will be generated containing the private key.
   - password is the password.
   - test.req is the name of the generated CSR file.
   - server.icarus.com is the dn of the server.

4. Pass the text in test.req to a Certificate Authority to obtain a server certificate. The CA will generate the server certificate. Save this in a file (our example uses the name servercert.crt).

5. Obtain the root certificate from the CA in text format, and save it in a file (our example uses rootcert.crt).

6. Use the odscertconv command to create an identity file for the SSL/IDS configuration:

   ```
   odscertconv -certificate servercert.crt -certificate rootcert.crt
   -pkcs8 pkfile.p8 "password" toPEM -pkcs12 cert.p12 "firewall"
   ```

   servercert.crt

   Contains the server certificate generated by the CA

   rootcert.crt

   Contains the root certificate from the CA

   pkfile.p8

   Represents the private key file

   password

   Represents the password

   cert.p12

   Specifies the name of the identity file that will be generated by odscertconv

7. Using iCon, go to the DSA, click on "Comms", then "LDAP", then "LDAP Security".

8. Enter an SLL port (636) and a name for the PKCS12 identity ("test").

9. For the identity file name, enter the name of the identity file created in Step 7 ("cert.p12"). Also, enter the password ("password") used in the same step for the PKCS#12 Password field.
10. Click Apply, and restart the DSA.

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

Upgrade a 5.5 Policy Store to a 6.0 Policy Store

Note: This section is for users upgrading their policy store from 5.5 to 6.0 only.

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

To upgrade existing SiteMinder 5.5 policy store to SiteMinder 6.0 policy store schema in IDS

1. Stop the DSA that contains the 5.5 Policy Store. Go to dsa, comms, LDAP and modify the option "paging mode" to always. Restart the DSA.
2. On the DSA that contains the SiteMinder 5.5 policy store, perform an LDAP modify, using the supplied IDS_Upgrade_Schema_55TO60.ldif file.

   Example:

   ```
   ldapmodify -h <server_IP> -p <port_number> -D "cn=manager" -w
   <password> -c -f "IDS_Upgrade_Schema_55TO60.ldif"
   ```

   Note: ldapmodify requires version 4.2 of the Critical Path InJoin Directory Server.
3. Use the iCon GUI to reload the schema or verify that the schema has been updated.

4. Point the SiteMinder 6.0 Policy Server to the existing 5.5 policy store on which the schema was upgraded.
5. Import the base policy store data for upgrade from 5.5 to 6.0 from the file sm_upgrade_55_to_60.smdif.

   Example:

   ```
   smobjimport -i<siteminder_installation>\db\smdif\
   sm_upgrade_55_to_60.smdif -v -f
   ```

Chapter 5: Domino Directory Server

This section contains the following topics:

Connect to a Domino User Directory

To connect to a Domino user directory

1. From the Policy Server user interface, click Edit > Create User Directory.

   The User Directory Properties dialog appears.

2. Enter values for the following fields in Directory Setup tab:

   - Server

     Example: 172.25.142.165:389

   - Root

     Example: o=myOrg

   - Start

     Example: (cn=

   - End

     Example: *)

3. Click Apply.

   The values are saved.

4. Click Credentials and Connections.

   The Credentials and Connections tab moves to the front.

5. Select Require Credentials, and enter the required values.

   Note: Select Secure Connection to configure SSL communication to the user store.

6. Click Apply.

   The values are saved.

7. Click the User Attributes tab.

   The User Attributes tab moves to the front.

8. Complete the user attribute values, and click Apply.

   The values are saved.

9. Click OK.

   The User Directory Properties dialog closes and the Policy Server is configured to use the Domino user directory.

Chapter 6: IBM DB2

This section contains the following topics:

How to Configure a Data Store in an IBM DB2 Database

To configure a SiteMinder data store in an IBM DB2 Database

1. Create a DB2 Database with SiteMinder schema.
2. Configure the DB2 Data Source for SiteMinder.
3. Configure the policy, key, logging, or session stores.

   Note: More information about configuring data stores exists in the *Policy Server Installation Guide*.
4. Import default SiteMinder Objects into the policy store.

   Note: More information about importing default SiteMinder objects exists in the *Policy Server Installation Guide*.

Step 1: Create a DB2 Database With SiteMinder Schema

SiteMinder provides schema files to create schemas for storing policies, keys, logs, session data, and sample users. The following schema files are provided with this .zip file:

sm_db2_ps.sql

Creates the SiteMinder policy store or key store (if you are storing keys in a different database) in a DB2 database.

Note: When configuring a DB2 database as a policy store, you must create a tablespace with the 32-KB page size and a system temporary tablespace with the 32-KB page size for the user associated with the database.

sm_db2_logs.sql

Creates the schema for SiteMinder audit logs in a DB2 database.

sm_db2_ss.sql

Creates the schema for the Session Server in a DB2 database.

smsampleusers_db2.sql

(Optional) Creates the schema for SiteMinder sample users in a DB2 database and populates the database with sample users. For example, if you look in the script, you can see a sample user named GeorgeC with a password of siteminder.

Create the database objects by running the appropriate SQL script using IBM DB2.

To delete these database objects, refer to "Deleting SiteMinder Data in ODBC Databases" in the *Policy Server Installation Guide*.

You can store SiteMinder data in a single DB2 database or run each script on its own to create a separate:

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

Note: For information about running SQL scripts, refer to the DB2 database documentation.

Step 2: 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.

To create the DB2 data source

1. Select Programs, Administrative Tools, Data Sources (ODBC) to access the ODBC Data Source Administrator.
2. Click the System DSN tab and click Add.
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, do the following:
   a. In the Data Source Name field, enter any name you want.

      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 machine.

   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.

Next Steps

More information about configuring policy, key, logging, and session stores and importing default SiteMinder objects in to the policy store exists in the *Policy Server Installation Guide*.

Upgrade the Session Server from 6.0 to 6.0 SP 5

If you have a 6.x Session Server installed, you must upgrade it to leverage features that utilize it in 6.0 SP5.

To upgrade the Session Server

Import the the following .sql scheme script into the existing session store database. The script, located in *<siteminder_installation>*\db\SQL, is:

sm_db2_ss_upgrade_60_to_60SP5.sql

Upgrades a session store in a DB2 database from 6.0 to 6.0 SP 5. This script adds a new Expiry Data table to the session store.

Note: More information on importing a .sql script into a session store database exists in one of the following sections in the "Configure SiteMinder Data in a Relational Database" chapter in the 6.0 SP 5 *Policy Server Installation Guide*:

- "Step 1: Create an Oracle Database With SiteMinder Schema"
- "Step 1: Create a SQL Server Database With SiteMinder Schema"

Chapter 7: 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.

More information:

How to Store Key Information in MySQL (see page 48)
How to Store Audit Logs in MySQL (see page 51)
How to Store Session Information in MySQL (see page 54)

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. Download the SiteMinder schema files.
5. Create the SiteMinder schema.
6. 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.
7. Point the Policy Server to the database.
8. Set the SiteMinder super user password.
9. Import the default SiteMinder objects.
10. Import the policy store data definitions.
11. Restart the Policy Server.
12. Prepare for the Policy Server User Interface registration.

Download the SiteMinder Schema Files

One or more of the schema files required to configure the SiteMinder schema are not included as part of the Policy Server installation. These files are located in the CA SiteMinder Tier 2 Directories product components download.

To download the tier 2 directories product components

1. Log into the Technical Support site.
2. Under Support, click Download Center.

   The Download Center screen appears.
3. Type SiteMinder in the Select a Product field.

4. Select a release from the Select a Release list.
5. Select a service pack from the Select a Gen Level list.
6. Click Go.

   The Product Downloads screen appears. The tier 2 directory components download is at the bottom of the list.
7. Save the zip file locally and extract the file to the Policy Server host system.

Create the SiteMinder Schema

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

To create SiteMinder schema in a MySQL database

1. Navigate to *path*\MySQL.

   path

   Specifies the path to the schema files extracted from the tier 2 directory zip.
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 into a query and execute the query.

   The policy and key store schema is created.

   Note: You can also use this schema file to create a stand–alone 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.

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 Store Key Information in MySQL (see page 48)
How to Store Audit Logs in MySQL (see page 51)
How to Store Session Information in MySQL (see page 54)
How to Configure a MySQL User Store (see page 57)

Create a MySQL Data Source on Windows

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

To create the MySQL data source

1. Log into the Policy Server host system.
2. Open the ODBC Data Source Administrator.
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. Do the following 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 should use to connect to the database functioning as the policy store.

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

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.

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 Policy Store from the Database list.

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 25 connection default for best performance.
7. Click Apply.

   The settings are saved.
8. Select Key Store from the Database list.

   Data source information appears.
9. Select the Use the policy store database check box and click Apply.
10. Select Audit Logs from the Database list.

    Data source settings appear.
11. Select the Use the policy store database check box and click Apply.
12. Click Test Connection.

    SiteMinder returns a confirmation that the Policy Server can access the data store.
13. 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`*

   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 Policy Server User Interface for the first–time. You can use the default super user to create an administrator with super user permissions.

Import the Default Policy Store Objects

Importing the default policy store objects sets up the policy store for use with the Policy Server User Interface. 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, run the following command

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

Note: 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

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

Restart the Policy Server

You restart the Policy Server for the policy store or other data store settings to take effect.

Note: UNIX systems can use the stop-all followed by the start-all commands to restart the Policy Server.

To restart the Policy Server

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.

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. Download the SiteMinder schema files.
3. Gather database information.
4. Create the key store schema.
5. Configure a MySQL data source for SiteMinder.
6. Point the Policy Server to the database.
7. Restart the Policy Server.

More information:

Gather Database Information (see page 37)
Configure a MySQL Data Source for SiteMinder (see page 40)

Download the SiteMinder Schema Files

One or more of the schema files required to configure the SiteMinder schema are not included as part of the Policy Server installation. These files are located in the CA SiteMinder Tier 2 Directories product components download.

To download the tier 2 directories product components

1. Log into the Technical Support site.
2. Under Support, click Download Center.

   The Download Center screen appears.
3. Type SiteMinder in the Select a Product field.
4. Select a release from the Select a Release list.
5. Select a service pack from the Select a Gen Level list.
6. Click Go.

   The Product Downloads screen appears. The tier 2 directory components download is at the bottom of the list.
7. Save the zip file locally and extract the file to the Policy Server host system.

Create the Key Store Schema

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

To create the key store schema

1. Navigate to *path*\MySQL.

   path

   Specifies the path to the schema files extracted from the tier 2 directory zip.
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 key store.

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

   ```
   DROP FUNCTION IF EXISTS `smkeystore`.`getdate` $$
   CREATE FUNCTION `smkeystore`.`getdate` () RETURNS DATE
   ```
5. Copy the contents of the entire file.

6. 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 the policy store or other data store settings to take effect.

Note: UNIX systems can use the stop-all followed by the start-all commands to restart the Policy Server.

To restart the Policy Server

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.

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

More information:

Gather Database Information (see page 37)
Configure a MySQL Data Source for SiteMinder (see page 40)

Download the SiteMinder Schema Files

One or more of the schema files required to configure the SiteMinder schema are not included as part of the Policy Server installation. These files are located in the CA SiteMinder Tier 2 Directories product components download.

To download the tier 2 directories product components

1. Log into the Technical Support site.
2. Under Support, click Download Center.

   The Download Center screen appears.
3. Type SiteMinder in the Select a Product field.
4. Select a release from the Select a Release list.
5. Select a service pack from the Select a Gen Level list.
6. Click Go.

   The Product Downloads screen appears. The tier 2 directory components download is at the bottom of the list.
7. Save the zip file locally and extract the file to the Policy Server host system.

Create the Audit Log Schema

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

To create the audit log schema

1. Navigate to *path*\MySQL.

   path

   Specifies the path to the schema files extracted from the tier 2 directory zip.
2. Open the following file in a text editor:

   sm_mysql_logs.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 audit store.

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

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

5. Copy the contents of the entire file.
6. 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 the policy store or other data store settings to take effect.

Note: UNIX systems can use the stop-all followed by the start-all commands to restart the Policy Server.

To restart the Policy Server

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.

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. Download the SiteMinder schema files.
3. Gather database information.
4. Create the session store schema.
5. Configure a MySQL data source for SiteMinder.
6. Point the Policy Server to the database.
7. Restart the Policy Server.

More information:

Gather Database Information (see page 37)
Configure a MySQL Data Source for SiteMinder (see page 40)

Download the SiteMinder Schema Files

One or more of the schema files required to configure the SiteMinder schema are not included as part of the Policy Server installation. These files are located in the CA SiteMinder Tier 2 Directories product components download.

To download the tier 2 directories product components

1. Log into the Technical Support site.
2. Under Support, click Download Center.

   The Download Center screen appears.
3. Type SiteMinder in the Select a Product field.
4. Select a release from the Select a Release list.
5. Select a service pack from the Select a Gen Level list.
6. Click Go.

   The Product Downloads screen appears. The tier 2 directory components download is at the bottom of the list.
7. Save the zip file locally and extract the file to the Policy Server host system.

Create the Session Store Schema

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

To create the session store schema

1. Navigate to *path*\MySQL.

   path

   Specifies the path to the schema files extracted from the tier 2 directory zip.
2. Open the following file in a text editor:

   sm_mysql_ss.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 session store.

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

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

5. Copy the contents of the entire file.
6. 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 the policy store or other data store settings to take effect.

Note: UNIX systems can use the stop-all followed by the start-all commands to restart the Policy Server.

To restart the Policy Server

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.

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 40)

Import the SiteMinder Sample Users

Importing the SiteMinder sample users is optional. You import these users to populate the database with fictional SiteMinder users.

To import the SiteMinder sample users

1. Navigate to *path*\MySQL.

   path

   Specifies the path to the schema files extracted from the tier 2 directory zip.
2. Open the following file in a text editor:

   smsampleusers_mysql.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 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
   ```

5. Copy the contents of the entire file.
6. 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.
7. Configure the user directory connection to the Policy Server.

Configure MySQL Server Directory Connections

You configure a user directory connection to let the Policy Server communicate with a MySQL Server user store.

To connect the user store

1. Click Edit, System Configuration, Create User Directory.

   The User Directories Properties dialog appears with the Directory Setup tab open.
2. Complete the following:
   - Enter the user directory name in Name field.
   - Select ODBC from the NameSpace list.
   - Enter the data source name in the Data Source field.
   - Select a SQL query scheme from the SQL Query Scheme list.

     Note: If you have not created a SQL query scheme, click New. More information on creating SQL query schemes exists in the *Policy Design Guide*.
3. Click the Credentials and Connection tab.

   The Credentials and Connection tab opens.
4. Complete the following:
   a. Select Require Credentials.
   b. Type *root* in the Username field.
   c. Enter the administrator password in the Password and Confirm Password fields.

5. Click the User Attributes tab.

   The User Attributes tab opens.

6. Specify the database attribute record attributes that correspond to the following fields:

   - Universal ID (R)

     Example: Name

   - Disabled Flag (RW)

     Example: Disabled

   - Password Attribute (RW)

     Example: Password

   - Password Data (RW)

     Example: PasswordData

7. Click OK.

   SiteMinder saves the user directory settings, and the user directory appears in the User Directory List.

Chapter 8: Oracle Internet Directory Server

This section contains the following topics:

Policy Store Schema Considerations

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

- smpolicy.smdif
- smpolicy-secure.smdif

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

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

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

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

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

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

Create a SiteMinder 5.5 or 6.0 Policy Store in Oracle Internet Directory (OID) Directory Server

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

To create the required SiteMinder 5.5 or 6.0 policy store schema in OID Directory Server

1. Create a domain in OID using the ODM by right-clicking Entry Management and selecting Create.
2. In the Distinguished Name dialog:
   a. Click Add.
   b. Select the domain.
3. Enter:
   a. **dc=dcbok** for the Distinguished Name value.
   b. **dc** for the dc value.
4. Do the following:
   a. Create an organizational unit.
   b. Select the organizational unit.
   c. Enter **ou=bok,dc=dcbok** for Distinguished Name value and **bok** for the ou value.
5. Point the Policy Server at the OID Directory Server that you plan to use as a policy store by following the instructions in the *Policy Server Installation Guide*.

   The following are sample values you can enter on the Data tab of the 6.0 Policy Server Management Console. You can use similar values for 5.5:

   Database

   Policy Store

Storage

LDAP

LDAP IP Address

192.168.122.18:389

Admin Username

oracleadmin

Root DN

ou=ps6,dc=CA

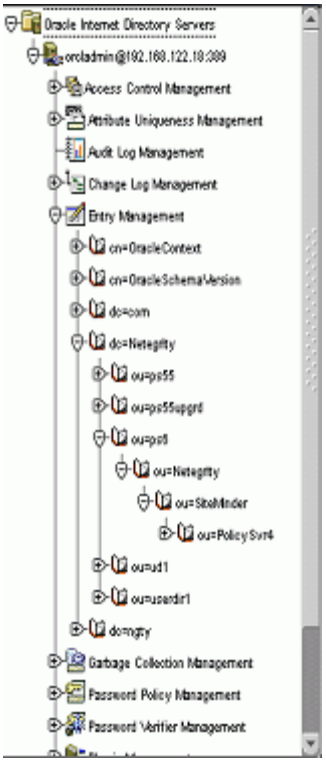
6. Create the schema file, using the Policy Server's smldapsetup utility. On the system where the Policy Server is installed, use the command prompt to go to <nete_ps_root>\bin. Run the following command:

```
smldapsetup ldgen -fpstoreschema.ldif
```

7. Import the schema you created in to the policy store server by running the following command:

```
smldapsetup ldmod -fpstoreschema.ldif
```

8. In OID, to confirm that you have performed the steps correctly, the base tree structure that holds the policy store data looks like the following:



9. Confirm that the Policy Server is pointing to the OID policy store by using the Data tab of the Policy Server Management Console. For detailed instructions, see the *Policy Server Management Guide*.
10. Import the base policy store data from the file smpolicy.smdif:

    ```
    smobjimport -i<siteminder_installation>\db\smdif\smpolicy.smdif -v
    ```

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

    - smpolicy.smdif
    - smpolicy–secure.smdif

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

Connect to an OID User Directory

To configure the Policy Server to use an OID user directory

1. In OID:
    a. Create another organizational unit (for example, OracleSchemaVersion) under a domain and follow the instructions from step 4 in Create a SiteMinder 5.5 or 6.0 Policy Store in Oracle Internet Directory (OID) Directory Server (see page 62).
    b. Enter a Distinguished Name. For example, **ou=people,cn=OracleSchemaVersion**.
2. To add users to the organizational unit under the same domain as mentioned in step 4 in Create a SiteMinder 5.5 or 6.0 Policy Store in Oracle Internet Directory (OID) Directory Server (see page 62):
    a. Repeat steps 1 and 2 from that section.
    b. Instead of adding a domain, click **Add** and choose **inetOrgPerson**.
3. In the Mandatory Properties tab enter:
    a. **cn=user1**
    b. **sn =user1**
    c. **uid=user1**
    d. **userpassword=user1**
    e. dn as **cn=user1,ou=people,cn=OracleSchemaVersion**
4. Create a user directory in the Policy Server and use the Policy Server Management Console to connect to the user directory.

The Credentials and Connection Tab

To access the users on an SSL port, open the User Directories Properties dialog, click the Credentials and Connection tab, and select Secure Connection.

The User Attributes Tab

Following are sample values for the User Attributes tab on the User Directories Properties dialog:

- Name: ud1
- Universal ID (R): uid
- Disabled Flag (RW): carLicense
- Password Attribute (RW): userPassword
- Password Data (RW): audio
- Challenge Response (RW): jpegPhoto

LDAP Referral Limitation for OID User Directory

LDAP referrals do not work when an Oracle Internet Directory Directory Server is configured as a user store and enhanced referrals are enabled. This limitation is an OID limitation.

SiteMinder SSL Configuration for OID

To configure SiteMinder to use encryption (SSL) when communicating with the OID Directory

1. Install the certificate Authority's (CA) root certificate into the Netscape cert7.db database on each machine that expects to use SSL to communicate with the OID directory.

   Note: SiteMinder requires the certificate to be in a Netscape version file format (cert7.db), so do not use Microsoft Internet Explorer to install the certificate.

2. Configure the SiteMinder Policy Server to use SSL by entering the following values on the Data tab from the Policy Server Management Console:
   - Database: Policy Store
   - Storage: LDAP
   - LDAP IP Address: 192.168.122.18:636
   - Admin Username: cn=orcladmin
   - Root DN: ou=ps6,dc=Netegrity

Note: If you have not done so previously, configure SSL communication to the user store by checking "Secure Connection" on the Credentials and Connection tab of the User Directories Properties dialog.

Chapter 9: OpenWave Directory Server 6.0.1

This section contains the following topics:

Policy Store Schema Considerations

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

- smpolicy.smdif
- smpolicy-secure.smdif

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

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

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

Parameter Name	Value in smpolicy.smdif	Value in smpolicy-secure.smdif
BadCssChars	No value	<, >, ', ;,), (, &, +, %00
BadQueryChars	No value	<, >, ', ;,), (, &, +, %00
BadUrlChars	//, ./, /., /*, *., ~, \, %00-%1f, %7f-%ff, %25	smpolicy.smdif values plus: <, >, ', ;,), (, &, +
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	smpolicy.smdif values plus .jsp

ValidTargetDomain	Note: This parameter does not exist in smpolicy.smdif.	Provide a valid redirection domain as follows: validtargetdomain=".example.com"

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

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

Create a SiteMinder 6.0 Policy Store in an Openwave Directory Server

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

To create a policy store in a Openwave directory server

1. Point the Policy Server at the directory by doing the following:
   a. In the Database drop-down menu, select Policy Store.
   b. In the Storage drop-down menu, select LDAP.
   c. In the LDAP Policy Store box, configure the fields for the LDAP policy store.

      The following lists sample values for the fields:

      - LDAP IP Address: 123.123.12.12:3500
      - Root DN: o=nete,c=us
      - Admin Username: cn=root
      - Password: <masked password>

      Note: Refer to the *Policy Server Management Guide* for a complete description of the LDAP settings.

   d. Click Apply after you have modified the LDAP fields.
   e. Click the Test LDAP Connection button to test the connection.

   If the connection is successful, SiteMinder returns a confirmation. If it is not successful, SiteMinder returns an error message. If you receive an error message, verify that the values you entered are correct and that the directory is running.
2. Copy the supplied schema.txt into *<siteminder_installation>*\bin directory.

3. Execute the following command from the <*siteminder_installation*>\bin directory:

   ```
   smldapsetup ldmod -fschema.txt
   ```

4. On the machine where Openwave Directory Server is installed, log in to the primary master directory server as the directory user.
5. For the supplied index.sql file:
   a. Edit the file by changing the path for the tablespace creation.
   b. Place the file in the home directory.
6. Execute the following command:
   ```
   sqlplus /nolog
   ```
7. At the sql prompt, run the following commands:

   ```
   conn <directory user name>/<directory user password>
   @index.sql
   ```

8. Execute the following Openwave command:

   ```
   imconfedit
   ```

9. Do the following:
   a. Find the configuration key /*/common/tableMapping:
   b. At the end of this key, add the contents of the supplied tablemap.txt file.
10. Save the file and restart the directory server.
11. To check whether the server has started properly, execute the following command:

    ```
    imservping imdirserv
    ```

12. On the Policy Server machine, change the SiteMinder Super User password by completing the following steps:
    a. Copy smreg from either \win32\tools or solaris/tools on the SiteMinder CD-ROM to <*siteminder_installation*>\bin.
    b. Execute the following command:

       smreg -su <*superuserpassword*>

       where <*superuserpassword*> is the password for the SiteMinder Super User account.

       Note: Ensure there is a space between -su and the <*superuserpassword*>.
    c. Delete smreg.exe.

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

13. From <*siteminder_installation*>/bin, import the basic SiteMinder objects required to set up a policy store by running:

    ```
    smobjimport -i<siteminder_installation>\db\smdif\smpolicy.smdif
    -d<SM_Super_User_Name> -w<superuserpassword> -v
    ```

    siteminder_installation

    Specifies the installed location of SiteMinder.

    smpolicy.smdif

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

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

    - smpolicy.smdif
    - smpolicy–secure.smdif

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

    SM_Super_User_Name

    Specifies the Super User name of the SiteMinder administrator.

    superuserpassword

    Specifies the password for the SiteMinder Super User.

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

    Windows Systems:

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

    UNIX Systems:

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

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

Connect to an Openwave Policy Store

To connect to the Openwave policy store, follow the instructions in the *Policy Server Installation Guide*.

Connect to an Openwave User Directory

To configure SiteMinder to use an Openwave user directory

1. From the Policy Server user interface, click Edit > Create User Directory.

   The User Directory Properties dialog appears.

2. Enter values for the following fields in Directory Setup tab:

   - Server
   - Root
   - Start
   - End

3. Click Apply.

   The values are saved.

4. Click Credentials and Connections.

   The Credentials and Connections tab moves to the front.

5. Select Require Credentials, and enter the required values.

   Note: Enter the full DN of the administrative user in the Username field.

6. Click Apply.

   The values are saved.

7. Click the User Attributes tab.

   The User Attributes tab moves to the front.

8. Complete the user attribute values, and click Apply.

   The values are saved.

9. Click OK.

   The User Directory Properties dialog closes and the Policy Server is configured to use the Openwave user directory.

SiteMinder SSL Configuration for Openwave

If you have not done so previously, configure SSL communication to the user store by checking.

To configure SSL communication

1. Right-click the user directory from the User Directory List, and click Properties of User Directory.

   The User Directory Properties dialog appears.

2. Click the Credentials and Connection tab.

   The Credentials and Connection tab moves to the front.

3. Select Secure Connection, and click OK.

   SSL communication to the user store is set.

LDAP Referrals

The Openwave Directory Server does not support LDAP referrals.

Chapter 10: Siemens DirX 6.0 D00 Directory Server

This section contains the following topics:

Policy Store Schema Considerations

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

- smpolicy.smdif
- smpolicy-secure.smdif

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

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

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

Parameter Name	Value in smpolicy.smdif	Value in smpolicy-secure.smdif
BadCssChars	No value	<, >, ', ;,), (, &, +, %00
BadQueryChars	No value	<, >, ', ;,), (, &, +, %00
BadUrlChars	//, ./, /., /*, *., ~, \, %00-%1f, %7f-%ff, %25	smpolicy.smdif values plus: <, >, ', ;,), (, &, +
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	smpolicy.smdif values plus .jsp

ValidTargetDomain	Note: This parameter does not exist in smpolicy.smdif.	Provide a valid redirection domain as follows: validtargetdomain=".example.com"

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

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

Create a SiteMinder 6.0 Policy Store in DirX Directory Server

Use these procedures to configure the Policy Server with a Siemens DirX 6.0 D00 on Windows 2000 SP4 Advanced Server.

Note: This procedure uses script files to help with Policy Store configuration. Download the files from the Technical Support Site (https://support.netegrity.com).

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

To create the required SiteMinder 6.0 policy store schema in Siemens DirX 6.0 D00 Directory Server

1. Install DirX 6.0 D00.

   If you do not have an existing database, install the example database.

   Accept all the defaults during the install.

2. Copy the following files to:

   <DirX_ install_ path>\scripts\security\Netegrity\SiteMinder

   Example: C:\program files\siemens\dirx\scripts\security\Netegrity\SiteMinder

   ```
   schema_ext_for_SiteMinder60.adm
   l-bind.cp
   subschema_ext_for_SiteMinder60.cp
   _setup.bat
   setup.bat
   bind.tcl
   GlobalVar.tcl
   ```

3. Rename the following files by removing the characters 6*n* from the file names:
   - schema_ext_for_SiteMinder60.adm becomes schema_ext_for_SiteMinder.adm
   - subschema_ext_for_SiteMinder60.cp becomes subschema_ext_for_SiteMinder.cp
4. Copy dirxabbr-ext.Siteminder60 to <DirX_install_path>\client\conf.
5. Rename dirxabbr-ext.Siteminder60 to dirxabbr-ext.Siteminder.
6. Stop and start the DirX service.
7. Edit GlobalVar.tcl to change to the global variables the DirX scripts reference. These are some of the default values:
   - Root DN: o=pqr
   - Admin username: cn=admin,o=pqr
   - Admin password: dirx
   - LDAP port: 389
8. Run setup.bat.

   Check the resulting log file, setup.txt, for errors.
9. Rebind to the DSA using the DirXmanage tool. Watch for potential errors.
10. In DirX, create the base tree structure to hold the policy store data. Use the DirXmanage tool to create the following organizational units:
    a. Under o=PQR, create:

       ```
       OU=Netegrity
       ```

    b. Under ou=Netegrity, create:

       ```
       OU=SiteMinder
       ```

    c. Under ou=SiteMinder, create:

       ```
       OU=PolicySvr4
       ```
11. Use the Data tab of the Policy Server Management Console to point SiteMinder to the DirX directory that you installed.

12. Import the base policy store data from the file smpolicy.smdif into DirX. If you need to import from an existing policy store, refer to the *Policy Server Installation Guide* section on migrating policy store data.

    ```
    $ smobjimport -i<siteminder_installation>\db\smdif\smpolicy.smdif -v
    ```

    You can pipe smobjimport output to a log file. After the policy store data import is complete, you can check the log file for errors.

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

    - smpolicy.smdif
    - smpolicy–secure.smdif

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

13. Set the Siteminder admin password:

    ```
    smreg -su <password>
    ```

14. Configure the Siteminder policy server to point to DirX:
    - LDAP IP Address: 123.456.7.8
    - Root DN: o=pqr
    - Admin username: cn=admin,o=pqr
    - Admin password: ********

Connect to a DirX Policy Store

To connect to the DirX Policy Store, follow the instructions in the section "Configure Policy Servers to Use an LDAP Policy Store or Key Store," in the "Set up the Policy Store on *<os_platform>*" chapter in the *Policy Server Installation Guide*.

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.

Upgrade a 5.5 Policy Store to a 6.0 Policy Store

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

To upgrade a 5.5 policy store to a 6.0 policy store

1. On the server having the SiteMinder 5.5 policy store, copy the following files in the Siemens_DirX folder, in <*DirX_ install_path*>\scripts\security\Netegrity\SiteMinder:
   - setup-upgrade.bat
   - dirxabbr-ext.SiteMinder55to60
   - schema_ext_for_SiteMinder55to60.adm
   - subschema_ext_for_SiteMinder55to60.cp
2. Do not to delete the schema files for 5.5 policy store, which are already there in that folder:
   - dirxabbr-ext.SiteMinder55,
   - schema_ext_for_SiteMinder55.adm,
   - subschema_ext_for_SiteMinder55.cp
3. Copy dirxabbr-ext.Siteminder55to60 to <*DirX_install_path*>\client\conf.
4. Run setup-upgrade.bat.

5. Check the resulting log file, setup.txt, for errors.
6. Rebind to the DSA using the DirXmanage tool. Watch for potential errors.
7. Point SiteMinder 6.0 policy server to the existing 5.5 policy store on which the schema was upgraded.
8. Import the base policy store data for upgrade from 5.5 to 6.0 from the file sm_upgrade_55_to_60.smdif. For example:

```
smobjimport -i<siteminder_installation>\db\smdif\ sm_upgrade_55_to_60.smdif -v
-f
```

Chapter 11: Siemens DirX EE 1.0 Directory Server

This section contains the following topics:

Policy Store Schema Considerations

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

- smpolicy.smdif
- smpolicy-secure.smdif

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

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

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

Parameter Name	Value in smpolicy.smdif	Value in smpolicy-secure.smdif
BadCssChars	No value	<, >, ', ;,), (, &, +, %00
BadQueryChars	No value	<, >, ', ;,), (, &, +, %00
BadUrlChars	//, ./, /., /*, *., ~, \, %00-%1f, %7f-%ff, %25	smpolicy.smdif values plus: <, >, ', ;,), (, &, +
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	smpolicy.smdif values plus .jsp

ValidTargetDomain	Note: This parameter does not exist in smpolicy.smdif.	Provide a valid redirection domain as follows: validtargetdomain=".example.com"

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

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

Create a SiteMinder 6.0 Policy Store in a DirX Directory Server

Use these procedures to configure the Policy Server with a Siemens DirX EE 1.0 directory server on Windows 2000 SP 4 Advanced Server.

Note: This procedure uses script files to help with Policy Store configuration. Download the files from the Technical Support Site (https://support.netegrity.com).

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

To create the required SiteMinder 6.0 policy store schema in Siemens DirX EE 1.0 Directory Server

1. Install DirX EE 1.0.
2. Keep the Siemens_DirXEE folder in

   <DirX EE_Installation_Path>\scripts\Stand_alone\

   The folder contains the following files:

   - dirxabbr-ext.SiteMinder60,
   - schema_EE_ext_for_SiteMinder60.adm,
   - subschema_ext_for_SiteMinder60.cp,
   - bind.tcl,
   - GlobalVar.tcl,
   - initialize_DSA.cp,
   - setup.bat
3. Copy dirxabbr-ext.Siteminder60 to <DirX_install_path>\client\conf.
4. Run setup.bat.

5. Check the resulting log file, setup.txt, for errors.
6. Rebind to the DSA using the DirXmanage, through the administrator of DSA (cn=admin,o=My-Company), to download all classes attribute types and nameforms from the DSA schema. Then, bind through the user (cn=user,o=My-Company). Watch for potential errors.

   (Solaris Only)

   a. Run setup.sh and answer yes to the first two questions
   b. Open another terminal window. Use dirxadm to bind as admin, stop the server, then start the server
   c. Go back to the terminal window running setup.sh and answer yes to the last question.

      This creates a log file (setup.log). Check in this file for errors.
7. In DirX, create the base tree structure to hold the policy store data. Use the DirXmanage tool to create the following organizational units:

   a. Under o=My-Company, create:

      ```
      OU=Netegrity
      ```

   b. Under ou=Netegrity, create:

      ```
      OU=SiteMinder
      ```

   c. Under ou=SiteMinder, create:

      ```
      OU=PolicySvr4
      ```
8. Use the Data tab of the Policy Server Management Console to point SiteMinder to the DirX directory that you set up.
9. Import the base policy store data from the file smpolicy.smdif into DirX. If you need to import from an existing policy store, refer to the *Policy Server Installation Guide* section on migrating policy store data.

   ```
   $ smobjimport -i<siteminder_installation>\db\smdif\smpolicy.smdif -v
   ```

   You can pipe smobjimport output to a log file. After the policy store data import is complete, you can check the log file for errors.

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

   - smpolicy.smdif
   - smpolicy–secure.smdif

   The file named smpolicy–secure provides additional security through enhanced default Web Agent configuration parameters.
10. Set the Siteminder admin password:

    ```
    smreg -su <password>
    ```

11. Configure the Siteminder policy server to point to DirX:
    - LDAP IP Address: 123.456.7.8
    - Root DN: o=My-Company
    - Admin username: cn=admin,o=My-Company
    - Admin password: direx

Connect to a DirX Policy Store

To connect to the DirX Policy Store, follow the instructions in the *Policy Server Installation Guide*.

Sample User Directory Settings--Siemens DirX EE 1.0

The following are sample user directory settings:

Directory Setup

- Namespace: LDAP
- Server: 123.456.7.8
- Root: o=My=Company
- DN Lookup Start: (cn=
- DN Lookup End:)

Credentials and Connection

- Admin Username: cn=admin,o=My-Company
- Admin Password: dirx

User Attributes

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

Upgrade a 5.5 Policy Store to a 6.0 Policy Store

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

To upgrade a 5.5 policy store to a 6.0 policy store

1. On the server that has the SiteMinder 5.5 policy store, copy the following files in the Siemens_DirX folder, in <*DirX_install_path*>\scripts\security\Netegrity\SiteMinder:
   - setup-upgrade.bat
   - dirxabbr-ext.SiteMinder55to60
   - schema_EE_ext_for_SiteMinder55to60.adm
   - subschema_ext_for_SiteMinder55to60.cp
2. Do not to delete the schema files for 5.5 policy store, which are already there in that folder:
   - dirxabbr-ext.SiteMinder55
   - schema_EE_ext_for_SiteMinder55.adm
   - subschema_ext_for_SiteMinder55.cp
3. Copy dirxabbr-ext.Siteminder55to60 to <*DirX_install_path*>\client\conf.
4. Run setup-upgrade.bat.
5. Check the resulting log file, setup.txt, for errors.
6. Rebind to the DSA using the DirXmanageusing DirXmanage, through the administrator of DSA (cn=admin,o=My-Company), to download all classes attribute types and nameforms from the DSA schema. Then bind through the user (cn=user,o=My-Company). Watch for potential errors.
7. Point SiteMinder 6.0 policy server to the existing 5.5 policy store on which the schema was upgraded.
8. Import the base policy store data for upgrade from 5.5 to 6.0 from the file sm_upgrade_55_to_60.smdif. For example:

```
smobjimport -i<siteminder_installation>\db\smdif\ sm_upgrade_55_to_60.smdif -v
-f
```

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 92).
    - 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. Ensure you are working from the bin directory of the NSS utility or you may 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. For more information, see the release notes for your SiteMinder component.

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. Ensure you are working from the bin directory of the NSS utility or you may 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. For more information, see the release notes for your SiteMinder component.

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. Ensure you are working from the bin directory of the NSS utility or you may 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. For more information, see the release notes for your SiteMinder component.

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. Ensure you are working from the bin directory of the NSS utility or you may 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 Policy Server User Interface, 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 Policy Server User Interface.
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 Policy Server User Interface, 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, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the 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 Policy Server User Interface, use ASCII characters. Object creation or modification with non-ASCII characters is not supported.

To verify the SSL connection

1. Log in to the Policy Server User Interface.
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.

Index

T

U

V

W