CA™ SOA Security Manager

Directory Configuration Guide

r12.1

Second Edition

CA Product References

This document references the following CA products:

- CA SOA Security Manager
- CA SiteMinder® Web Access Manager Federation Security Services

Contact CA

Contact Technical 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 also available on the CA Support website, found at http://ca.com/docs.

Contents

Chapter 1: About this Guide 9

Directory Configuration Overview 9

Chapter 2: Critical Path inJoin Directory Server v4.2 11

Configure an inJoin Directory Server as a Policy Store 11
Import the Policy Store Data Definitions 14
Point the Policy Server to the Policy Store 15
Enable LDAP Tracing in IDS 15
Configure an SSL Connection 16
Sample User Directory Settings--Critical Path InJoin Directory Server 18
Sample Policy Server Settings--Critical Path InJoin Directory Server 19
Upgrade a 5.5 Policy Store 19
Import the Policy Store Data Definitions 22
How to Upgrade a 6.x Policy Store 23
- Extend the inJoin Policy Store Schema 23
- Import the Base Policy Store Objects 25
- Import the Policy Store Data Definitions 27

Chapter 3: IBM DB2 29

How to Configure an IBM DB2 Database as a Data Store 29
- Create a DB2 Database with SiteMinder Schema 29
- Configure a DB2 Data Source for SiteMinder 30
- Import the Default Policy Store Objects 34
- Import the Policy Store Data Definitions 36

Upgrade a 6.x Session Server 36
How to Upgrade a 6.x Policy Store 37
- Extend the IBM DB2 Policy Store Schema 38
- Import the Base Policy Store Objects 38
- Import the Policy Store Data Definitions 40

Chapter 4: IBM Directory Server 43

IBM Directory Server as a Policy Store 43
- IBM Directory Server 43
- Gather Directory Server Information 45
- How to Configure the Policy Store 45

Upgrade a 5.x IBM Directory Server Policy Store 52

How to Upgrade an IBM Secureway Directory Policy Store . . . 52
Upgrade Limitations for IBM Secureway Directory Server Policy Stores . . . 60
How to Upgrade a 6.x Policy Store . . . 61
Extend the IBM Directory Server Policy Store Schema . . . 61
Import the Base Policy Store Objects . . . 62
Import the Policy Store Data Definitions . . . 64

Chapter 5: MySQL Server 65

How to Set Up a MySQL Server . . . 65
Install the MySQL Connector . . . 65
Assign Root User Privileges . . . 65
Create a MySQL Data Source . . . 66
How to Configure a Connection from the Policy Server to a MySQL Server User Store . . . 67
Create a Sample User Store . . . 67
Configure MySQL Server Directory Connections . . . 67

Chapter 6: Novell eDirectory 69

Novell eDirectory as a Policy Store . . . 69
Gather Directory Server Information . . . 69
How to Configure the Policy Store . . . 70
Limitations of Policy Store Objects in Novell eDirectory . . . 78
Upgrade a 5.x Novell eDirectory Policy Store . . . 78
How to Upgrade a Novell eDirectory Policy Store . . . 78
How to Upgrade a 6.x Policy Store . . . 85
Edit the Novell XPS Schema File . . . 86
Extend the Novell Policy Store Schema . . . 87
Import the Base Policy Store Objects . . . 87
Import the Policy Store Data Definitions . . . 90

Chapter 7: Oracle Internet Directory Server 91

Oracle Internet Directory as a Policy Store . . . 91
Gather Directory Server Information . . . 91
How to Configure the Policy Server . . . 92
How to Upgrade an Oracle Internet Directory Policy Store . . . 99
Gather Directory Server Information . . . 100
Gather SiteMinder Information . . . 101
Create the Policy Store Schema . . . 101
Import the Base Policy Store Objects . . . 103
Import the Policy Store Data Definitions . . . 105
Restart the Policy Server . . . 106
Set Oracle Internet Directory Attributes . . . 106

How to Upgrade a 6.x Policy Store . . . 107
Extend the Oracle Internet Directory Policy Store Schema . . . 107
Import the Base Policy Store Objects . . . 109
Import the Policy Store Data Definitions . . . 111

Chapter 8: OpenLDAP Server 113

How to Configure the Slapd Configuration File . . . 113
Specify the SiteMinder Schema Files . . . 113
Enable User Authentication . . . 114
Specify Database Directives . . . 114
Support Client-Side Sorting . . . 115
Test the Configuration File . . . 116
Restart the OpenLDAP Server . . . 117
How to Create the Database . . . 117
Create the Base Tree Structure . . . 117
Add Entries . . . 118
How to Configure the Directory Server as a Policy Store . . . 118
Point the Policy Server to the Directory Server . . . 119
Create the Policy Store . . . 120
Import the Policy Store Data Definitions . . . 122
How to Configure the Directory Sever as a User Store . . . 122
Create a User Store . . . 123
Configure a Connection from the Policy Server to an OpenLDAP User Store . . . 123
Configure SSL for a Policy Store . . . 124
How to Upgrade a 6.x Policy Store . . . 125
Extend the OpenLDAP Policy Store Schema . . . 126
Import the Base Policy Store Objects . . . 127
Import the Policy Store Data Definitions . . . 129
Troubleshooting OpenLDAP . . . 130
Cyrus SASL Installation . . . 130
Berkeley Database Version Mismatch Errors . . . 130
Building and Installing openSSL . . . 130

Chapter 9: OpenWave Directory Server 6.0.1 131

Configure an OpenWave Directory Server as a Policy Store . . . 131
Import the Policy Store Data Definitions . . . 135
Connect to an OpenWave Policy Store . . . 135
Configure a Connection from the Policy Server to an OpenWave Directory User Store . . . 136
How to Upgrade a 6.x Policy Store . . . 138
Extend the OpenWave Directory Server Policy Store Schema . . . 138
Import the Base Policy Store Objects . . . 139

Import the Policy Store Data Definitions . . . 141
LDAP Referrals . . . 142

Chapter 10: Siemens DirX 6.0 D00 Directory Server 143

Configure a DirX 6.0 D00 Directory Server as a Policy Store . . . 143
Import the Policy Store Data Definitions . . . 146
Sample User Directory Settings--Siemens DirX 6.0 . . . 147
Upgrade a 5.5 Policy Store . . . 148
Import the Policy Store Data Definitions . . . 151
How to Upgrade a 6.x Policy Store . . . 152
Extend the Siemens DirX Policy Store Schema . . . 152
Import the Base Policy Store Objects . . . 153
Import the Policy Store Data Definitions . . . 156

Chapter 11: Siemens DirX EE 2.0 Directory Server 157

How to Configure a Siemens DirX EE 2.0 Policy Store . . . 157
Configure a DirX EE 2.0 Directory Server as a r12.1 Policy Store . . . 157
Import the Policy Store Data Definitions . . . 160
How to Upgrade a Siemens DirX EE 2.0 Policy Store . . . 160
Upgrade a DirX EE 2.0 Policy Store from 6.x to r12.1 . . . 161
Import the Policy Store Data Definitions . . . 162

Appendix A: Configuring SOA Security Manager Connections over SSL 163

How to Configure an LDAP User Directory Connection over SSL . . . 163
Before You Configure a Connection over SSL . . . 164
Install the NSS Utility . . . 165
Create the Certificate Database Files . . . 165
Add the Root Certificate Authority to the Certificate Database . . . 166
Add the Server Certificate to the Certificate Database . . . 168
List the Certificates in the Certificate Database . . . 169
Configure the User Directory Connection for SSL . . . 170
Point the Policy Server to the Certificate Database . . . 171
Verify the SSL Connection . . . 171

Index 173

Chapter 1: About this Guide

This section contains the following topics:

Directory Configuration Overview (see page 9)

Directory Configuration Overview

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

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

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

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

Chapter 2: Critical Path inJoin Directory Server v4.2

This section contains the following topics:

Configure an inJoin Directory Server as a Policy Store (see page 11)
Import the Policy Store Data Definitions (see page 14)
Point the Policy Server to the Policy Store (see page 15)
Enable LDAP Tracing in IDS (see page 15)
Configure an SSL Connection (see page 16)
Sample User Directory Settings--Critical Path InJoin Directory Server (see page 18)
Sample Policy Server Settings--Critical Path InJoin Directory Server (see page 19)
Upgrade a 5.5 Policy Store (see page 19)
Import the Policy Store Data Definitions (see page 22)
How to Upgrade a 6.x Policy Store (see page 23)

Configure an inJoin Directory Server as a Policy Store

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

To configure a Critical Path inJoin Directory Server (IDS) as a policy store

1. Start the DSA.
2. Navigate to policy_server_home\bin on the machine where the Policy Server is installed.

   policy_server_home

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

   ldapmodify -h*host* -p*port* -d*AdminDN* -w*AdminPW* -c
   -f*dir_config_home*\criticalpath\IDS_Add_Schema_R12sp1.ldif

   -h host

   Specifies the IP address of the LDAP server.

   -p port

   Specifies the port number of the LDAP server.

-d AdminDN

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

Example: cn=manager

-w AdminPW

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

-c

Specifies continuous mode (do not stop on errors).

-f

Specifies the path and name of the schema file that is supplied with r12.1.

dir_config_home

Specifies the Directory Configuration installation path.

Note: ldapmodify requires version 4.2 of the Critical Path inJoin Directory Server.

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

   ldapmodify -h*host* -p*port* -d*AdminDN* -w*AdminPW* -c
   -f*dir_config_home*\xps\criticalpath\CriticalPath.ldif

   -f

   Specifies the path and name of the XPS schema file that is supplied with r12.1.

6. Reload the schema, or verify that the schema has been updated.
7. Go to dsa, comms, LDAP, change the "paging mode" option to "always", and restart the DSA.

   The policy store schema is created for r12.1.

8. Manually create the following root nodes using Critical Path's iCon DIT administrator interface:
   - ou=Netegrity
   - ou=SiteMinder
   - ou=PolicySvr4

9. Run the following command:

   smobjimport -i*policy_server_home*/db/smdif/smpolicy.smdif -v

   -i

   Specifies the path and name of the import file.

   -v

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

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

10. Run the following command:

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

    -i

    Specifies the path and name of the import file.

    -d*siteminder_super_user_name*

    Specifies the name of the SOA Security Manager Super User account.

    -w*siteminder_super_user_password*

    Specifies the password for the SOA Security Manager Super User account.

    -f

    Overrides duplicate objects

    -v

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

    Default value: stdout

    -l

    Creates a log file.

    -c

    Indicates that the smdif input file contains unencrypted data.

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

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

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

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

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Point the Policy Server to the Policy Store

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

To point the Policy Server to the policy store

1. Open the Policy Server Management Console.
2. Click the Data tab.

   Database settings appear.
3. Select Policy Store from the Database list.
4. Select LDAP from the Storage list.
5. Configure the following settings in the LDAP Policy Store group box.
   - LDAP IP Address
   - Admin Username
   - Password
   - Confirm Password

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

   The policy store settings are saved.
7. Click Test LDAP Connection.

   SOA Security Manager returns a confirmation that the Policy Server can access the policy store.

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 an SSL Connection

You can configure an SSL connection.

To configure SSL

1. Install the SSL version of IDS.

   Note: The CD is entitled "InJoin Directory Server Secure Sockets Layer Option for Microsoft Windows NT". Despite the name, Solaris support is included.

2. (Optional) Check on whether 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.

   e. Verify that the following is displayed:

      admin>m_read_lkey

      read:

      read result:

      Entry information:

      Name: root

      Attribute type = licenseKey

      Maximum number of entries: 20000

      Demonstration expiry time: 06 August 2002

      Instance: 8192

Options:

Shadowing enabled

Enterprise iCon enabled

SSL enabled

Result = OK

3. Go to the SSL directory of IDS: c:\ids\icon\dsa1\ssl, create a file containing a random key (such as ds43jr58vndn3), and use the file name in the next step.
4. Create a Certificate Signing Request (CSR) file containing one line made up of a string of random characters and numbers.

   Example:

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

   random

   Specifies the name of the file that was created in the previous step.

   pkfile.p8

   Specifies the name of the file containing the private key that is created in this step.

   password

   Specifies the password.

   test.req

   Specifies the name of the CSR file that is created in this step.

   server.icarus.com

   Specifies the dn of the server.
5. Pass the text in test.req to a Certificate Authority (CA).

   The CA creates a server certificate.
6. Save the server certificate in a file (such as servercert.crt).
7. Obtain the root certificate from the CA in text format and save it in a file (such as rootcert.crt).
8. Run the following command:

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

   servercert.crt

   Specifies the name of the file that contains the server certificate created by the CA.

rootcert.crt

Specifies the name of the file containing the root certificate from the CA.

pkfile.p8

Specifies the name of the file that contains the private key.

password

Specifies the password.

cert.p12

Specifies the name of the identity file that is created by odscertconv.

An identity file is created for the SSL/IDS configuration.

9. Go to the DSA, click Comms, LDAP, LDAP Security using iCon.
10. Enter an SLL port (such as 636) and a name for the PKCS12 identity (such as test).
11. Enter the name of the identity file created that you created.

    Example: cert.p12
12. Enter the password that you used when you created the identity file.

    Example: password
13. Click Apply, and restart the DSA.

    Note: If the Policy Server is operating in FIPS mode and the directory connection is to use a secure SSL connection when communicating with the Policy Server, the certificates used by the Policy Server and the directory store must be FIPS compliant.

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

You can upgrade an existing 5.5 policy store to a r12.1 policy store using the Critical Path's iCon GUI.

To upgrade an existing 5.5 policy store to a r12.1 policy store

1. Stop the DSA that contains the 5.5 policy store. Go to dsa, comms, LDAP, and change the "paging mode" option to "always". Restart the DSA.

2. Navigate to policy_server_home\bin on the machine where the Policy Server is installed.

   policy_server_home

   Specifies the Policy Server installation path.

3. Run the following command:

   ldapmodify -h*host* -p*port* -d*AdminDN* -w*AdminPW* -c
   -f*dir_config_home*\criticalpath\IDS_Upgrade_Schema_55TOR12sp1.ldif

   -h host

   Specifies the IP address of the LDAP server.

   -p port

   Specifies the LDAP server port number.

   -d AdminDN

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

   Example: cn=manager

   -w AdminPW

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

   -c

   Specifies continuous mode (do not stop on errors).

   -f

   Specifies the path and name of the schema file that is supplied with r12.1.

   dir_config_home

   Specifies the Directory Configuration installation path.

   Note: ldapmodify requires version 4.2 of the Critical Path InJoin Directory Server.

4. Reload the schema, or verify that the schema has been updated.

5. Run the following command:

   ldapmodify -h*host* -p*port* -d*AdminDN* -w*AdminPW* -c
   -f*dir_config_home*\xps\criticalpath\CriticalPath.ldif

   -f

   Specifies the path and name of the XPS schema file that is supplied with r12.1.

   The policy store schema is extended to include the objects introduced by r12.1.

6. Reload the schema, or verify that the schema has been updated.
7. Go to dsa, comms, LDAP, change the "paging mode" option to "always", and restart the DSA.

   The policy store is extended to include the objects introduced by r12.1.
8. Point the Policy Server at the existing 5.5 policy store that you are upgrading to r12.1.
9. Run the following command:

   smobjimport
   -i*policy_server_home*\db\smdif\sm_upgrade_55_to_R12sp1.smdif -v -f

   -i

   Specifies the path and name of the import file.

   -v

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

   -f

   Overwrites duplicate SOA Security Manager objects.

   The base policy store data is imported from the file sm_upgrade_55_to_R12sp1.smdif, and the Critical Path inJoin Directory Server (IDS) is configured as a policy store.
10. Run the following command:

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

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

    -i*policy_server_home*

    Specifies the Policy Server installation path.

    -d*siteminder_super_user_name*

    Specifies the name of the SOA Security Manager administrator account.

    -w*siteminder_super_user_password*

    Specifies the password for the SOA Security Manager administrator account.

    -f

    Overrides duplicate objects.

    -v

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

    Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing policy store to r12.1.

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

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

   Note: The existing r6.x policy store schema has not changed. The r12.1 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.1.
3. Import the Base Policy Store Objects.

   Note: There is no change to policy store data if you are upgrading from 6.0 SP5. You do not have to import a policy store data (.smdif) file if you are upgrading from 6.0 SP5.
4. Import the Policy Store Data Definitions.

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

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

Extend the inJoin Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.1 using the Critical Path's iCon GUI. There are no changes to the existing 6.x policy store schema.

To extend an existing inJoin policy store schema

1. Start the DSA.
2. Navigate to policy_server_home/bin.

   policy_server_home

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

   ldapmodify -h*host* -p*port* -d*AdminDN* -w*AdminPW* -c
   -f*dir_config_home\xps\CriticalPath.ldif*

-h host

Specifies the IP address of the LDAP server.

-p port

Specifies the port number of the LDAP server.

-d AdminDN

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

Example: cn=manager

-w AdminPW

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

-c

Specifies continuous mode (do not stop on errors).

-f

Specifies the path and name of the XPS upgrade file that is supplied with r12.1.

dir_config_home

Specifies the Directory Configuration installation path.

Note: ldapmodify requires version 4.2 of the Critical Path inJoin Directory Server.

4. Reload the schema, or verify that the schema has been updated.
5. Go to dsa, comms, LDAP, change the "paging mode" option to "always", and restart the DSA.

   The policy store schema is extended to include the objects introduced by r12.1.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:
   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif*upgrade_smdif_file_name* -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v -f

   -i

   Specifies the path and name of the import file.

   upgrade_smdif_file_name

   Specifies the name of the import file:
   - **6.0 to r12.1:** sm_upgrade_60_to_R12sp1.smdif
   - **6.0 SP1 to r12.1:** sm_upgrade_60sp1_to_R12sp1.smdif
   - **6.0 SP2 to r12.1:** sm_upgrade_60sp2_to_R12sp1.smdif
   - **6.0 SP3 to r12.1:** sm_upgrade_60sp3_to_R12sp1.smdif
   - **6.0 SP4 to r12.1:** sm_upgrade_60sp4_to_R12sp1.smdif
   - **6.0 SP5 to r12.1:** sm_upgrade_60sp5_to_R12sp1.smdif

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager administrator account.

   -v

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

   Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.1.

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

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

UNIX example: smobjimport

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

The base policy store objects are imported.

3. Run the following command:

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

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

-i

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Chapter 3: IBM DB2

This section contains the following topics:

How to Configure an IBM DB2 Database as a Data Store (see page 29)
Upgrade a 6.x Session Server (see page 36)
How to Upgrade a 6.x Policy Store (see page 37)

How to Configure an IBM DB2 Database as a Data Store

SiteMinder provides schema files that you can use to create schemas for storing policies, keys, audit data, token data, and session data in an IBM DB2 Database. The schema files (or SQL scripts) are provided with SiteMinder in a ZIP file.

Configuring an IBM DB2 Database as a data store is a four-step process:

1. Create a DB2 Database with SiteMinder Schema
2. Configure a DB2 Data Source for SiteMinder
3. Import the Default Policy Store Objects
4. Import the Policy Store Data Definitions

Create a DB2 Database with SiteMinder Schema

You can create one or more SOA Security Manager schemas in a DB2 database.

To create SOA Security Manager schemas in a DB2 database

1. Navigate to *dir_config_home*\ibmdb2.

   dir_config_home

   Specifies the Directory Configuration installation path.

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

   sm_db2_ps.sql

   Specifies the schema for a policy or key store in a DB2 database.

3. Paste the file contents into a query, and execute the query.

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

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

   sm_db2_logs.sql

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

   sm_db2_token.sql

   Specifies the schema for a token store in a DB2 database.

   sm_db2_ss.sql

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

   smsampleusers_db2.sql

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

   The corresponding SOA Security Manager schema is created in the DB2 database.

   Note: You can create multiple SOA Security Manager schemas in a single DB2 database or create each schema in a separate database, optionally creating the following stores:

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

5. Open the following XPS schema file in a text editor and copy the contents of the entire file:

   policy_server_home/xps/db/DB2.sql

   policy_server_home

   Specifies the Policy Server installation path.

6. Paste the file contents into a query, and execute the query.

   The policy store schema is created for r12.1.

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.

Import the Default Policy Store Objects

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

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

To import the default policy store objects

1. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif\smpolicy.smdif
   -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v

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

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

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

   policy_server_home

   Specifies the Policy Server installation path.

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager super user account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager super user account.

   -v

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

   Default value: stdout

   -cf

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

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

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

2. Run the following command:

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

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager super user account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager super user account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Upgrade a 6.x Session Server

If you have a 6.x Session Server installed, you can upgrade it to take advantage of the features in r12.1.

Note: If you are upgrading a 6.0 SP5 Session Server, there are no changes in policy store data, and there is no need to import policy store data.

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

6.0, 6.0 SP1 or 6.0 SP2 to r12.1

dir_config_home\ibmdb2\sm_db2_ss_upgrade_60_60sp1or2_to_R12sp1.sql

6.0 SP3 or 6.0 SP4 to r12.1

dir_config_home\ibmdb2\sm_db2_ss_upgrade_60sp3or4_to_R12sp1.sql

dir_config_home

Specifies the Directory Configuration installation path.

A DB2 database session store is upgraded from 6.x to r12.1, and a new Expiry Data table is added to the session store.

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

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing policy store to r12.1.

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

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

   Note: The existing r6.x policy store schema has not changed. The r12.1 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.1.
3. Import the Base Policy Store Objects.

   Note: There is no change to policy store data if you are upgrading from 6.0 SP5. You do not have to import a policy store data (.smdif) file if you are upgrading from 6.0 SP5.
4. Import the Policy Store Data Definitions.

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

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

Extend the IBM DB2 Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.1. There are no changes to the existing 6.x policy store schema.

To extend an existing IBM DB2 policy store schema

1. Log into SQL Server as the user who administers the Policy Server database information.
2. Start the Query Analyzer.
3. Select the policy store database instance from the database list.
4. Navigate to policy_server_home\xps\db, open the file DB2.sql in a text editor, and copy the contents of the entire file.

   policy_server_home

   Specifies the Policy Server installation path.
5. Paste the file contents into a query, and execute the query.

   The policy store schema is extended to include the objects introduced by r12.1.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:
   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

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

   smobjimport -i*policy_server_home*\db\smdif*upgrade_smdif_file_name* -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v -f

   -i

   Specifies the path and name of the import file.

upgrade_smdif_file_name

Specifies the name of the import file:

- **6.0 to r12.1:** sm_upgrade_60_to_R12sp1.smdif
- **6.0 SP1 to r12.1:** sm_upgrade_60sp1_to_R12sp1.smdif
- **6.0 SP2 to r12.1:** sm_upgrade_60sp2_to_R12sp1.smdif
- **6.0 SP3 to r12.1:** sm_upgrade_60sp3_to_R12sp1.smdif
- **6.0 SP4 to r12.1:** sm_upgrade_60sp4_to_R12sp1.smdif
- **6.0 SP5 to r12.1:** sm_upgrade_60sp5_to_R12sp1.smdif

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-v

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

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.1.

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

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

UNIX example: smobjimport

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

The base policy store objects are imported.

3. Run the following command:

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

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

-i

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-wsiteminder_super_user_password

Specifies the password for the SOA Security Manager administrator account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

   XPSDDInstall imports the required data definitions.

3. Run the following command:

   XPSDDInstall EPMObjects.xdd

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   XPSDDInstall SecCat.xdd

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Chapter 4: IBM Directory Server

This section contains the following topics:

IBM Directory Server as a Policy Store (see page 43)
Upgrade a 5.x IBM Directory Server Policy Store (see page 52)
How to Upgrade a 6.x Policy Store (see page 61)

IBM Directory Server as a Policy Store

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

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

IBM Directory Server

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

1. Edit the V3 Matchingrules File

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

2. Create a Directory Entry and Root Nodes
3. Add the SOA Security Manager Schema File to Manage Schema Files

Edit the V3 Matchingrules File

Before you create the default policy store objects in the directory server, edit the V3.matchingrulesR12sp1 file.

To edit the file

1. Navigate to policy_server_home\IBMDirectoryServer.

   policy_server_home

   Specifies the Policy Server installation path.

2. Open the V3.matchingrulesR12sp1 file.

3. Add the following line:

   MatchingRules=(2.5.13.15 NAME
   'integerOrderingMatch' SYNTAX 1.3.6.1.4.1.1466.115.121.1.27)

4. Save the file.

   The V3.matchingrulesR12sp1 file is updated and the default policy store objects can be safely created.

Create a Directory Entry and Root Nodes

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

To create a directory entry and root nodes

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

   Example: ou=Nete

2. Create the following root nodes under ou=Nete:

   ou=Netegrity,ou=SiteMinder,ou=PolicySvr4

Add the SOA Security Manager Schema File to Manage Schema Files

You use the IBM Directory Server Configuration Tool to add the SOA Security Manager supplied schema file to Manage Schema Files.

To add the SOA Security Manager schema file

1. Navigate to policy_server_home\IBMDirectoryServer.

   policy_server_home

   Specifies the Policy Server installation path.

2. Move the IBM Directory Server V3.siteminderR12sp1 schema file to the Manage Schema Files section of the schema configuration.

3. Restart the IBM Directory Server.

   The file is added and the schema changes take effect.

Gather Directory Server Information

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

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

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Store

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

1. Verify that you have met the IBM Directory Server prerequisites.
2. Verify that you have gathered the necessary information.

3. Complete the following procedures:
   a. Point the Policy Server to the Policy Store
   b. Set the SOA Security Manager Super User Password

      Note: You do not have to complete this procedure if you already have a SOA Security Manager Super User password.
   c. Create the Policy Store Schema
   d. Import the Default Policy Store Objects
   e. Import the Policy Store Data Definitions
   f. Restart the Policy Server
   g. Prepare for the Administrative UI Registration

Point the Policy Server to the Policy Store

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

To point the Policy Server to the policy store

1. Open the Policy Server Management Console.
2. Click the Data tab.

   Database settings appear.
3. Select Policy Store from the Database list.
4. Select LDAP from the Storage list.
5. Configure the following settings in the LDAP Policy Store group box.
   - LDAP IP Address
   - Admin Username
   - Password
   - Confirm Password

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

   The policy store settings are saved.
7. Click Test LDAP Connection.

   SOA Security Manager returns a confirmation that the Policy Server can access the policy store.

Set the SOA Security Manager Super User Password

The Policy Server installer installs the [set the ufi variable for your book] and SOA Security Manager utilities with a default Super User account named SOA Security Manager. You set the SOA Security Manager Super User password to let an administrator:

- log into the FSS Administrative UI using the default SOA Security Manager account
- use SOA Security Manager utilities using the default account

Note: You use the smreg utility to change the SOA Security Manager Super User. The smreg utility is located at the top level of the Policy Server installation kit on the Technical Support site.

To locate installation kits on the Support site

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

To set the SOA Security Manager Super User password

1. Copy smreg to *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smreg -su *siteminder_super_user_password*

   siteminder_super_user_password

   Specifies the SOA Security Manager Super User password.

   Limit: The password can be from 6 to 24 characters in length.

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

3. Delete smreg from *policy_server_home*\bin.

   Note: Deleting smreg prevents anyone from changing the password without knowing the previous one.

   The password for the default SOA Security Manager Super User account is set.

Create the Policy Store Schema

You can configure an IBM directory server as a policy store for r12.1.

To create the policy store schema

1. Navigate to policy_server_home\bin or policy_server_home/bin from a command window.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smldapsetup ldgen -h*host* -p*port* -d*AdminDN* -w*AdminPW*
   -r*root* -ssl*1|0* -c*cert* -f*file_name* -m*LDAP_version*

   Note: For more information on the smldapsetup tool, see the *Policy Server Administration Guide*.

   -h host

   Specifies the IP address of the directory server.

   Example: 123.123.12.12

   -p port

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

   Example: 3500

   -d AdminDN

   Specifies the name of the LDAP user account with privileges to create a new LDAP root.

   Example: "cn=Directory Manager"

   -w AdminPW

   Specifies the password for the LDAP user account with privileges to create a new LDAP root.

   Example: MyPassword123

   -r root

   Specifies the directory server's root.

   Example: c=domain,dc=com

   -ssl 1|0

   (Optional) Specifies an SSL connection.

   Limits: 0=no or 1=yes

   Default: 0

-c cert

(Only required if ssl is set to 1) Defines the absolute path to the SSL client certificate database.

-f file_name

Specifies the name of the schema file that you are creating for the policy store.

-m LDAP_version

Specifies the directory server version.

3. Run the following command:

   smldapsetup ldmod -f*file_name*

   -f file_name

   Specifies the name of the schema file that you created for the policy store.

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

   - IBMDirectoryServer.ldif

5. Restart the IBM Directory Server.

   The policy store schema is created for r12.1.

Import the Default Policy Store Objects

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

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

To import the default policy store objects

1. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif\smpolicy.smdif
   -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v

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

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

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

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager super user account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager super user account.

-v

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

Default value: stdout

-cf

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

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

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

2. Run the following command:

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

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager super user account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager super user account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   XPSDDInstall SecCat.xdd

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Restart the Policy Server

You restart the Policy Server for 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.

Upgrade a 5.x IBM Directory Server Policy Store

You can upgrade an existing 5.x policy store to a r12.1 policy store.

How to Upgrade an IBM Secureway Directory Policy Store

A new directory server instance is not required for a r12.1 policy store. You may upgrade an existing IBM Secureway Directory policy store to r12.1.

1. Gather Directory Server Information
2. Gather SiteMinder Information
3. Edit the V3 Matchingrules File
4. Create the Policy Store Schema
5. Import the Base Policy Store Objects
6. Import the Policy Store Data Definitions

7. Add the SOA Security Manager Schema File to Manage Schema Files
8. Restart the Policy Server

Gather Directory Server Information

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

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

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

Gather SiteMinder Information

The SOA Security Manager tools used to configure or upgrade a policy store require specific SOA Security Manager administrator account information. Gather the following SOA Security Manager administrator information before configuring or upgrading a policy store:

- **SOA Security Manager User account name**—Identify the name of a SOA Security Manager administrator account.
- **SOA Security Manager User account password**—Identify the password for the SOA Security Manager administrator account.

Edit the V3 Matchingrules File

Before you create the default policy store objects in the directory server, edit the V3.matchingrulesR12sp1 file.

To edit the file

1. Navigate to policy_server_home\IBMDirectoryServer.

   policy_server_home

   Specifies the Policy Server installation path.

2. Open the V3.matchingrulesR12sp1 file.
3. Add the following line:

   MatchingRules=(2.5.13.15 NAME
   'integerOrderingMatch' SYNTAX 1.3.6.1.4.1.1466.115.121.1.27)

4. Save the file.

   The V3.matchingrulesR12sp1 file is updated and the default policy store objects can be safely created.

Add the SOA Security Manager Schema File to Manage Schema Files

You use the IBM Directory Server Configuration Tool to add the SOA Security Manager supplied schema file to Manage Schema Files.

To add the SOA Security Manager schema file

1. Navigate to policy_server_home\IBMDirectoryServer and locate the V3.siteminderR12sp1 schema file.

   policy_server_home

   Specifies the Policy Server installation path.

2. Remove the V3.modifiedschema50 or V3.modifiedschema55 file from the Manage Schema Files section of the schema configuration.
3. Add the supplied IBM Directory Server V3.siteminderR12sp1 schema file to the Manage Schema Files section of the schema configuration.
4. Restart the IBM Directory Server.

   The file is added and the schema changes take affect.

Create the Policy Store Schema

You create the r12.1 policy store schema so that the existing policy store can function as a r12.1 policy store.

To create the policy store schema

1. Navigate to policy_server_home\bin or policy_server_home/bin from a command window.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smldapsetup ldgen -h*host* -p*port* -d*AdminDN* -w*AdminPW*
   -r*root* -ssl*1|0* -c*cert* -f*file_name* -u -m*LDAP_version*

   Note: For more information on the smldapsetup tool, see the *Policy Server Administration Guide*.

   -h host

   Specifies the IP address of the directory server.

   Example: 123.123.12.12

   -p port

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

   Example: 3500

   -d AdminDN

   Specifies the name of the LDAP user account with privileges to create a new LDAP root.

   Example: "cn=Directory Manager"

   -w AdminPW

   Specifies the password for the LDAP user account with privileges to create a new LDAP root.

   Example: MyPassword123

-r root

Specifies the directory server's root.

Example: c=domain,dc=com

-ssl 1|0

(Optional) Specifies an SSL connection.

Limits: 0=no or 1=yes

Default: 0

-c cert

(Only required if ssl is set to 1) Defines the absolute path to the SSL client certificate database.

-f file_name

Specifies the name of the schema file that you are creating for the policy server.

-u

Specifies the creation of an upgrade schema file.

-m LDAP_version

Specifies the directory server version.

3. Run the following command:

   smldapsetup ldmod -f*file_name*

   -f file_name

   Specifies the name of the schema file that you created for the policy server.

4. Navigate to policy_server_home\xps\db, locate the following files, and add them to the Manage Schema Files section of the schema configuration using the IBM Directory Server Configuration Tool:

   - IBMDirectoryServer.ldif

5. Restart the IBM Directory Server.

   The policy store schema is extended to include the objects introduced by r12.1.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:
   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif\sm_upgrade_55_to_R12sp1.smdif -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v -f

   -i

   Specifies the path and name of the import file.

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager administrator account.

   -v

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

   Default output: stdout

   -f

   Overwrites duplicate policy store objects with those from r12.1.

   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

   The base policy store objects are imported.

3. Run the following command:

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

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

   -i

   Specifies the path and name of the import file.

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager administrator account.

   -f

   Overrides duplicate objects.

   -v

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

   Default value: stdout

   -l

   Creates a log file.

   -c

   Indicates that the smdif input file contains unencrypted data.

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

You may now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Restart the Policy Server

You restart the Policy Server for 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.

Upgrade Limitations for IBM Secureway Directory Server Policy Stores

The following limitations exist when upgrading an IBM Directory Server instance when to r12.1:

- If a domain existed in the policy store prior to the upgrade, no domain (including those you create after the upgrade) can have more than five user directories associated with it. If no domain existed prior to the upgrade, there is no such limitation.
- If an Agent group existed in the policy store prior to the upgrade, no Agent group (including those you create after the upgrade) can have more than five Agents in it. If no Agent group existed prior to the upgrade, there is no such limitation.
- If a rule group existed in the policy store prior to the upgrade, no rule group (including those you create after the upgrade) can have more than five rules in it. If no rule group existed prior to the upgrade, there is no such limitation.
- If a response group existed in the policy store prior to the upgrade, no response group (including those you create after the upgrade) can have more than five responses in it. If no response group existed prior to the upgrade, there is no such limitation.
- If the Option Pack is installed on the Policy Server, and a variable existed in the policy store prior to the upgrade, no variable (including those you create after the upgrade) can have a definition longer than 240 characters. In particular, you cannot create Web Service variables. If no variable existed prior to the upgrade, there is no such limitation.

The same limitations apply to a r12.1 Policy Server working in mixed mode with a 5.x policy store residing in IBM Directory Server.

To prevent these limitations, export the 5.x policy store data and then import the data into a new r12.1 policy store.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing policy store to r12.1.

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

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

   Note: The existing r6.x policy store schema has not changed. The r12.1 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.1.
3. Import the Base Policy Store Objects.

   Note: There is no change to policy store data if you are upgrading from 6.0 SP5. You do not have to import a policy store data (.smdif) file if you are upgrading from 6.0 SP5.
4. Import the Policy Store Data Definitions.

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

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

Extend the IBM Directory Server Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.1. There are no changes to the existing 6.x policy store schema.

To extend the IBM Directory Server policy store schema

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

   - IBMDirectoryServer.ldif

   policy_server_home

   Specifies the Policy Server installation path.
2. Restart the IBM Directory Server.

   The policy store schema is extended to include the objects introduced by r12.1.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:
   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif*upgrade_smdif_file_name* -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v -f

   -i

   Specifies the path and name of the import file.

   upgrade_smdif_file_name

   Specifies the name of the import file:
   - **6.0 to r12.1:** sm_upgrade_60_to_R12sp1.smdif
   - **6.0 SP1 to r12.1:** sm_upgrade_60sp1_to_R12sp1.smdif
   - **6.0 SP2 to r12.1:** sm_upgrade_60sp2_to_R12sp1.smdif
   - **6.0 SP3 to r12.1:** sm_upgrade_60sp3_to_R12sp1.smdif
   - **6.0 SP4 to r12.1:** sm_upgrade_60sp4_to_R12sp1.smdif
   - **6.0 SP5 to r12.1:** sm_upgrade_60sp5_to_R12sp1.smdif

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager administrator account.

   -v

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

   Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.1.

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

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

UNIX example: smobjimport

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

The base policy store objects are imported.

3. Run the following command:

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

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

-i

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Chapter 5: MySQL Server

This section contains the following topics:

How to Set Up a MySQL Server (see page 65)
How to Configure a Connection from the Policy Server to a MySQL Server User Store (see page 67)

How to Set Up a MySQL Server

Before configuring a connection from the Policy Server to a MySQL Server user store, you must set up the MySQL Server. Setting up the MySQL Server is a three-step process:

1. Install the MySQL Connector
2. Assign Root User Privileges
3. Create a MySQL Data Source

Install the MySQL Connector

Before configuring a connection from the Policy Server to the MySQL user store, you must install the MySQL ODBC drivers. To install the drivers, run the MySQL Connector/ODBC Setup Wizard and use the default options.

Assign Root User Privileges

You can use the MySQL Command Line Client to create the user directory administrator's username and password. This step is required before you can connect the Policy Server to the user directory.

To create a root user and assign a password

1. Click Start, MySQL, MySQL Server 5.0, MySQL Command Line Client.

   The MySQL Command Line Client opens.

2. Run the following command:

   mysql> GRANT ALL ON Test.* to 'root'@'<m/c_IP>' IDENTIFIED BY '<password>'

   m/c_IP

   Specifies the MySQL server IP address.

   password

   Specifies the password for the root user.

   A root user is created, and a password is assigned.

Create a MySQL Data Source

ODBC requires a data source for the MySQL Server wire protocol driver. You can create the MySQL data source using the ODBC Data Source Administrator.

To create a MySQL data source

1. Click Add on the UserDN tab of the ODBC Data Source Administrator.

   The Create New Data Source dialog opens.

2. Select MySQL ODBC 3.5.1 Driver from the list of available drivers, and click Finish.

   The Connector/ODBC dialog and Login tab open.

3. Complete the Data Source Name, Server, User, Password, and Database fields on the Login tab, and click the Connect Options tab.

   Note: The data source name is required for configuring a connection between the Policy Server and the user store.

   Note: Enter the password that you specified when you assigned the root user privileges.

4. Type the server port number in the Port field, and click the Advanced tab.
5. Select Don't Optimize Column Width and Return Matching Rows on the Flags 1 tab, and click Test.

   The MySQL data source is created.

How to Configure a Connection from the Policy Server to a MySQL Server User Store

Connecting the Policy Server to a MySQL Server user store is a two-step process. The first step, Create a Sample User Store, populates the MySQL Server with sample users. The second step, Configure MySQL Server Directory Connections, configures a connection from the Policy Server to the MySQL Server user store.

1. Create a Sample User Store
2. Configure MySQL Server Directory Connections

Create a Sample User Store

To create a sample user store using a MySQL server, open the MySQL Command Line Client and run the schema file provided with the Policy Server installation: smsampleusers_mysql.sql. Running the schema file creates the required objects in the specified database and populates the database with the sample users.

To create a sample user store

1. Click Start, MySQL Server 5.0, MySQL Command Line Client.

   The MySQL Command Line Client opens.

2. Select the name of the database that you specified when you created the data source.
3. Run the schema file:

   mysql> source <path_to_smsampleusers_mysql.sql>

   A sample user store is created.

Configure MySQL Server Directory Connections

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

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

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

   The Create User Directory pane opens.

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

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

      Attribute type: string

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

      Attribute type: string

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

      Attribute type: binary

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

      Attribute type: binary

      Note: This attribute is required by Password Services.

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

      Attribute type: string

   f. Leave the Email field blank.

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

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

      Attribute type: string

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

   The Create Attribute Mapping pane opens.

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

   The Create User Directory task is submitted for processing.

Chapter 6: Novell eDirectory

This section contains the following topics:

Novell eDirectory as a Policy Store (see page 69)
Upgrade a 5.x Novell eDirectory Policy Store (see page 78)
How to Upgrade a 6.x Policy Store (see page 85)

Novell eDirectory as a Policy Store

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

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

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

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

Gather Directory Server Information

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

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

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Store

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

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

   Note: You do not have to complete this procedure if you already have a SOA Security Manager Super User password.
5. Create the Policy Store Schema
6. Import the Default Policy Store Objects
7. Import the Policy Store Data Definitions
8. Refresh the LDAP Server
9. Restart the Policy Server
10. Prepare for the Administrative UI Registration

Edit the Policy Store Schema File

Edit the Novell policy store schema file (Novell_ADD_SMR12sp1.ldif) to ensure that it contains your Novell server DN information. You edit the Novell policy store schema file from the Novell Client.

To edit the policy store schema file

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

   policy_server_home

   Specifies the policy server installation path.

2. Run the following command:

   ldapsearch -h*host* -p*port* -b*container* -s*sub* -d*AdminDN* -w*AdminPW* objectclass=ncpServer dn

   Example:

   ldapsearch -h*192.168.1.47* -p*389* -b*o=nwqa47container* -s*sub* -d*cn=admin,o=nwqa47container* -w*password* objectclass=ncpServer dn

   The Novell server DN opens.

3. Open the Novell policy store schema file:

   policy_server_home\novell\Novell_ADD_SMR12sp1.ldif

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

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

5. Save and close the LDIF file.

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

Edit the Novell XPS Schema File

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

To edit the Novell XPS schema file

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

   policy_server_home

   Specifies the policy server installation path.

2. Run the following command:

   ldapsearch -h*host* -p*port* -b*container* -s*sub* -d*AdminDN* -w*AdminPW* objectclass=ncpServer dn

   Example:

   ldapsearch -h*192.168.1.47* -p*389* -bo=*nwqa47container* -s*sub* -dc*n=admin,o=nwqa47container* -w*password* objectclass=ncpServer dn

   The Novell server DN opens.

3. Open the Novell XPS schema file:

   policy_server_home\xps\db\Novell.ldif

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

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

5. Save and close the XPS file.

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

Point the Policy Server to the Policy Store

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

To point the Policy Server to the policy store

1. Open the Policy Server Management Console.
2. Click the Data tab.

   Database settings appear.

3. Select Policy Store from the Database list.
4. Select LDAP from the Storage list.

5. Configure the following settings in the LDAP Policy Store group box.
   - LDAP IP Address
   - Admin Username
   - Password
   - Confirm Password

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

   The policy store settings are saved.
7. Click Test LDAP Connection.

   SOA Security Manager returns a confirmation that the Policy Server can access the policy store.

Set the SOA Security Manager Super User Password

The Policy Server installer installs the [set the ufi variable for your book] and SOA Security Manager utilities with a default Super User account named SOA Security Manager. You set the SOA Security Manager Super User password to let an administrator:

- log into the FSS Administrative UI using the default SOA Security Manager account
- use SOA Security Manager utilities using the default account

Note: You use the smreg utility to change the SOA Security Manager Super User. The smreg utility is located at the top level of the Policy Server installation kit on the Technical Support site.

To locate installation kits on the Support site

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

To set the SOA Security Manager Super User password

1. Copy smreg to *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smreg -su *siteminder_super_user_password*

   siteminder_super_user_password

   Specifies the SOA Security Manager Super User password.

   Limit: The password can be from 6 to 24 characters in length.

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

3. Delete smreg from *policy_server_home*\bin.

   Note: Deleting smreg prevents anyone from changing the password without knowing the previous one.

   The password for the default SOA Security Manager Super User account is set.

Create the Policy Store Schema

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

To create the policy store schema

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

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smldapsetup ldmod -v

   -f*policy_server_home*/novell/Novell_Add_SMR12sp1.ldif

   -v

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

   -f

   Specifies the name of the schema file that is supplied with r12.1.

3. Run the following command:

   smldapsetup ldmod -v -f*policy_server_home*\xps\db\Novell.ldif

   -f

   Specifies the path and name of the XPS schema file that is supplied with r12.1.

   The policy store schema is created for r12.1.

Import the Default Policy Store Objects

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

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

To import the default policy store objects

1. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif\smpolicy.smdif
   -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v

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

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

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

   policy_server_home

   Specifies the Policy Server installation path.

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager super user account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager super user account.

   -v

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

   Default value: stdout

-cf

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

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

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

2. Run the following command:

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SOA Security Manager super user account.

-wsiteminder_super_user_password

Specifies the password for the SOA Security Manager super user account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Refresh the LDAP Server

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

To refresh the LDAP Server

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

   The LDAP server is refreshed.

Restart the Policy Server

You restart the Policy Server for 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.

Limitations of Policy Store Objects in Novell eDirectory

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

- When the policy store resides in Novell eDirectory, policy store objects cannot have names longer than 64 characters since eDirectory does not allow an attribute to be set to a value longer than 64. This affects Certificate Maps particularly since they routinely have long names by design.
- The Policy Server does not support LDAP referrals for policy stores residing in Novell eDirectory.

Upgrade a 5.x Novell eDirectory Policy Store

You can upgrade an existing 5.x policy store to a r12.1 policy store.

How to Upgrade a Novell eDirectory Policy Store

A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing 5.x Novell eDirectory policy store to r12.1 by following these procedures:

1. Gather Directory Server Information
2. Gather SiteMinder Information
3. Edit the Policy Store Schema File
4. Edit the Novell XPS Schema File

5. Create the Policy Store Schema
6. Import the Base Policy Store Objects
7. Import the Policy Store Data Definitions
8. Refresh the LDAP Server
9. Restart the Policy Server

Gather Directory Server Information

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

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

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

Gather SiteMinder Information

The SOA Security Manager tools used to configure or upgrade a policy store require specific SOA Security Manager administrator account information. Gather the following SOA Security Manager administrator information before configuring or upgrading a policy store:

- **SOA Security Manager User account name**—Identify the name of a SOA Security Manager administrator account.
- **SOA Security Manager User account password**—Identify the password for the SOA Security Manager administrator account.

Edit the Policy Store Schema File

Edit the Novell policy store schema upgrade file (Novell_Upgrade_SM55_to_SMR12sp1.ldif) to ensure that it contains your Novell server DN information. You edit the Novell policy store schema upgrade file from the Novell Client.

To edit the policy store schema file

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

   policy_server_home

   Specifies the policy server installation path.

2. Run the following command:

   ldapsearch -h*host* -p*port* -b*container* -s*sub* -d*AdminDN* -w*AdminPW* objectclass=ncpServer dn

   Example:

   ldapsearch -h*192.168.1.47* -p*389* -b*o=nwqa47container* -s*sub* -d*cn=admin,o=nwqa47container* -w*password* objectclass=ncpServer dn

   The Novell server DN opens.

3. Open the Novell policy store schema upgrade file:

   policy_server_home\novell\Novell_Upgrade_SM55_to_SMR12sp1.ldif

4. Manually edit the open LDIF file by replacing every NCP_Server variable with the value of your Novell server DN.

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

5. Save and close the LDIF file.

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

Edit the Novell XPS Schema File

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

To edit the Novell XPS schema file

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

   policy_server_home

   Specifies the policy server installation path.

2. Run the following command:

   ldapsearch -h*host* -p*port* -b*container* -s*sub* -d*AdminDN* -w*AdminPW* objectclass=ncpServer dn

   Example:

   ldapsearch -h*192.168.1.47* -p*389* -bo=*nwqa47container* -s*sub* -dc*n=admin,o=nwqa47container* -w*password* objectclass=ncpServer dn

   The Novell server DN opens.

3. Open the Novell XPS schema file:

   policy_server_home\xps\db\Novell.ldif

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

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

5. Save and close the XPS file.

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

Create the Policy Store Schema

You can upgrade a 5.x policy store to a r12.1 policy store.

To create the policy store schema

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

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smldapsetup ldmod -v

   -f*policy_server_home*\novell\Novell_Upgrade_SM55_To_SMR12sp1.ldif

   -v

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

   -f

   Specifies the name of the upgrade file.

3. Run the following command:

   smldapsetup ldmod -f*policy_server_home*/xps/db/Novell.ldif

   -f

   Specifies the path and name of the XPS schema file that is supplied with r12.1.

   The policy store schema is extended to include the objects introduced by r12.1.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:

   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif\sm_upgrade_55_to_R12sp1.smdif
   -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v -f

   -i

   Specifies the path and name of the import file.

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-v

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

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.1.

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

The base policy store objects are imported.

3. Run the following command:

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

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

-i

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

You may now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Refresh the LDAP Server

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

To refresh the LDAP Server

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

   The LDAP server is refreshed.

Restart the Policy Server

You restart the Policy Server for 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 Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing policy store to r12.1.

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

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

   Note: The existing r6.x policy store schema has not changed. The r12.1 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.1.

3. Import the Base Policy Store Objects.

   Note: There is no change to policy store data if you are upgrading from 6.0 SP5. You do not have to import a policy store data (.smdif) file if you are upgrading from 6.0 SP5.

4. Import the Policy Store Data Definitions.

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

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

Edit the Novell XPS Schema File

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

To edit the Novell XPS schema file

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

   policy_server_home

   Specifies the policy server installation path.

2. Run the following command:

   ldapsearch -h*host* -p*port* -b*container* -s*sub* -d*AdminDN* -w*AdminPW* objectclass=ncpServer dn

   Example:

   ldapsearch -h*192.168.1.47* -p*389* -b*o=nwqa47container* -s*sub* -d*cn=admin,o=nwqa47container* -w*password* objectclass=ncpServer dn

   The Novell server DN opens.

3. Open the Novell XPS schema file:

   policy_server_home\xps\db\Novell.ldif

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

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

5. Save and close the XPS file.

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

Extend the Novell Policy Store Schema

You can extend a Novell 6.0 policy store schema to include the objects introduced by r12.1. There are no changes to the existing 6.0 policy store schema or data.

To extend the Novell policy store schema

Run the following command:

smldapsetup ldmod -f*policy_server_home*/xps/db/Novell.ldif

-f

Specifies the path and name of the XPS schema file that is supplied with r12.1.

policy_server_home

Specifies the Policy Server installation path.

The policy store schema is extended to include the objects introduced by r12.1.

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

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:
   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

smobjimport -i*policy_server_home*\db\smdif*upgrade_smdif_file_name*
-d*siteminder_super_user_name* -w*siteminder_super_user_password*
-v -f

-i

Specifies the path and name of the import file.

upgrade_smdif_file_name

Specifies the name of the import file:

- **6.0 to r12.1:** sm_upgrade_60_to_R12sp1.smdif
- **6.0 SP1 to r12.1:** sm_upgrade_60sp1_to_R12sp1.smdif
- **6.0 SP2 to r12.1:** sm_upgrade_60sp2_to_R12sp1.smdif
- **6.0 SP3 to r12.1:** sm_upgrade_60sp3_to_R12sp1.smdif
- **6.0 SP4 to r12.1:** sm_upgrade_60sp4_to_R12sp1.smdif
- **6.0 SP5 to r12.1:** sm_upgrade_60sp5_to_R12sp1.smdif

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-v

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

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.1.

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

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

UNIX example: smobjimport

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

The base policy store objects are imported.

3. Run the following command:

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

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

   -i

   Specifies the path and name of the import file.

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager administrator account.

   -f

   Overrides duplicate objects.

   -v

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

   Default value: stdout

   -l

   Creates a log file.

   -c

   Indicates that the smdif input file contains unencrypted data.

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Chapter 7: Oracle Internet Directory Server

This section contains the following topics:

Oracle Internet Directory as a Policy Store (see page 91)
How to Upgrade an Oracle Internet Directory Policy Store (see page 99)
How to Upgrade a 6.x Policy Store (see page 107)

Oracle Internet Directory as a Policy Store

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

Gather Directory Server Information

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

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

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Server

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

1. Configure a Domain in Oracle Internet Directory
2. Point the Policy Server to the Directory Server
3. Set the SOA Security Manager Super User Password

   Note: You do not have to complete this procedure if you already have a SOA Security Manager Super User password.
4. Create the Policy Store Schema
5. Import the Default Policy Store Objects
6. Import the Policy Store Data Definitions
7. Restart the Policy Server
8. Prepare for the Administrative UI Registration

Configure a Domain in Oracle Internet Directory

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

To configure a domain in Oracle Internet Directory

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

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

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

   The OID domain is configured.

Point the Policy Server to the Directory Server

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

To point the Policy Server to the directory server

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

   smldapsetup status -h *host* -p *port* -d *AdminDN*
   -w *AdminPW* -r *root* -ssl *1/0* -c *cert*

   -h *host*

   Specifies the IP Address of the LDAP server.

   -p *port*

   Specifies the port number of the LDAP server.

   -d *AdminDN*

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

   ADAM: Specifies the full domain name, including the guid value, of the ADAM administrator.

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

   -w *AdminPW*

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

   -r *root*

   Specifies the DN location of the SOA Security Manager data in the LDAP directory.

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

   -ssl 1|0

   Specifies an SSL connection.

   Limits: 0=no | 1=yes

   Default: 0

-c *cert*

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

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

2. Run the following command:

smldapsetup reg -h *host* -p *port* -d *AdminDN*
-w *AdminPW* -r *root* -ssl *1/0* -c *cert*

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

Set the SOA Security Manager Super User Password

The Policy Server installer installs the [set the ufi variable for your book] and SOA Security Manager utilities with a default Super User account named SOA Security Manager. You set the SOA Security Manager Super User password to let an administrator:

- log into the FSS Administrative UI using the default SOA Security Manager account
- use SOA Security Manager utilities using the default account

Note: You use the smreg utility to change the SOA Security Manager Super User. The smreg utility is located at the top level of the Policy Server installation kit on the Technical Support site.

To locate installation kits on the Support site

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

To set the SOA Security Manager Super User password

1. Copy smreg to *policy_server_home*\bin.

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

   smreg -su *siteminder_super_user_password*

   siteminder_super_user_password

   Specifies the SOA Security Manager Super User password.

   Limit: The password can be from 6 to 24 characters in length.

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

3. Delete smreg from *policy_server_home*\bin.

   Note: Deleting smreg prevents anyone from changing the password without knowing the previous one.

   The password for the default SOA Security Manager Super User account is set.

Create the Policy Store Schema

You can create the policy store schema to include the objects introduced by r12.1.

To create the policy store schema

1. Navigate to policy_server_home/bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smldapsetup ldgen -f*file_name.ldif*

   -f

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

3. Run the following command:

   smldapsetup ldmod -f*file_name.ldif*

   -f

   Specifies the name of the schema file that you created.

4. Run the following command:

   ldapmodify -h*host* -p*port* -d*AdminDN* -w*AdminPW*
   -c -f*dir_config_home*/xps/oid_10g/OID_10g.ldif
   -Z -P*cert*

   -h host

   Specifies the IP address of the LDAP directory server.

   Example: 123.123.12.12

-p port

Specifies the port number of the LDAP directory server.

Example: 3500

-d AdminDN

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

-w AdminPW

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

-c

Specifies continuous mode (do not stop on errors).

-f

Specifies the path and name of the XPS schema file that is supplied with r12.1.

dir_config_home

Specifies the Directory Configuration installation path.

-Z

Specifies an SSL-encrypted connection.

-P cert

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

Example:

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

-Papp/siteminder/ssl

The policy store schema is created for r12.1.

Import the Default Policy Store Objects

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

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

To import the default policy store objects

1. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif\smpolicy.smdif
   -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v

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

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

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

   policy_server_home

   Specifies the Policy Server installation path.

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager super user account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager super user account.

   -v

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

   Default value: stdout

   -cf

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

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

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

2. Run the following command:

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

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager super user account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager super user account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

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

   XPSDDInstall SmObjects.xdd

   XPSDDInstall imports the required data definitions.

3. Run the following command:

   XPSDDInstall EPMObjects.xdd

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   XPSDDInstall SecCat.xdd

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Restart the Policy Server

You restart the Policy Server for 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 Upgrade an Oracle Internet Directory Policy Store

You can upgrade an existing 5.x Oracle Internet Directory (OID) policy store to a r12.1 policy store. A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing 5.x OID policy store to r12.1 by following these procedures:

1. Gather Directory Server Information
2. Gather SiteMinder Information

3. Create the Policy Store Schema
4. Import the Base Policy Store Objects
5. Import the Policy Store Data Definitions
6. Restart the Policy Server
7. Set Oracle Internet Directory Attributes

   Note: If the Policy Server is not operating in mixed mode, this step is optional.

Gather Directory Server Information

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

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

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

Gather SiteMinder Information

The SOA Security Manager tools used to configure or upgrade a policy store require specific SOA Security Manager administrator account information. Gather the following SOA Security Manager administrator information before configuring or upgrading a policy store:

- **SOA Security Manager User account name**—Identify the name of a SOA Security Manager administrator account.
- **SOA Security Manager User account password**—Identify the password for the SOA Security Manager administrator account.

Create the Policy Store Schema

You can upgrade an existing 5.x policy store to a r12.1 policy store.

To upgrade the policy store schema

1. Navigate to policy_server_home/bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smldapsetup ldgen -h*host* -p*port* -d*AdminDN* -w*AdminPW* -r*root* -ssl1|0 -c*cert* -f*file_name.ldif* -u -m4

   -h host

   Specifies the IP address of the directory server.

   Example: 123.123.12.12

   -p port

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

   Example: 3500

   -d AdminDN

   Specifies the name of an LDAP user with privileges to create a new LDAP root.

   Example: cn=Directory Manager

   -w AdminPW

   Specifies the password of an LDAP user with privileges to create a new LDAP root.

   Example: MyPassword123

-r root

Specifies the root node of the schema in the LDAP tree.

Example: c=domain,dc=com

-ssl 1|0

Specifies an SSL-encrypted connection.

Limits: 0=no | 1=yes

Default: 0

-c cert

(Required for an SSL-encrypted connection) Specifies the path of the SSL client certificate database file.

-f

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

-u

Specifies the creation of a schema file for an upgrade.

-m4

Specifies the LDAP server type Oracle Internet Directory.

3. Run the following command using the same values as you used when creating the upgrade schema file, but without the "-u" option:

   smldapsetup ldmod -h*host* -p*port* -d*AdminDN* -w*AdminPW*
   -r*root* -ssl*1|0* -c*cert* -f*file_name.ldif* -m4

   -f

   Specifies the name of the schema file that you created.

4. Run the following command:

   ldapmodify -h*host* -p*port* -d*AdminDN* -w*AdminPW*
   -c -f*dir_config_home*/xps/oid_10g/OID_10g.ldif
   -Z -P*cert*

   -f

   Specifies the name of the XPS schema file that is supplied with r12.1.

   dir_config_home

   Specifies the Directory Configuration installation path.

   -Z

   Specifies an SSL-encrypted connection.

-P cert

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

Example:

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

-Papp/siteminder/ssl

The policy store schema is extended to include the objects introduced by r12.1.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:
   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif\sm_upgrade_55_to_R12sp1.smdif -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v -f

   -i

   Specifies the path and name of the import file.

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager administrator account.

   -v

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

   Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.1.

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

The base policy store objects are imported.

3. Run the following command:

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

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

-i

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

You may now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Restart the Policy Server

You restart the Policy Server for 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.

Set Oracle Internet Directory Attributes

If the Policy Server is connected to a 5.x policy store that resides in an Oracle Internet Directory, the Policy Server is operating in mixed mode and you must specify that the following attributes are searchable in OID:

- smFilterPath4
- smIsAffiliate4
- smusractiveexproid5
- smIs4xTrustedHost5
- smDomainMode5
- smNoMatch5
- smImsEnvironmentOIDs5

  Note: This attribute does not apply to a 5.0 policy store.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing policy store to r12.1.

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

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

   Note: The existing r6.x policy store schema has not changed. The r12.1 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.1.
3. Import the Base Policy Store Objects.

   Note: There is no change to policy store data if you are upgrading from 6.0 SP5. You do not have to import a policy store data (.smdif) file if you are upgrading from 6.0 SP5.
4. Import the Policy Store Data Definitions.

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

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

Extend the Oracle Internet Directory Policy Store Schema

You can extend a 6.x policy store schema to include the objects introduced by r12.1. There are no changes to the existing 6.x policy store schema.

To extend the Oracle Internet Directory policy store schema

1. Navigate to *policy_server_home*/bin or *policy_server_home*\bin.

   policy_server_home

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

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

-h host

Specifies the IP address of the LDAP directory server.

Example: 123.123.12.12

-p port

Specifies the port number of the LDAP directory server.

Example: 3500

-d AdminDN

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

-w AdminPW

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

-c

Specifies continuous mode (do not stop on errors).

-f

Specifies the path and file name of the XPS upgrade file that is provided with r12.1.

dir_config_home

Specifies the Directory Configuration installation path.

-Z

Specifies an SSL-encrypted connection.

-P cert

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

Example:

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

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

The policy store schema is extended to include the objects introduced by r12.1.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:
   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif*upgrade_smdif_file_name* -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v -f

   -i

   Specifies the path and name of the import file.

   upgrade_smdif_file_name

   Specifies the name of the import file:
   - **6.0 to r12.1:** sm_upgrade_60_to_R12sp1.smdif
   - **6.0 SP1 to r12.1:** sm_upgrade_60sp1_to_R12sp1.smdif
   - **6.0 SP2 to r12.1:** sm_upgrade_60sp2_to_R12sp1.smdif
   - **6.0 SP3 to r12.1:** sm_upgrade_60sp3_to_R12sp1.smdif
   - **6.0 SP4 to r12.1:** sm_upgrade_60sp4_to_R12sp1.smdif
   - **6.0 SP5 to r12.1:** sm_upgrade_60sp5_to_R12sp1.smdif

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager administrator account.

   -v

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

   Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.1.

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

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

UNIX example: smobjimport

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

The base policy store objects are imported.

3. Run the following command:

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

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

-i

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Chapter 8: OpenLDAP Server

This section contains the following topics:

How to Configure the Slapd Configuration File (see page 113)
How to Create the Database (see page 117)
How to Configure the Directory Server as a Policy Store (see page 118)
How to Configure the Directory Sever as a User Store (see page 122)
Configure SSL for a Policy Store (see page 124)
How to Upgrade a 6.x Policy Store (see page 125)
Troubleshooting OpenLDAP (see page 130)

How to Configure the Slapd Configuration File

An OpenLDAP directory server requires additional configuration before you can use it as a SiteMinder policy store. The following process lists the configuration steps:

1. Specify the SiteMinder Schema Files
2. Enable User Authentication
3. Specify Database Directives
4. Test the Configuration File
5. Restart the OpenLDAP Server

Specify the SiteMinder Schema Files

Specifying the schema files in the include section of the slapd configuration file (slapd.conf) ensures that the slapd process (the LDAP Directory Server daemon) reads the additional configuration information. The included files must follow the correct slapd configuration file format.

To specify the schema files

1. Copy the following schema files to the schema folder in the OpenLDAP installation directory:
   - dir_config_home/openldap/openldap_attribute.schema
   - dir_config_home/openldap/openldap_object.schema

- dir_config_home/xps/openldap/openldap_attribute_XPS.schema
- dir_config_home/xps/openldap/openldap_object_XPS.schema

dir_config_home

Specifies the Directory Configuration installation path.

2. Type the following in the include section of the slapd configuration file:

```
....
.....
include /usr/local/etc/openldap/schema/openldap_attribute.schema
include /usr/local/etc/openldap/schema/openldap_object.schema
include /usr/local/etc/openldap/schema/openldap_attribute_XPS.schema
include /usr/local/etc/openldap/schema/openldap_object_XPS.schema
```

Note: This procedure assumes that the OpenLDAP server is located at /usr/local/etc/openldap and that the schema files are located in the schema subdirectory.

The policy store schema is created for r12.1.

Enable User Authentication

Enabling user authentication ensures that you can protect resources with a supported authentication scheme.

To enable user authentication, add the following to the slapd configuration file:

```
access to attr=userpassword
by self write
by anonymous auth
by * none
```

Specify Database Directives

The slapd configuration file requires values for additional database directives.

To specify the directives, edit the following:

database

Specify any supported backend type.

Example: bdb

suffix

Specify the database suffix.

Example: dc=example,dc=com

rootdn

Specify the DN of root.

Example: cn=Manager,dc=example,dc=com

rootpw

Specify the password to root.

directory

Specify the path of the database directory.

Example: /usr/local/var/openldap-data

Note: The database directory must exist prior to running slapd and should only be accessible to the slapd process.

Support Client-Side Sorting

OpenLDAP is the only supported LDAP directory that does not support server-side sorting. Instead, OpenLDAP requires that all sorting be performed on the client side. To accomplish this, all XPS objects are retrieved at start-up using server-side paging.

To support client-side sorting, the OpenLDAP directory administrator must configure the following settings in the slapd.conf file:

- Enable reading of the Root DSE.

  This setting allows the XPS client to read the OpenLDAP directory's type and capabilities.

- Set the maximum number of entries that can be returned from a search operation >= 500.

  This setting accommodates XPS objects which are retrieved in increments of 500 by server-side paging.

- Allow a simple V2 bind.

  This setting allows smconsole to test the LDAP connection using a simple V2 bind.

To support client-side sorting

1. Add the following lines to the slapd.conf file:

   ```
   access to *
   by users read
   by anonymous read
   access to dn.base=ACL by users read
   ```

   ACL

   Specifies an access control list or list of permissions.

   Note: For more information on how to specify the ACL, see http://www.openldap.org/doc/admin24/access-control.html.

2. Verify that the value specified by the sizelimit directive in the slapd.conf file >= 500:

   ```
   sizelimit 500
   ```

   Note: The default sizelimit value is 500. For more information, see http://www.openldap.org/doc/admin24/slapdconfig.html.

3. Add the following line to the slapd.conf file:

   ```
   allow bind_v2
   ```

The slapd.conf file is configured to support client-side sorting.

Test the Configuration File

Testing the configuration file ensures that it is correctly formatted.

To test the configuration file

1. Change the directory to the OpenLDAP server directory.
2. Run the following command:

   ```
   ./slapd
   ```

   Note: Unless you specified a debugging level, including level 0, slapd automatically forks, detaches itself from its controlling terminal, and runs in the background.

3. Run the following command:

   ```
   ./slapd -Tt
   ```

   The slapd configuration file is tested.

Restart the OpenLDAP Server

Restarting the OpenLDAP directory server loads the SiteMinder schema. The Policy Server requires that the SiteMinder schema is loaded before you can use the directory server as a policy store.

To restart the directory server

1. Stop the directory server using the following command:

   kill ?INT 'cat *path_of_var/run_directory/slapd.pid*'

   path_of_var/run_directory

   Specifies the path of the database directory.

   Example: kill ?INT 'cat /usr/local/var/run/slapd.pid'

2. Start the directory server using the following command:

   ./slapd

How to Create the Database

The following process lists the steps for creating the directory server database for the policy store:

1. Create the Base Tree Structure
2. Add Entries

Create the Base Tree Structure

You can create a base tree structure in the policy store.

Specify the following under the root DN:

ou=Netegrity,ou=SiteMinder,ou=PolicySvr4

The base tree structure is created in the policy store.

Add Entries

Add entries to the directory server so that SOA Security Manager has the necessary organization and organizational role information.

To add database entries

1. Create an LDIF file.

   Example: The following example contains an organization entry and an organizational role entry for the entries.ldif.

   ```
   # Organization for example.com
   dn: root_DN (example.com)
   objectClass: dcObject
   objectClass: organization
   dc: example
   o: Example Corporation

   # Organizational Role for Directory Manager
   dn: cn=Manager,root_DN
   objectClass: organizationalRole
   objectClass: top
   cn: Manager
   description: Directory Manager
   ```

2. Use the following command to add the entries.

   ldapadd -*<file_name.ldif>*
   -D "*cn=Manager,dc=example,dc=com*" -w*<password>*

How to Configure the Directory Server as a Policy Store

You can use the Policy Server Management Console and the Administrative UI to configure the directory server as a policy store. The following process lists the steps for using the directory server as a policy store:

1. Create the Policy Store
2. Connect to the Policy Store

Point the Policy Server to the Directory Server

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

To point the Policy Server to the directory server

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

   smldapsetup status -h *host* -p *port* -d *AdminDN*
   -w *AdminPW* -r *root* -ssl *1/0* -c *cert*

   -h *host*

   Specifies the IP Address of the LDAP server.

   -p *port*

   Specifies the port number of the LDAP server.

   -d *AdminDN*

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

   ADAM: Specifies the full domain name, including the guid value, of the ADAM administrator.

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

   -w *AdminPW*

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

   -r *root*

   Specifies the DN location of the SOA Security Manager data in the LDAP directory.

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

   -ssl 1|0

   Specifies an SSL connection.

   Limits: 0=no | 1=yes

   Default: 0

-c *cert*

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

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

2. Run the following command:

smldapsetup reg -h *host* -p *port* -d *AdminDN* -w *AdminPW* -r *root* -ssl *1/0* -c *cert*

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

Create the Policy Store

To configure an OpenLDAP directory server as a policy store, import the base policy store data.

To create the policy store

1. Start the Policy Server Management Console.
2. Click the Data tab.
3. Type the root DN in the Root DN field, and click OK.

   The root DN is saved.
4. Go to policy_server_home/bin.

   policy_server_home

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

   smreg -su *adminPW*

   The administrator's password is saved.
6. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif\smpolicy.smdif -d*AdminDN* -w*AdminPW* -v

   -i

   Specifies the name of the import file.

   -d AdminDN

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

-w AdminPW

Specifies the password of an LDAP user with privileges to create a new LDAP schema in the LDAP directory.

-v

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

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

7. Run the following command:

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

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager Super User account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager Super User account.

-f

Overrides duplicate objects

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

Note: You can now import policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

How to Configure the Directory Sever as a User Store

You can use the OpenLDAP directory server as a user store. The following process lists the steps for using the directory server as a user store:

1. Create a User Store
2. Connect to the User Store

Create a User Store

You can use an OpenLDAP directory server as a user store

To create a user store

1. Use an LDIF file to create ou=People under the root DN.
2. Create users under the organizational unit.

Configure a Connection from the Policy Server to an OpenLDAP User Store

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

To configure a connection from the Policy Server to an OpenLDAP user store

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

   The Create User Directory pane opens.

   Note: You can specify user directory properties on this pane. For more information on the fields, settings, and options, click Help.
3. Type the name and a description of the new User Directory object in the fields on the General group box.
4. Verify that LDAP is selected from the Namespace list, and type the IP address and port number in the Server field on the Directory Setup group box.

   Note: When the Policy Server is operating in FIPs mode and the User Directory connection is a secure SSL connection, the certificates used by the Policy Server and the user store must be FIPs compliant.
5. Select the Require Credentials check box, and type the full DN and password of the administrator in the fields on the Administrator Credentials group box.
6. Type the root node and search parameters in the fields on the LDAP Search group box.
7. Type a beginning text string and an ending text string in the fields on the LDAP User DN Lookup group box.

   Note: The beginning text string, username, and ending text string are combined to create a string that is used for searching the User Directory tree.
8. (Optional) Complete the fields on the User Attributes group box.
   a. Type the Universal ID in the Universal ID field.

      Attribute type: string

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

Attribute type: string

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

Attribute type: binary

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

Attribute type: binary

Note: This attribute is required by Password Services.

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

Attribute type: string

f. Leave the Email field blank.

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

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

Attribute type: string

Note: This string is sent to the user after each challenge.

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

The Create Attribute Mapping pane opens.

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

10. Click Submit.

The Create User Directory task is submitted for processing.

More information:

How to Configure an LDAP User Directory Connection over SSL (see page 163)

Configure SSL for a Policy Store

Policy stores support Secure Socket Layers (SSL). You configure the policy store for SSL from the Policy Server Management Console.

The following procedure assumes:

- The OpenLDAP environment is configured for SSL.
- The certificate Authority's (CA) root certificate (cacert.pem) is installed on the Netscape cert7.db database on each machine that will use SSL to communicate with the directory server.

- A key3.db file has been created.

  Note: SiteMinder requires that the root certificate adheres to the Netscape file format. You cannot use Microsoft IE to install the certificate.

To configure SSL for a policy store

1. Start the Policy Server Management Console.
2. Click the Data tab.

   The Data tab opens.
3. Select Use SSL.
4. Enter the absolute path to cert7.db in the Netscape Certificate Database File field.

   Note: Consider the following:

   – A known limitation requires that the file name be included in the path. You can resolve this issue after providing a complete absolute path. Fix the path by removing the last substring (cert7.db) in the CertDbPath variable in the registry.

   – The key3.db file must also be in the same directory as the cert7.db file.
5. Click OK.

   SSL is enabled for the policy store.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing policy store to r12.1.

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

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

   Note: The existing r6.x policy store schema has not changed. The r12.1 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.1.
3. Import the Base Policy Store Objects.

   Note: There is no change to policy store data if you are upgrading from 6.0 SP5. You do not have to import a policy store data (.smdif) file if you are upgrading from 6.0 SP5.

4. Import the Policy Store Data Definitions.

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

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

Extend the OpenLDAP Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.1 by specifying the schema files in the include section of the slapd configuration file (slapd.conf). This ensures that the slapd process (the LDAP Directory Server daemon) reads the additional configuration information. The included files must follow the correct slapd configuration file format. There are no changes to the existing 6.x policy store schema.

To extend an existing OpenLDAP policy store schema

1. Copy the following schema files from *dir_config_home*\xps\openldap to the schema folder in the OpenLDAP installation directory:
   - openldap_attribute_XPS.schema
   - openldap_object_XPS.schema

   dir_config_home

   Specifies the Directory Configuration installation path.

2. Type the following in the include section of the slapd configuration file:

   ....
   .....
   include /usr/local/etc/openldap/schema/openldap_attribute_XPS.schema
   include /usr/local/etc/openldap/schema/openldap_object_XPS.schema

   Note: This procedure assumes that the OpenLDAP server is located at /usr/local/etc/openldap and that the schema files are located in the schema subdirectory.

   The policy store schema is extended to include the objects introduced by r12.1.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:
   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif*upgrade_smdif_file_name* -d*siteminder_super_user_name* -w*siteminder_super_user_password* -v -f

   -i

   Specifies the path and name of the import file.

   upgrade_smdif_file_name

   Specifies the name of the import file:
   - **6.0 to r12.1:** sm_upgrade_60_to_R12sp1.smdif
   - **6.0 SP1 to r12.1:** sm_upgrade_60sp1_to_R12sp1.smdif
   - **6.0 SP2 to r12.1:** sm_upgrade_60sp2_to_R12sp1.smdif
   - **6.0 SP3 to r12.1:** sm_upgrade_60sp3_to_R12sp1.smdif
   - **6.0 SP4 to r12.1:** sm_upgrade_60sp4_to_R12sp1.smdif
   - **6.0 SP5 to r12.1:** sm_upgrade_60sp5_to_R12sp1.smdif

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager administrator account.

   -v

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

   Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.1.

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

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

UNIX example: smobjimport

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

The base policy store objects are imported.

3. Run the following command:

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

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

-i

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Troubleshooting OpenLDAP

For information on troubleshooting OpenLDAP, see the following topics:

- Cyrus SASL Installation
- Berkeley Database Version Mismatch Errors
- Building and Installing openSSL

Cyrus SASL Installation

Symptom:

When I install Cyrus SASL, I am experiencing compiling problems.

Solution:

More information on troubleshooting Cyrus SASL installation problems can be found at:

http://marc.theaimsgroup.com/?l=cyrus-sasl&m=111835942621184&w=2

Berkeley Database Version Mismatch Errors

Symptom:

I am receiving Berkeley database version mismatch errors.

Solution:

More information on troubleshooting Berkeley database version mismatch errors can be found at:

http://www.openldap.org/faq/data/cache/1113.html

Building and Installing openSSL

Symptom:

I am having problems building and installing openSSL.

Solution:

More information on building and installing openSSL can be found at:

http://www.proscrutiny.com/howtos/OpenLDAP.html#confssl-co

Chapter 9: OpenWave Directory Server 6.0.1

This section contains the following topics:

Configure an OpenWave Directory Server as a Policy Store (see page 131)
Import the Policy Store Data Definitions (see page 135)
Connect to an OpenWave Policy Store (see page 135)
Configure a Connection from the Policy Server to an OpenWave Directory User Store (see page 136)
How to Upgrade a 6.x Policy Store (see page 138)
LDAP Referrals (see page 142)

Configure an OpenWave Directory Server as a Policy Store

You can configure an OpenWave directory server as a policy store by following the steps in this procedure:

1. Point the Policy Server to the OpenWave directory server.
2. Initialize the OpenWave directory server.
3. Create the policy store schema for r12.1.
4. Change the SiteMinder Super User password.
5. Import the base policy store data.

To configure an OpenWave Directory Server as a policy store

1. Point the Policy Server to the OpenWave 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 group box, configure the fields for an LDAP policy store.

      Sample values:

      - 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 Administration Guide* for a complete description of the LDAP settings.

d. Click Apply.

e. Click the Test LDAP Connection button.

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 OpenWave directory is running.

2. Copy the supplied file schema.txt from *dir_config_home*\openwave to *policy_server_home*\bin.

dir_config_home

Specifies the Directory Configuration installation path.

policy_server_home

Specifies the Policy Server installation path.

3. Navigate to *policy_server_home*\bin, and run the following command:

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

-f

Specifies the name of the schema file that is supplied with r12.1.

4. On the machine where the OpenWave directory server is installed, log in to the primary master directory server as the directory user.

5. For the supplied file *dir_config_home*\openwave\index.sql:

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 file:

dir_config_home\openwave\tablemap.txt

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. Run the following command:

    smldapsetup ldmod -f*dir_config_home*\xps\openwave\OpenWave.ldif

    -f

    Specifies the path and name of the XPS schema file that is supplied with r12.1.

    dir_config_home

    Specifies the Directory Configuration installation path.

    The policy store schema is created for r12.1.

13. 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 policy_server_home\bin.

    b. Execute the following command:

    smreg -su *superuserpassword*

    superuserpassword

    Specifies the password for the SiteMinder Super User account.

    Note: Ensure there is a space between -su and the password.

    c. Delete smreg.exe.

    Note: Deleting smreg.exe prevents someone from changing the Super User password without knowing the previous password.

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

    smobjimport -i*policy_server_home*\db\smdif\smpolicy.smdif
    -d*superusername* -w*superuserpassword* -v

    The base policy store data is imported.

    superusername

    Specifies the Super User name of the SiteMinder administrator.

    superuserpassword

    Specifies the password for the SiteMinder Super User.

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

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
```

15. Run the following command:

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

-dsiteminder_super_user_name

Specifies the name of the SOA Security Manager Super User account.

-wsiteminder_super_user_password

Specifies the password for the SOA Security Manager Super User account.

-f

Overrides duplicate objects

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

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

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

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Connect to an OpenWave Policy Store

You can configure a connection from the Policy Server to an OpenWave policy store by pointing the Policy Server at the policy store.

To point the Policy Server at the policy store

1. Open the Policy Server Management Console.
2. Click the Data tab.
3. Select Policy Store from the Database list.
4. Select LDAP from the Storage list.

5. Configure the following settings on the LDAP policy store group box:
   - LDAP IP Address
   - Admin Username
   - Password
   - Confirm Password

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

   The policy store settings are saved.
7. Click Test LDAP Connection.

   SiteMinder returns a confirmation that the Policy Server is connected to the policy store.

Configure a Connection from the Policy Server to an OpenWave Directory User Store

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

To configure a connection from the Policy Server to an Openwave Directory user store

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

   The Create User Directory pane opens.
3. Click OK.

   The Create User Directory: *Name* pane opens.

   Note: You can specify user directory properties on this pane. For more information about the fields, settings, and options, click Help.
4. Type the name and a description of the new User Directory object in the fields on the General group box.
5. Verify that LDAP is selected from the Namespace list, and type the IP address and port number in the Server field on the Directory Setup group box.

   Note: When the Policy Server is operating in FIPS mode and the User Directory connection is a secure SSL connection, the certificates used by the Policy Server and the user store must be FIPS compliant.
6. Select the Require Credentials check box, and type the full DN and password of the administrator in the fields on the Administrator Credentials group box.

7. Type the root node and search parameters in the fields on the LDAP Search group box.
8. Type a beginning text string and an ending text string in the fields on the LDAP User DN Lookup group box.

   Note: The beginning text string, username, and ending text string are combined to create the string that is used for searching the User Directory tree.
9. (Optional) Complete the fields on the User Attributes group box.
   a. Type the Universal ID in the Universal ID field.

      Attribute type: string

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

      Attribute type: string

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

      Attribute type: binary

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

      Attribute type: binary

      Note: This attribute is required by Password Services.

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

      Attribute type: string

   f. Leave the Email field blank.

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

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

      Attribute type: string

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

    The Create Attribute Mapping pane opens.

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

    The Create User Directory task is submitted for processing.

More information:

How to Configure an LDAP User Directory Connection over SSL (see page 163)

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing policy store to r12.1.

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

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

   Note: The existing r6.x policy store schema has not changed. The r12.1 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.1.
3. Import the Base Policy Store Objects.

   Note: There is no change to policy store data if you are upgrading from 6.0 SP5. You do not have to import a policy store data (.smdif) file if you are upgrading from 6.0 SP5.
4. Import the Policy Store Data Definitions.

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

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

Extend the OpenWave Directory Server Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.1. There are no changes to the existing 6.x policy store schema.

To extend an existing OpenWave Directory Server policy store schema

1. Navigate to *policy_server_home*/bin or *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smldapsetup ldmod
   -f*dir_config_home*/xps/openwave/OpenWave.ldif

   -f

   Specifies the path and name of the XPS upgrade file.

   dir_config_home

   Specifies the Directory Configuration installation path.

   The policy store schema is extended to include the objects introduced by r12.1.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:
   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif*upgrade_smdif_file_name*
   -d*siteminder_super_user_name* -w*siteminder_super_user_password*
   -v -f

   -i

   Specifies the path and name of the import file.

   upgrade_smdif_file_name

   Specifies the name of the import file:
   - **6.0 to r12.1:** sm_upgrade_60_to_R12sp1.smdif
   - **6.0 SP1 to r12.1:** sm_upgrade_60sp1_to_R12sp1.smdif
   - **6.0 SP2 to r12.1:** sm_upgrade_60sp2_to_R12sp1.smdif
   - **6.0 SP3 to r12.1:** sm_upgrade_60sp3_to_R12sp1.smdif
   - **6.0 SP4 to r12.1:** sm_upgrade_60sp4_to_R12sp1.smdif
   - **6.0 SP5 to r12.1:** sm_upgrade_60sp5_to_R12sp1.smdif

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-v

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

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.1.

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

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

UNIX example: smobjimport

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

The base policy store objects are imported.

3. Run the following command:

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

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

-i

Specifies the path and name of the import file.

-d*siteminder_super_user_name*

Specifies the name of the SOA Security Manager administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SOA Security Manager administrator account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   XPSDDInstall SecCat.xdd

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

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:

Configure a DirX 6.0 D00 Directory Server as a Policy Store (see page 143)
Import the Policy Store Data Definitions (see page 146)
Sample User Directory Settings--Siemens DirX 6.0 (see page 147)
Upgrade a 5.5 Policy Store (see page 148)
Import the Policy Store Data Definitions (see page 151)
How to Upgrade a 6.x Policy Store (see page 152)

Configure a DirX 6.0 D00 Directory Server as a Policy Store

You can configure a Siemens DirX 6.0 D00 Directory Server as a SOA Security Manager r12.1 policy store on a Windows 2000 SP4 Advanced Server.

To configure a Siemens DirX 6.0 D00 Directory Server as a policy store

1. Install DirX 6.0 D00, and accept all of the defaults during installation.

   Note: If you do not have an existing database, install the sample database.

2. Copy the following files from *dir_config_home*\dirx to

   DirX_install_path\scripts\security\Netegrity\SiteMinder:

   - dirxabbr-ext.SiteMinderR12sp1
   - schema_ext_for_SiteMinderR12sp1.adm
   - subschema_ext_for_SiteMinderR12sp1.cp
   - bind.tcl
   - l-bind.cp
   - _setup.bat
   - setup.bat
   - GlobalVar.tcl

dir_config_home

Specifies the Directory Configuration installation path.

DirX_install_path

Specifies the DirX installation path.

Example: C:\program files\siemens\dirx

3. Copy the following files from *dir_config_home*\xps\dirx to *DirX_install_path*\scripts\security\Netegrity\SiteMinder:
   - dirxabbr-ext.XPS
   - schema_ext_for_XPS.adm
   - subschema_ext_for_XPS.cp
4. Rename the following files:
   - schema_ext_for_SiteMinderR12sp1.adm to schema_ext_for_SiteMinder.adm
   - subschema_ext_for_SiteMinderR12sp1.cp to subschema_ext_for_SiteMinder.cp
5. Copy the following files to *DirX_install_path*\client\conf:
   - dirxabbr-ext.SiteMinderR12sp1
   - dirxabbr-ext.XPS
6. Rename dirxabbr-ext.SiteMinderR12sp1 to dirxabbr-ext.SiteMinder.
7. Stop and restart the DirX service.
8. Edit GlobalVar.tcl to update the global variables that the DirX scripts reference.

   Default values:
   - LDAP port: 389
   - Root DN: o=pqr
   - Admin username: cn=admin,o=pqr
   - Admin password: dirx
9. Run setup.bat, and check the resulting log file, setup.log, for errors.
10. Rebind to the DSA using the DirXmanage tool.

    Note: Watch for errors.

11. Create the base tree structure using the DirXmanage tool:
    a. Under o=PQR, create ou=Netegrity.
    b. Under ou=Netegrity, create ou=SiteMinder.
    c. Under ou=SiteMinder, create ou=PolicySvr4.

    The policy store schema is created for r12.1.

12. Navigate to policy_server_home\bin.

    policy_server_home

    Specifies the Policy Server installation path.

13. Run the following command:

    $ smobjimport -i*policy_server_home*\db\smdif\smpolicy.smdif -v

    -i

    Specifies the path and name of the import file.

    -v

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

    Note: You can output to a log file and check for errors.

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

    Note: To import data from an existing policy store, see the section on migrating policy store data in the *Policy Server Installation Guide*.

14. Run the following command:

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

    -i

    Specifies the path and name of the import file.

    -d*siteminder_super_user_name*

    Specifies the name of the SOA Security Manager Super User account.

    -w*siteminder_super_user_password*

    Specifies the password for the SOA Security Manager Super User account.

    -f

    Overrides duplicate objects

    -v

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

    Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

15. Run the following command:

    smreg -su *password*

    The administrator's password is set.

16. Point the Policy Server to the DirX Directory Server by using the Data tab on the Policy Server Management Console.

    Sample values:

    - LDAP IP Address: 123.456.7.8
    - Root DN: o=pqr
    - Admin username: cn=admin,o=pqr
    - Admin password: ********

    The DirX Directory Server is configured as a policy store.

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

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

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

   XPSDDInstall SmObjects.xdd

   XPSDDInstall imports the required data definitions.

3. Run the following command:

   XPSDDInstall EPMObjects.xdd

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   XPSDDInstall SecCat.xdd

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

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

You can can upgrade a Siemens DirX 6.0 D00 Directory Server that is configured as a 5.5 policy store to a r12.1 policy store.

To upgrade a 5.5 policy store

1. Copy the following files from *dir_config_home*\dirx to *DirX_install_path*\scripts\security\Netegrity\SiteMinder:
   - dirxabbr-ext.SiteMinder55ToR12sp1
   - schema_ext_for_SiteMinder55ToR12sp1.adm
   - subschema_ext_for_SiteMinder55ToR12sp1.cp
   - bind.tcl
   - l-bind.cp
   - _setup-upgrade.bat
   - setup-upgrade.bat
   - GlobalVar.tcl

   dir_config_home

   Specifies the Directory Configuration installation path.

   DirX_install_path

   Specifies the DirX installation path.

   Example: C:\program files\siemens\dirx

Note: Do not delete the following schema files already in the folder:

- dirxabbr-ext.SiteMinder55
- schema_ext_for_SiteMinder55.adm
- subschema_ext_for_SiteMinder55.cp

2. Copy the following files from *dir_config_home*\xps\dirx to

   DirX_install_path\scripts\security\Netegrity\SiteMinder:

   - dirxabbr-ext.XPS
   - schema_ext_for_XPS.adm
   - subschema_ext_for_XPS.cp

3. Copy the following files to *DirX_install_path*\client\conf:

   - dirxabbr-ext.Siteminder55toR12sp1
   - dirxabbr-ext.XPS

4. Stop and restart the DirX service.

5. Edit GlobalVar.tcl to update the global variables that the DirX scripts reference.

   Default values:

   - LDAP port: 389
   - Root DN: o=pqr
   - Admin username: cn=admin,o=pqr
   - Admin password: dirx

6. Run setup-upgrade.bat, and check the resulting log file, setup-upgrade.log, for errors.

7. Rebind to the DSA using the DirXmanage tool.

   Note: Watch for errors.

   The policy store schema is extended to include the objects introduced by r12.1.

8. Navigate to *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

9. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif\sm_upgrade_55_to_R12sp1.smdif -v -f

   -i

   Specifies the path and name of the import file.

-v

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

-f

Overwrites duplicate SOA Security Manager objects.

The base policy store data is imported from the file sm_upgrade_55_to_r12sp1.smdif, and the directory server is configured as a r12.1 policy store.

10. Run the following command:

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

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

-i

Specifies the path and name of the import file.

-dsiteminder_super_user_name

Specifies the name of the SOA Security Manager administrator account.

-wsiteminder_super_user_password

Specifies the password for the SOA Security Manager administrator account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

11. Point the Policy Server to the 5.5 policy store on which the schema was upgraded.

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

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

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

   XPSDDInstall SmObjects.xdd

   XPSDDInstall imports the required data definitions.

3. Run the following command:

   XPSDDInstall EPMObjects.xdd

   XPSDDInstall imports the required data definitions.

4. Run the following command:

   XPSDDInstall SecCat.xdd

   XPSDDInstall imports the required data definitions.

5. Run the following command:

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

How to Upgrade a 6.x Policy Store

A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing policy store to r12.1.

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

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

   Note: The existing r6.x policy store schema has not changed. The r12.1 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.1.
3. Import the Base Policy Store Objects.

   Note: There is no change to policy store data if you are upgrading from 6.0 SP5. You do not have to import a policy store data (.smdif) file if you are upgrading from 6.0 SP5.
4. Import the Policy Store Data Definitions.

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

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

Extend the Siemens DirX Policy Store Schema

You can extend an existing 6.x policy store schema to include the objects introduced by r12.1. There are no changes to the existing 6.x policy store schema.

To extend an existing Siemens DirX policy store schema

1. Copy the following files from *dir_config_home*\xps\dirx

   to *DirX_install_path*\scripts\security\Netegrity\SiteMinder:

   - _setup.bat
   - bind.tcl
   - dirxabbr-ext.XPS
   - GlobalVar.tcl
   - l-bind.cp
   - schema_ext_for_XPS.adm

- setup.bat
- subschema_ext_for_XPS.cp

dir_config_home

Specifies the Directory Configuration installation path.

DirX_install_path

Specifies the DirX installation path.

Example: C:\program files\siemens\dirx

2. Copy dirxabbr-ext.XPS to *DirX_install_path*\client\conf.
3. Stop and restart the DirX service.
4. Edit GlobalVar.tcl to update the global variables that the DirX scripts reference.

   Default values:

   - LDAP port: 389
   - Root DN: o=pqr
   - Admin username: cn=admin,o=pqr
   - Admin password: dirx
5. Run setup.bat, and check the resulting log file, setup.log, for errors.
6. Rebind to the DSA using the DirXmanage tool.

   Note: Watch for errors.

The policy store schema is extended to include the objects introduced by r12.1.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Navigate to one of the following locations from a command prompt:

   - Windows—*policy_server_home*\bin
   - UNIX—*policy_server_home*/bin

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   smobjimport -i*policy_server_home*\db\smdif*upgrade_smdif_file_name*
   -d*siteminder_super_user_name* -w*siteminder_super_user_password*
   -v -f

   -i

   Specifies the path and name of the import file.

   upgrade_smdif_file_name

   Specifies the name of the import file:

   - **6.0 to r12.1:** sm_upgrade_60_to_R12sp1.smdif
   - **6.0 SP1 to r12.1:** sm_upgrade_60sp1_to_R12sp1.smdif
   - **6.0 SP2 to r12.1:** sm_upgrade_60sp2_to_R12sp1.smdif
   - **6.0 SP3 to r12.1:** sm_upgrade_60sp3_to_R12sp1.smdif
   - **6.0 SP4 to r12.1:** sm_upgrade_60sp4_to_R12sp1.smdif
   - **6.0 SP5 to r12.1:** sm_upgrade_60sp5_to_R12sp1.smdif

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager administrator account.

   -v

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

   Default output: stdout

   -f

   Overwrites duplicate policy store objects with those from r12.1.

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

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

   UNIX example: smobjimport

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

   The base policy store objects are imported.

3. Run the following command:

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

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

   -i

   Specifies the path and name of the import file.

   -d*siteminder_super_user_name*

   Specifies the name of the SOA Security Manager administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SOA Security Manager administrator account.

   -f

   Overrides duplicate objects.

   -v

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

   Default value: stdout

   -l

   Creates a log file.

   -c

   Indicates that the smdif input file contains unencrypted data.

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Chapter 11: Siemens DirX EE 2.0 Directory Server

This section contains the following topics:

How to Configure a Siemens DirX EE 2.0 Policy Store (see page 157)
How to Upgrade a Siemens DirX EE 2.0 Policy Store (see page 160)

How to Configure a Siemens DirX EE 2.0 Policy Store

To configure a Siemens DirX EE 2.0 Directory Server as a r12.1 policy store, complete the following two procedures:

1. Configure a DirX EE 2.0 Directory Server as a r12.1 Policy Store
2. Import the Policy Store Data Definitions
3. Prepare for the Administrative UI Registration

Configure a DirX EE 2.0 Directory Server as a r12.1 Policy Store

To configure a Siemens DirX EE 2.0 Directory Server as a r12.1 policy store, create the XPS schema in the policy store.

To configure a Siemens DirX EE 2.0 Directory Server as a r12.1 policy store

1. Install DirX EE 2.0.
2. Open the DirX EE Manager, and create the following base tree structure to hold the policy store data:
   a. Under o=MyCompany, create ou=netegrity.
   b. Under ou=netegrity, create ou=Siteminder.
   c. Under ou=Siteminder, create ou=PolicySvr4.

3. Copy the following files from *dir_config_home*\dirxee

   to *DirX_EE_install_path*\scripts\stand_alone\extensions:

   - DirXEE20_SMR12sp1_Schema.ldif
   - add_PS_Indexes.adm
   - XPS_SchemaExt.ldif
   - add_XPS_Indexes.adm

   dir_config_home

   Specifies the Directory Configuration installation path.

   DirX_EE_install_path

   Specifies the DirX EE installation path.

4. From the command prompt, change to the following directory:

   DirX_EE_install_path\scripts\stand_alone\extensions

5. Run the following command:

   dirxmodify -f DirXEE20_SMR12sp1_Schema.ldif -D cn=admin,o=MyCompany -w dirx

   -f

   Specifies the name of the LDIF file.

   -D

   Specifies the bind DN.

   Example: cn=admin,o=MyCompany

   -w

   Specifies the password.

   Example: dirx

   -h

   (Optional) Specifies the host.

   Default: localhost

   -p

   (Optional) Specifies the port number.

   Default: 389

6. Run the following command:

   dirxadm add_PS_Indexes.adm

7. Run the following command:

   dirxmodify -f XPS_SchemaExt.ldif -D cn=admin,o=MyCompany -w dirx

8. Run the following command:

   dirxadm add_XPS_Indexes.adm

   The XPS schema is created.

9. Open the Policy Server Management Console, click the Data tab, and specify the following information in the fields on the tab:

   - LDAP IP Address

     Specifies the IP address of the policy store.

   - Root DN

     Example: o=MyCompany

   - Admin Username

     Example: cn=admin,o=MyCompany

   - Password

     Example: dirx

   The Policy Server points to the DirX EE policy store.

10. Run the following command:

    smreg –su firewall

    The SiteMinder administrator's password is set.

11. Run the following command:

    $smobjimport –i*policy_server_home*\db\smdif\smpolicy.smdif –v

    policy_server_home

    Specifies the Policy Server installation path.

    -i

    Specifies the path and name of the import file.

    -v

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

    Note: You can output to a log file and check for errors.

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

    Note: To import the base policy store data from an existing policy store, see the section on migrating policy store data in the *Policy Server Installation Guide*.

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

How to Upgrade a Siemens DirX EE 2.0 Policy Store

A new directory server instance is not required for a r12.1 policy store. You can upgrade an existing 6.x policy store to r12.1.

To upgrade a Siemens DirX EE 2.0 Directory Server from a 6.x policy store to a r12.1 policy store, complete the following two procedures:

1. Upgrade a DirX EE 2.0 Policy Store from 6.x to r12.1
2. Import the Policy Store Data Definitions

Upgrade a DirX EE 2.0 Policy Store from 6.x to r12.1

To upgrade a Siemens DirX EE 2.0 Directory Server from a 6.x policy store to a r12.1 policy store, create the XPS schema in the policy store.

To upgrade a DirX EE 2.0 Policy Store from 6.x to r12.1

1. Copy the following files from *dir_config_home*\xps\dirxee to *DirX_EE_install_path*\scripts\stand_alone\extensions:
   - add_PS_Indexes.adm
   - XPS_SchemaExt.ldif
   - add_XPS_Indexes.adm

   dir_config_home

   Specifies the Directory Configuration installation path.

   DirX_EE_install_path

   Specifies the DirX EE installation path.
2. From the command prompt, change to the following directory:

   DirX_EE_install_path\scripts\stand_alone\extensions
3. Run the following command:

   dirxadm add_PS_Indexes.adm
4. Run the following command:

   dirxmodify -f XPS_SchemaExt.ldif -D cn=admin,o=MyCompany -w dirx

   -f

   Specifies the name of the LDIF file.

   -D

   Specifies the bind DN.

   Example: cn=admin,o=MyCompany

   -w

   Specifies the password.

   Example: dirx

   -h

   (Optional) Specifies the host.

   Default: localhost

   -p

   (Optional) Specifies the port number.

   Default: 389

5. Run the following command:

   dirxadm add_XPS_Indexes.adm

The XPS schema is created. You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Appendix A: Configuring SOA Security Manager Connections over SSL

This section contains the following topics:

How to Configure an LDAP User Directory Connection over SSL (see page 163)

How to Configure an LDAP User Directory Connection over SSL

Configuring an LDAP user directory connection over SSL requires that you configure SOA Security Manager 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.

- SOA Security Manager uses a Netscape LDAP SDK to communicate with LDAP directories. As a result, SOA Security Manager 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 SOA Security Manager 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 SOA Security Manager user directory connection is configured for a secure connection. For more information, refer to Configure the User Directory Connection for SSL (see page 170).

    - 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 SOA Security Manager 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 2000 or 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! If you are running a SOA Security Manager utility or executable on Windows Server 2008, be sure to open the command–line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SOA Security Manager 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! If you are running a SOA Security Manager utility or executable on Windows Server 2008, be sure to open the command–line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SOA Security Manager 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! If you are running a SOA Security Manager utility or executable on Windows Server 2008, be sure to open the command–line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SOA Security Manager 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 [set the ufi variable for your book], use ASCII characters. Object creation or modification with non-ASCII characters is not supported.

To configure the user store connection for SSL

1. Log in to the Administrative UI.
2. Click Infrastructure, Directory.
3. Click User Directory, Modify User Directory.

   The Modify User Directory pane appears with a list of existing user directory connections.

4. Select the user directory connection you want, and click Select.

   User directory settings appear.

5. Select the Secure Connection check-box, and click Submit.

   The user directory connection is configured to communicate over SSL.

Point the Policy Server to the Certificate Database

You point the Policy Server to the certificate database to configure the Policy Server to communicate with the user directory over SSL.

Note: When you create or modify a Policy Server object in the [set the ufi variable for your book], 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 SOA Security Manager 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 [set the ufi variable for your book], use ASCII characters. Object creation or modification with non-ASCII characters is not supported.

To verify the SSL connection

1. Log in to the Administrative UI.
2. Click Infrastructure, Directory.
3. Click User Directory, View User Directory.

   The View User Directory pane appears with a list of existing user directory connections.
4. Select the connection you want, and click Select.

   User directory settings appear.
5. Click View contents.

   If SSL is properly configured, the Directory Content pane appears and lists the contents of the user directory.

Index

A

About this Guide • 9
Add Entries • 118
Add the Root Certificate Authority to the Certificate Database • 166
Add the Server Certificate to the Certificate Database • 168
Add the SOA Security Manager Schema File to Manage Schema Files • 44, 54
Assign Root User Privileges • 65

B

Before You Configure a Connection over SSL • 164
Berkeley Database Version Mismatch Errors • 130
Building and Installing openSSL • 130

C

CA Product References • iii
Configure a Connection from the Policy Server to an OpenLDAP User Store • 123
Configure a Connection from the Policy Server to an OpenWave Directory User Store • 136
Configure a DB2 Data Source for SiteMinder • 30
Configure a DirX 6.0 D00 Directory Server as a Policy Store • 143
Configure a DirX EE 2.0 Directory Server as a r12.1 Policy Store • 157
Configure a Domain in Oracle Internet Directory • 92
Configure an inJoin Directory Server as a Policy Store • 11
Configure an OpenWave Directory Server as a Policy Store • 131
Configure an SSL Connection • 16
Configure MySQL Server Directory Connections • 67
Configure SSL for a Policy Store • 124
Configure the DB2 Wire Protocol Driver • 32
Configure the User Directory Connection for SSL • 164, 170
Configuring SOA Security Manager Connections over SSL • 163
Connect to an OpenWave Policy Store • 135
Contact CA • iii
Create a DB2 Data Source on UNIX Systems • 31
Create a DB2 Data Source on Windows Systems • 31
Create a DB2 Database with SiteMinder Schema • 29
Create a Directory Entry and Root Nodes • 44
Create a MySQL Data Source • 66
Create a Sample User Store • 67
Create a User Store • 123
Create the Base Tree Structure • 117
Create the Certificate Database Files • 165
Create the Policy Store • 120
Create the Policy Store Schema • 48, 55, 74, 81, 95, 101
Critical Path inJoin Directory Server v4.2 • 11
Cyrus SASL Installation • 130

D

Directory Configuration Overview • 9

E

Edit the Novell XPS Schema File • 72, 81, 86
Edit the Policy Store Schema File • 71, 80
Edit the V3 Matchingrules File • 43, 54
Enable LDAP Tracing in IDS • 15
Enable User Authentication • 114
Extend the IBM DB2 Policy Store Schema • 38
Extend the IBM Directory Server Policy Store Schema • 61
Extend the inJoin Policy Store Schema • 23
Extend the Novell Policy Store Schema • 87
Extend the OpenLDAP Policy Store Schema • 126
Extend the OpenWave Directory Server Policy Store Schema • 138
Extend the Oracle Internet Directory Policy Store Schema • 107
Extend the Siemens DirX Policy Store Schema • 152

G

Gather Directory Server Information • 45, 53, 69, 79, 91, 100

Gather SiteMinder Information • 54, 80, 101

H

How to Configure a Connection from the Policy Server to a MySQL Server User Store • 67
How to Configure a Siemens DirX EE 2.0 Policy Store • 157
How to Configure an IBM DB2 Database as a Data Store • 29
How to Configure an LDAP User Directory Connection over SSL • 163
How to Configure the Directory Server as a Policy Store • 118
How to Configure the Directory Sever as a User Store • 122
How to Configure the Policy Server • 92
How to Configure the Policy Store • 45, 70
How to Configure the Slapd Configuration File • 113
How to Create the Database • 117
How to Set Up a MySQL Server • 65
How to Upgrade a 6.x Policy Store • 23, 37, 61, 85, 107, 125, 138, 152
How to Upgrade a Novell eDirectory Policy Store • 78
How to Upgrade a Siemens DirX EE 2.0 Policy Store • 160
How to Upgrade an IBM Secureway Directory Policy Store • 52
How to Upgrade an Oracle Internet Directory Policy Store • 99

I

IBM DB2 • 29
IBM Directory Server • 43
IBM Directory Server as a Policy Store • 43
Import the Base Policy Store Objects • 25, 38, 57, 62, 82, 87, 103, 109, 127, 139, 153
Import the Default Policy Store Objects • 34, 49, 75, 97
Import the Policy Store Data Definitions • 14, 22, 27, 36, 40, 51, 59, 64, 77, 84, 90, 98, 105, 111, 122, 129, 135, 141, 146, 151, 156, 160, 162
Install the MySQL Connector • 65
Install the NSS Utility • 165

L

LDAP Referrals • 142
Limitations of Policy Store Objects in Novell eDirectory • 78
List the Certificates in the Certificate Database • 169

M

MySQL Server • 65

N

Novell eDirectory • 69
Novell eDirectory as a Policy Store • 69

O

OpenLDAP Server • 113
OpenWave Directory Server 6.0.1 • 131
Oracle Internet Directory as a Policy Store • 91
Oracle Internet Directory Server • 91

P

Point the Policy Server to the Certificate Database • 171
Point the Policy Server to the Directory Server • 93, 119
Point the Policy Server to the Policy Store • 15, 46, 72

R

Refresh the LDAP Server • 77, 85
Restart the OpenLDAP Server • 117
Restart the Policy Server • 52, 59, 78, 85, 99, 106

S

Sample Policy Server Settings--Critical Path InJoin Directory Server • 19
Sample User Directory Settings--Critical Path InJoin Directory Server • 18
Sample User Directory Settings--Siemens DirX 6.0 • 147
Set Oracle Internet Directory Attributes • 106
Set the SOA Security Manager Super User Password • 47, 73, 94
Siemens DirX 6.0 D00 Directory Server • 143
Siemens DirX EE 2.0 Directory Server • 157
Specify Database Directives • 114
Specify the SiteMinder Schema Files • 113
Support Client-Side Sorting • 115

T

Test the Configuration File • 116
Troubleshooting OpenLDAP • 130

U

Upgrade a 5.5 Policy Store • 19, 148
Upgrade a 5.x IBM Directory Server Policy Store • 52
Upgrade a 5.x Novell eDirectory Policy Store • 78
Upgrade a 6.x Session Server • 36
Upgrade a DirX EE 2.0 Policy Store from 6.x to r12.1 • 161
Upgrade Limitations for IBM Secureway Directory Server Policy Stores • 60

V

Verify the SSL Connection • 171