CA SiteMinder®

Policy Server Installation Guide

12.52

technologies

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

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

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

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

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

The manufacturer of this Documentation is CA.

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

CA Technologies Product References

This document references the following CA Technologies products:

- CA Directory
- CA SiteMinder®
- CA Business Intelligence

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Documentation Changes

The following updates have been made to the 12.52 documentation as a result of issues found in previous releases of CA SiteMinder®:

- Restart the Report Server (see page 421)—Updated the value of the LD_LIBRARY_PATH variable.
- Edit the Policy Store Schema Files (see page 152)—Updated the command to edit the policy store scheme file used for configuring a Novell eDirectory policy store.
- Korn Shell (ksh) Package Required on Linux (see page 62)—Added to describe that the package is required for the Policy Server installation.
- Create the Audit Store Schema (see page 344)—Revised DB2 instructions. Remove only the NULL keyword from each assertion, instead of the entire assertion itself.
- Authentication Schemes Supporting MBCS URLs (see page 555)—Corrected typographical error. This update resolves CQ171840.
- Microsoft SQL Server Information (see page 39)—Added note stating that credentials for an administrator with create privilege are not required if the CA SiteMinder® schema is already present in the database.
- How to Configure the Policy Store (MySQL) (see page 272)—Revised this topic and the topic, Create the CA SiteMinder® Schema (see page 273) to include new schema files that support Unicode characters. This update resolves CQ178545.
- Required patches for the Java Cryptographic Extension (JCE) (see page 19)—This item details the files that require updates to use the cryptographic algorithms provided by Java. Resolves CQ 174929.
- Required Linux Libraries (see page 24)—Added note stating that all the RPM packages that are required for 64-bit Red Hat 6.x are 32-bit packages. This update resolves CQ 177043.
- Oracle Directory Server as a Policy Store (see page 176)—Made changes to smldapsetup command definitions. This update resolves CQ 177321.
- Configure an Oracle Policy Store (see page 299), Configure a MySQL Policy Store (see page 271), and Configure a SQL Server Policy Store (see page 285)—Updated to replace DataDirect 6.0 driver (no longer supported) instructions with instructions for DataDirect 7.1 drivers. Resolves CQ 177973.
- Microsoft SQL Server Information (see page 39)—Added note stating that if the CA SiteMinder schema is already present in the database, the wizard does not require the credentials of a database administrator with create permission. Resoves CQ 176984.
- How to Configure Oracle Virtual Directory as a Policy Store (see page 213)—Added section describing how to configure Oracle Virtual Directory as a Policy Store. Resolves CQ 174391.

- How to Configure Oracle Unified Directory as a Policy Store (see page 199)—Added section describing how to configure Oracle Unified Directory as a Policy Store. Resolves CQ 172420.
- Configure an Oracle Data Source for CA SiteMinder® (see page 305)—Added content describing how to creating the data source for Oracle Real Application Clusters 11g R2 with SCAN (Single Client Access Name) functionality. Resolves CQ 171215.
- Required Linux Libraries (see page 24)—Added complete list of required Linux libraries and included topic in the "Administrative UI Installation Requirements" chapter. Resolves CQs 169427 and 171403. Resolves STAR issues 21343328-04 and 21436925-1.

Contents

Chapter 7: Configuring CA SiteMinder® Data Stores in a Relational Database 265

Chapter 8: Installing the Administrative UI 365

Chapter 9: Installing Reports 391

Chapter 10: Configuring the OneView Monitor 435

Chapter 11: SNMP Support 443

Chapter 12: Installing the Administrative UI to an Existing Application Server 451

Chapter 13: Troubleshooting 475

Appendix A: Configuring the Policy Server for an International Environment 551

Appendix B: Modified Environment Variables 559

Index 561

Chapter 1: Policy Server Installation Requirements

Policy Server System Requirements

The following sections detail the minimum system requirements for installing a Policy Server on a Windows and UNIX system.

Windows

The Windows system where you install the Policy Server must meet the following minimum system requirements:

- **CPU**—x86 or x64.
- **Memory**—2 GB of system RAM.

  Note: We recommend 2 GB of RAM for Policy Server processing. We recommend at least 4 GB of RAM be available to the Policy Server host system for additional processing.
- **Available disk space**:
  - 4 GB of free disk space in the install location.
  - 3 GB of free space in the temporary file location of the system.

    Note: These requirements are based on a medium size policy database of approximately 1,000 policies.
- **JDK**—Verify that the required JRE, which is shipped with the JDK, is installed on the Policy Server host system.
- **JCE**—The current Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction patches are required to use the Java cryptographic algorithms. To locate the JCE package for your operating platform, go to the Oracle website.

  Apply the patches to the following files on your system:

  - local_policy.jar
  - US_export_policy.jar

  These files are in the directory *jre_home*\lib\security.

  jre_home

  This variable specifies the location of the Java Runtime Environment installation.

- **LDAP directory server or relational database**—Verify that you are using a CA SiteMinder®-supported LDAP directory server or relational database as a policy store.

  Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

UNIX

The UNIX system where you install the Policy Server must meet the following minimum system requirements:

- **CPU**
  - **Solaris**–UltraSparc 440MHz or better.
  - **Red Hat**–x86 or x64.

    Note: The Red Hat operating system relies on entropy for its performance. Before installing the component, increase entropy. Without sufficient entropy, the installation can take an exceedingly long time to complete. We recommend that you use the following command to set a symbolic link:

    ```
    mv /dev/random /dev/random.org
    ln –s /dev/urandom /dev/random
    ```
- **Memory**—2 GB of system RAM.

  Note: We recommend 2 GB of RAM for Policy Server processing. We recommend at least 4 GB of RAM be available to the Policy Server host system for additional processing.
- **Available disk space**:
  - 4 GB of free disk space.
  - 3 GB of free disk space in /tmp.

    Note: Typically, 10 MB of free disk space in /tmp is required for the daily operation of the Policy Server. The Policy Server creates files and named pipes under /tmp. The path to which these files and pipes are created cannot be changed.
- **JRE**—Verify that the required JRE version is installed on the system where you install the Policy Server.

- **JCE**—The current Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction patches are required to use the Java cryptographic algorithms. To locate the JCE package for your operating platform, go to the Oracle website.

  Apply the patches to the following files on your system:

  - local_policy.jar
  - US_export_policy.jar

  These files are in the directory *jre_home*/lib/security.

  jre_home

  This variable specifies the location of the Java Runtime Environment installation.

- **LDAP directory server or relational database**—Verify that you are using a CA SiteMinder®-supported LDAP directory server or relational database as a policy store.

  Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

Chapter 2: Administrative UI Installation Requirements

System Requirements

The following sections detail the minimum system requirements for installing the Administrative UI using the stand-alone installation option.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

Verify That the Windows Host Meets System Requirements

A Windows Administrative UI host system for a stand–alone install must meet the following minimum system requirements:

- **CPU**—x86 or x64, 1.2 GHz or better.
- **Memory**—1 GB of system RAM. We recommend 2 GB.
- **Available disk space**—840 MB.
- **Temp directory space**—3 GB.
- **Screen resolution**—1024 x 768 or higher resolution with 256 colors or better to view the Administrative UI properly.

Verify the UNIX Host Meets System Requirements

A UNIX Administrative UI host system for the stand–alone install meets the following minimum system requirements::

- **CPU**
  - Solaris—UltraSparc, 440 MHz or better.
  - Red Hat Linux—x86 or x64, 700 MHz or better.

    Note: The Red Hat 6 operating system relies on entropy for performance. Increase entropy before installing the component. Without sufficient entropy, the installation can take an exceedingly long time to complete. We recommend that you use the following command to set a symbolic link:

    ```
    mv /dev/random /dev/random.org
    ln –s /dev/urandom /dev/random
    ```

- **Memory**—1 GB of system RAM. We recommend 2 GB.
- **Available disk space**—840 MB.
- **Temp directory space**—3 GB.
- **Screen resolution**—1024 x 768 or higher resolution with 256 colors or better to view the Administrative UI properly.

Required Linux Libraries

Certain library files are required for components operating on Linux operating environments. Failure to install the correct libraries can cause the following error:

```
java.lang.UnsatisfiedLinkError
```

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

Red Hat 5.x:

compat–gcc-34-c++-3.4.6-*patch_version*.I386

libstdc++-4.x.x-x.el5.i686.rpm

Red Hat 6.x:

libstdc++-4.x.x-x.el6.i686.rpm

Additionally, for Red Hat 6.x (64-bit):

Note: All the RPM packages that are required for 64-bit Red Hat 6.x are *32-bit* packages.

libXau-1.0.5-1.el6.i686.rpm

libxcb-1.5-1.el6.i686.rpm

compat-db42-4.2.52-15.el6.i686.rpm

compat-db43-4.3.29-15.el6.i686.rpm

libX11-1.3-2.el6.i686.rpm

libXrender-0.9.5-1.el6.i686.rpm

libexpat.so.1 (provided by expat-2.0.1-11.el6_2.i686.rpm)

libfreetype.so.6 (provided by freetype-2.3.11-6.el6_2.9.i686.rpm)

libfontconfig.so.1 (provided by fontconfig-2.8.0-3.el6.i686.rpm)

libICE-1.0.6-1.el6.i686.rpm

libuuid-2.17.2-12.7.el6.i686.rpm

libSM-1.1.0-7.1.el6.i686.rpm

libXext-1.1-3.el6.i686.rpm

compat-libstdc++-33-3.2.3-69.el6.i686.rpm

compat-db-4.6.21-15.el6.i686.rpm

libXi-1.3-3.el6.i686.rpm

libXtst-1.0.99.2-3.el6.i686.rpm

libXft-2.1.13-4.1.el6.i686.rpm

libXt-1.0.7-1.el6.i686.rpm

libXp-1.0.0-15.1.el6.i686.rpm

Chapter 3: Report Server Installation Requirements

System Requirements

The following sections detail the minimum system requirements for installing the Report Server.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

Windows

The Windows system to which you are installing the Reports Server must meet the following minimum system requirements:

- **CPU**—Intel® Pentium™ 4–class processor, 2.0 GHz.
- **Memory**—2 GB of RAM.
- **Available disk space**—10 GB.

  Note: This requirement is the space that is required to install the Report Server. This requirement does not account for the disk space that is required to store reports.
- **Temp directory space**—1 GB.
- **Screen resolution**—1024 x 768 or higher resolution with 256 colors or better to view reports properly in the Administrative UI.

UNIX

The UNIX system to which you are installing the Reports Server must meet the following minimum system requirements:

- **CPU**
  - (Solaris) SPARC v8plusSparc
  - (Red Hat Linux) Intel Pentium 4–class processor, 2.0 GHz.
- **Memory**—2 GB of RAM.

- **Available disk space**—10 GB.

  Note: This requirement is the space that is required to install the Report Server. This requirement does not account for the disk space that is required to store reports.

- **Temp directory space**—1 GB.
- **Screen resolution**—1024 x 768 or higher resolution with 256 colors or better to view reports properly in the Administrative UI.

Solaris Required Patch Clusters

The Report Server requires specific Solaris patch clusters. Update the Solaris system before installing the Report Server.

Important! If you do not install the required patches, the Report Server installation fails.

Note: For more information about the Solaris patch clusters, see the *Policy Server Release Notes*.

Red Hat Required Patch Clusters

The Report Server requires specific Red Hat patch clusters. Update the Red Hat system before installing the Report Server.

Important! If you do not install the required patches, the Report Server installation fails.

Note: For more information about the Red Hat patch clusters, see the *Policy Server Release Notes*.

Report Database Requirements

The Report Server requires a report database to run reports. The Report Server installer can install an embedded version of Sun Microsystems MySQL™ (MySQL) to function as the report database.

If you do not install the embedded version of MySQL, a supported version of the following can be used:

- Microsoft® SQL Server® (SQL Server)
- Oracle®

Important! The Report Server is a CA common component that CA products can share. As such, the installer lets you configure the report database to database types and versions that other products support, but CA SiteMinder® does not. For a list of supported database types and versions, see the CA SiteMinder® 12.52 Platform Support Matrix.

Connectivity Requirements

The Report Server requires a driver to communicate with the following:

- A SQL Server or Oracle report database

  Note: If you use the embedded version of MySQL, there are no report database connectivity requirements.

- A CA SiteMinder® audit store

Be sure that a supported Microsoft SQL Server driver or Oracle Net client is installed on the Report Server host system.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

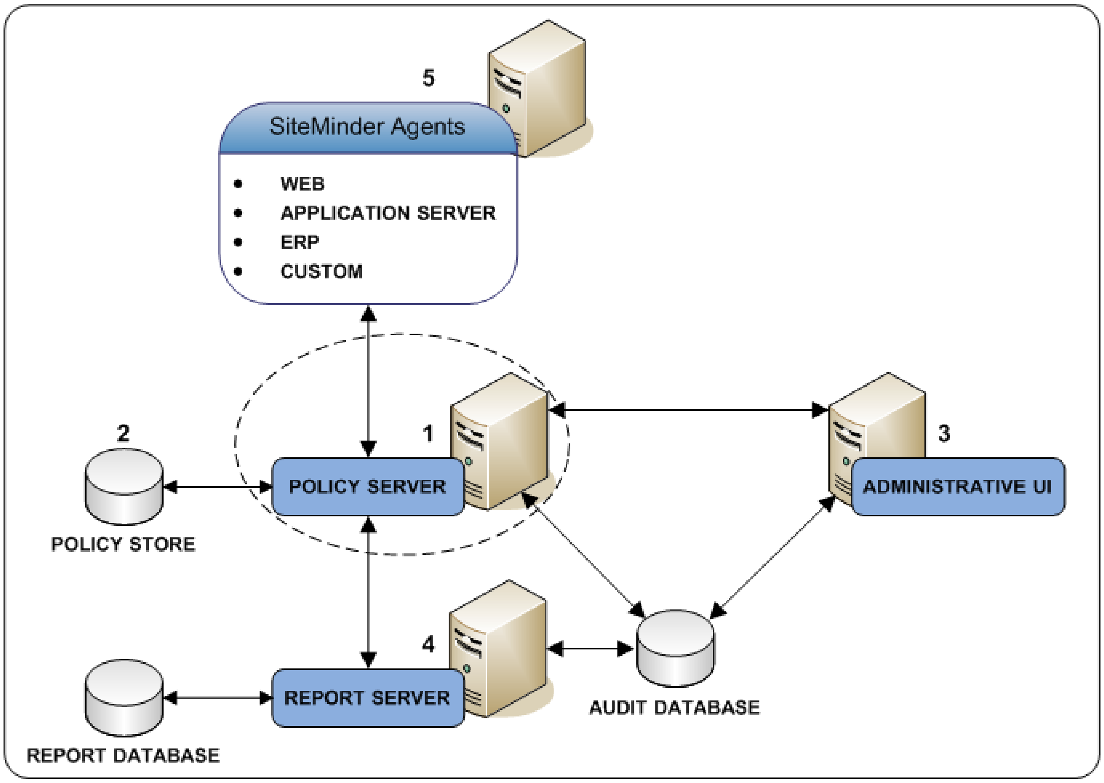
Chapter 4: Installing the Policy Server on Windows Systems

Installation Road Map

The following diagram illustrates a sample CA SiteMinder® installation and lists the order in which you install and configure each component. Consider the following items:

- Confirm that the Policy Server host system meets the minimum system requirements. We recommend doing so before installing the Policy Server.
- A dotted line surrounds the Policy Server. Install this component now.

Figure 1: Installation Roadmap



More information:

Policy Server System Requirements (see page 19)

Before You Install the Policy Server

Consider the following items before installing the Policy Server:

- **Administrator privileges**—A Windows account with local administrator privileges is required to install the Policy Server.
- **System path length**—If the system path length exceeds 1024 characters, the Policy Server installation fails. The limitation applies to both included or excluded CA SiteMinder® added directories.

  Note: We recommend trimming the pre–CA SiteMinder® system path to approximately 700 characters for best results.

- (Windows 2008) **Firewall settings**–If you are installing a Policy Server on Windows 2008, update the Windows firewall settings to allow inbound connections on the following ports:
  - 44441
  - 44442
  - 44443

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

  Note: For more information, see the Microsoft documentation.

- **Environment variables**—The Policy Server installation modifies environment variables.

How to Install the Policy Server

To install the Policy Server complete the following procedures:

1. Review the Policy Server component considerations.
2. Review the policy store considerations.
3. Review the FIPS considerations.
4. Gather information for the Policy Server installer.
5. Run the Policy Server installer.
6. (Optional) If you configured SNMP, enable SNMP event trapping.
7. (Optional) If you do not use the Policy Server installer to configure a policy store, manually configure the policy store.

More information:

Reinstall the Policy Server (see page 51)

Policy Server Component Considerations

In addition to the Policy Server, the installer can install and configure the following components. Review the following items before installing the Policy Server:

- OneView Monitor

  The OneView Monitor enables the monitoring of CA SiteMinder® components.

  Note: A supported Java SDK and ServletExec/AS is required to configure the OneView Monitor.

- Policy store

  Note: The key store and the certificate data store are automatically configured and collocated with the policy store.

- SNMP

  Be sure that you have an SNMP Service (Master OS Agent) installed with your Windows operating system before installing the Policy Server.

  Note: For more information about installing the SNMP Service, see the Windows online help system.

- Audit Logs

  You can store audit logs in either a relational database or a text file. After you install the Policy Server, audit logging is set to a text file and not to ODBC by default.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

Policy Store Considerations

Consider the following items before running the Policy Server installer or the Policy Server Configuration wizard:

- The Policy Server installer and the Policy Server Configuration wizard can automatically configure one of the following stores as a policy store:

  - Microsoft Active Directory Lightweight Directory Services (AD LDS)

    Note: Be sure that you have met the prerequisites for configuring AD LDS as a policy store.

  - Oracle® Directory Enterprise Edition (formerly Sun Java™ System Directory Server)

    Important! The Policy Server installer and the Policy Server Configuration wizard cannot automatically configure a policy store that is being connected to using an SSL connection.

  - Microsoft SQL Server®
  - Oracle RDBMS

- (RDB policy store) The Policy Server installer or the Policy Server Configuration Wizard use specific database information to create the policy store data source. The Policy Server uses this data source to communicate with the policy store. Consider the following items:
  - The name of data source is CA CA SiteMinder® DSN.
  - The installer saves the data source to the Microsoft ODBC Data Source Administrator tool, under the System DSN tab.

- (RDB policy store) Verify that the database server that is to host the policy store is configured to store objects in UTF–8 form. This configuration avoids possible policy store corruption.
  - (Oracle) Be sure that the database is configured to store objects in UTF–8 form. Oracle supports unicode within many of their character sets. For more information about configuring your database to store objects in UTF–8 form, see your vendor–specific documentation.
  - (SQL Server) Be sure that the database is configured using the default collation (SQL_Latin1_General_CP1_CI_AS). Using a collation that is case–sensitive can result in unexpected behaviors. For more information about configuring your database to store objects using the default collation, see your vendor–specific documentation.

- The certificate data store is automatically collocated with the policy store.
- You manually configure any other supported directory server or relational database as a policy store after installing the Policy Server. Configuring a policy store manually is detailed in this document.

More information:

Configuring CA SiteMinder® Data Stores in a Relational Database (see page 265)

FIPS Considerations

The Policy Server uses certified Federal Information Processing Standard (FIPS) 140-2 compliant cryptographic libraries. FIPS is a US government computer security standard that is used to accredit cryptographic modules that meet the Advanced Encryption Standard (AES). The libraries provide a FIPS mode of operation when a CA SiteMinder® environment only uses FIPS-compliant algorithms to encrypt sensitive data.

You can install the Policy Server in one of the following FIPS modes of operation.

Note: The FIPS mode a Policy Server operates in is system-specific. For more information, see the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

- **FIPS-compatibility mode**—The default FIPS mode of operation during the installation is FIPS-compatibility mode. In FIPS-compatibility mode, the environment uses existing CA SiteMinder® algorithms to encrypt sensitive data and is compatible with previous versions CA SiteMinder®:
  - The use of FIPS-compliant algorithms in your environment is optional.
  - If your organization does not require the use of FIPS-compliant algorithms, install the Policy Server in FIPS-compatibility mode. No further configuration is required.
- **FIPS-migration mode**—FIPS-migration mode lets you transition an 12.52 environment running in FIPS-compatibility mode to FIPS-only mode.

  In FIPS-migration mode, the 12.52 Policy Server continues to use existing CA SiteMinder® encryption algorithms as you migrate the 12.52 environment to use only FIPS-compliant algorithms.

  Install the Policy Server in FIPS-migration mode if you are in the process of configuring the existing environment to use only FIPS-compliant algorithms.
- **FIPS-only mode**—In FIPS-only mode, the environment only uses FIPS-compliant algorithms to encrypt sensitive data.

  Install the Policy Server in FIPS-only mode if the existing environment is upgraded to 12.52 and the existing environment is configured to use only FIPS-compliant algorithms.

  Important! A 12.52 environment that is running in FIPS-only mode cannot operate with versions of CA SiteMinder® that do not also fully support FIPS (that is, versions before r12.0). This restriction applies to all agents, custom software using older versions of the Agent API, and custom software using PM APIs or any other API that the Policy Server exposes. Relink all such software with the 12.52 versions of the respective SDKs to achieve the required FIPS support.

Note: For more information about migrating an environment to use only FIPS-compliant algorithms, see the *Upgrade Guide*.

Gather Information for the Installer

The Policy Server installer requires specific information to install the Policy Server and any optional components.

Note: Installation worksheets are provided to help you gather and record information prior to installing or configuring Policy Server components using the Policy Server Installation Wizard or the Policy Server Configuration Wizard. You may want to print these worksheets and use them to record required information prior to running either wizard.

Required Information

Gather the following required information before running the Policy Server installer or the Configuration wizard. You can use the Required Information Worksheet to record your values.

- **Java version** - Identify the supported Java Runtime Environment version for the Policy Server to use. On UNIX, verify that the JAVA_HOME system variable is set to the location of the JRE. If the JAVA_HOME system variable is incorrectly set, the installer cannot locate the JRE.

- **Policy Server installation location** - Determine where the installer is to install the Policy Server.

  Default: C:\Program Files\CA

- **CA SiteMinder® Encryption key value** - Determine the encryption key value. An encryption key is a case–sensitive, alphanumeric key that secures the data that is sent between the Policy Server and the policy store. All Policy Servers that share a policy store are required to use the same encryption key. For stronger protection, define a long encryption key.

  Limits: 6 to 24 characters.

- **Advanced Authentication Server Encryption key value** - Determine the encryption key value. Use a case–sensitive, alphanumeric value. This key secures the data that is sent between the Policy Server and the advanced authentication server (running on the CA SiteMinder® SPS). The CA SiteMinder® SPS and all Policy Servers require the same key. For stronger protection, define a long encryption key.
  Limits: 6 to 24 characters.

Active Directory LDS Server Information

Gather the following required information to configure Microsoft Active Directory LDS as a policy store:

- **System IP address**—Identify the IP address of the directory server host system.
- **Port number—**Identify the port number on which the directory server is listening.
- **Root DN of the application partition**—Identify the root DN location of the application partition in the directory server where the policy store schema data must be installed.

  Example: dc=ca,dc=com

- **Administrator domain name**—Identify the full domain name, including the guid value, of the directory administrator.

  Example: CN=user1,CN=people,CN=Configuration,CN=*guid*

- **Administrator password**—Identify the password of the directory administrator.
- **Alternate user account**—By default, CA SiteMinder® uses the administrator account to communicate with the directory server. However, you can use a different user account to administer the policy store. Identify the complete administrator DN and password to configure CA SiteMinder® to use an alternative user account to administer the policy store.

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

- **CA SiteMinder® superuser password**—The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

  ```
  siteminder
  ```

  Limits:

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

  Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

Oracle Directory Server Information

Gather the following required information to configure Oracle Directory Server to function as a policy store:

- **System IP address**—Determine the IP address of the Oracle Directory Server host system.
- **Directory instance port number**—Determine the port number for the Oracle Directory Server instance.

  Default: 389
- **Root DN—**Identify the root DN of the Oracle Directory Server.

  Example: o=yourorg.com
- **Administrator account**—Identify the user name (Bind DN) for the LDAP administrator account.

  Example: cn=Directory Manager
- **Administrator password**—Identify the password for the Oracle Directory Server administrator.
- **Alternate LDAP administrator**—By default, CA SiteMinder® uses the LDAP administrator account to communicate with the LDAP server. However, you can use a different LDAP user account to administer the policy store. Identify the complete administrator DN and password to configure CA SiteMinder® in this way.

  Note: This user must have the necessary permissions to modify attributes and change passwords.
- **CA SiteMinder® superuser password**—The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

  ```
  siteminder
  ```

  Limits:

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

  Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

Microsoft SQL Server Information

To configure Microsoft SQL Server as a policy store, gather the following required information:

Database server name

Identify the IP address or name of the database host system.

Note: For more information about IPv6 support, see the CA SiteMinder® Platform Support Matrix.

Database name

Identify the named instance or the name of the database that is to function as the policy store.

Database port

Identify the port on which the database is listening.

Database administrator user name and password

Identify the name and password of an administrator account with permission to do the following operations:

- Create schema
- Create, read, modify, and delete objects.

Note: If the CA SiteMinder® schema is already present in the database, the wizard does not require the credentials of a database administrator with **create** permission. For more information, see Configure a SQL Server Policy Store (see page 285).

CA SiteMinder® superuser password

The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

```
siteminder
```

Limits:

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

Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

Oracle RDBMS Information

Gather the following required information to configure Oracle RDBMS as a policy store.

Database server name

Identify the IP address or the name of the database host system.

Note: For more information about IPv6 support, see the CA SiteMinder® Platform Support Matrix.

Database service name

Identify the service name of the database that is to function as the policy store.

Database port

Identify the port on which the database is listening.

Database administrator user name

Identify the name of an administrator account with permission to do the following operations:

- Create schema
- Create, read, modify, and delete objects.

Database administrator password

Identify the password of the administrator account.

CA SiteMinder® superuser password

The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

```
siteminder
```

Limits:

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

Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

OneView Monitor Information

You only have to gather OneView Monitor information if you plan on configuring the OneView Monitor.

Gather the following required information to configure the OneView Monitor. You can use the OneView Monitor Information Worksheet to record your values.

- **JDK path**—Identify the path to the required JDK version.
- **ServletExec installation directory**—Identify ServletExec installation directory.

  Example: /usr/local/NewAtlanta/ServletExecAS
- **ServletExec port number**—Determine the port number for the ServletExec instance.
- **Sun Java System administrator directory**—Determine the following information:
  - The installed location of the Sun Java System.
  - The installed location of the Sun Java System Web servers.

  Example: /*sunjavasystem_home*/*location*

  sunjavasystem home

  Specifies the installed location of the Sun Java System.

  location

  Specifies the installed location of the Sun Java System Web servers.
- **Multiple ServletExec instances**—If you have multiple ServletExec instances, determine the instance to which you want to configure the OneView Monitor GUI.

Run the Policy Server Installer

You install the Policy Server using the installation media on the Technical Support site.

Note: For a list of installation media names, see the *Policy Server Release Notes*.

Follow these steps:

1. Be sure that the system meets the windows requirements.
2. Exit all applications that are running.
3. Do the step appropriate for your version of Windows:
   - **Windows 2008 and Windows 7**: Right-click *installation_media* and select Run as administrator.
   - **Other Windows versions**: Double–click *installation_media*.

     installation_media

     Specifies the name of the Policy Server installation executable.

   The installer starts.

4. Use the gathered system and component information to install the Policy Server and configure Policy Server components. Considering the following items when running the installer:

   - You are prompted to select a FIPS mode of operation. For more information about which FIPS mode to select, see FIPS Considerations (see page 35).

   - When the installer prompts you to select components, clear the Policy Store check box if you are not configuring a policy store automatically. For more information about which stores can be automatically configured as a policy store, see Policy Store Considerations (see page 33).

   - If you are initializing a policy store, you are prompted to enter a password for the default CA SiteMinder® user account. The default account name is

     ```
     siteminder
     ```

   - You are prompted to install the default certificate authority certificates to the certificate data store. You can add additional certificates and private keys to the certificate data store after installation.

   - If you are using IPv6 addresses, surround entries with brackets.

     Example: [2001:db8::1428:57ab]

   - Create an encryption key for the Advanced Authentication server. Use the same key on all Policy Servers in your environment.

5. Review the installation settings and click Install.

   The Policy Server and all selected components are installed and configured.

6. (Optional) If you did not use the installer to configure a policy store, manually configure the policy store.

Note: If you experience problems during the installation, you can locate the installation log file and the policy store details file in *siteminder_home*\siteminder\install_config_info.

siteminder_home

Specifies the Policy Server installation path.

Troubleshoot the Policy Server Installation

Use the following files to troubleshoot the Policy Server installation:

- CA_SiteMinder_Policy_Server_*release*_InstallLog.log

  The installation log contains a summary section that lists the number of successes, warnings, non–fatal errors, and errors that occurred during the installation. Individual installation actions are listed with the respective status.

  release

  Specifies the Policy Server release.

  Location: *siteminder_home*\siteminder\install_config_info

- ca-ps-details.log

  The policy store log details the policy store status.

  Location: *siteminder_home*\siteminder\install_config_info

- smps.log

  The smps.log is created when you start the Policy Server. This log contains the following line if the Policy Server installed successfully:

  ```
  [Info] Journaling thread started, will delete commands older than 60 minutes.
  ```

  Location: *siteminder_home*\siteminder\log

  siteminder_home

  Specifies the Policy Server installation path.

Enable SNMP Event Trapping

This is an optional step. You only have to enable SNMP trapping if you configured this feature when installing the Policy Server.

Note: Before completing this procedure, ensure you have an SNMP Service installed on the Windows systems.

To enable SNMP event trapping, use the XPSConfig utility to set the event handler library (eventsnmp.dll) to the XPSAudit list. The default location of eventsnmp.dll is *policy_server_home*\bin.

policy_server_home

Specifies the Policy Server installation location.

Note: More information on using the XPSConfig utility to set event handler libraries exists in the *Policy Server Administration Guide*.

To finish configuring SNMP event trapping, configure the snmptrap.conf file. The necessary SNMP prerequisites and procedures are detailed in SNMP Support.

More information:

SNMP Support Overview (see page 443)

Configure a Policy Store

If you did not use the Policy Server installer to configure a policy store automatically, manually configure a supported LDAP directory server or relational database as a policy store.

Unattended Policy Server Installation

After the Policy Server is manually installed on one machine, you can reinstall it or install it on a separate machine using an unattended installation mode. An unattended installation lets you install or uninstall the Policy Server without any user interaction.

The installer provides a ca-ps-installer.properties template file that lets you define installation variables. The default parameters, passwords, and paths in this file reflect the information you entered during the initial Policy Server installation. In this file, you can either store encrypted or plain text passwords. If you are using encrypted passwords, for example, a shared secret and CA SiteMinder® Super User, you must use the same ones that you entered during the initial installation since they are encrypted in the file and cannot be modified. However, you can use plain text passwords by modifying the file.

More information:

How to Run an Unattended Policy Server Install (see page 499)

Policy Server Configuration Wizard

Use the Policy Server Configuration wizard to configure or reconfigure the following components after installing the Policy Server:

- A policy store.
- SNMP support.
- The OneView Monitor UI.

Note: You cannot change the Policy Server FIPS–mode of operation using the Policy Server Configuration Wizard. For more information about changing the Policy Server FIPS–mode of operation, see the *CA SiteMinder® Upgrade Guide*.

Important! If you configured an Oracle iPlanet web server instance for the OneView Monitor UI or SNMP, do not use the wizard to configure new instances. Configuring new web server instances can cause the existing web server instance to fail.

More information:

Policy Store Considerations (see page 33)

How to Use the Configuration Wizard

Complete the following procedures to use the Policy Server Configuration wizard:

1. Review the policy store considerations (see page 33).
2. If you are configuring the OneView Monitor UI or one of the following stores as a policy store, gather information for the wizard:
   - Active Directory LDS
   - Oracle Directory Server
   - SQL Server
   - Oracle RDBMS
3. Run the wizard.

Gather Information for the Configuration Wizard

The Policy Server Configuration Wizard requires specific information to configure Policy Server components.

Note: Installation worksheets are provided to help you gather and record information prior to installing or configuring Policy Server components using the Policy Server Installation Wizard or the Policy Server Configuration Wizard. You may want to print these worksheets and use them to record required information prior to running either wizard.

Active Directory LDS Server Information

Gather the following required information to configure Microsoft Active Directory LDS as a policy store:

- **System IP address**—Identify the IP address of the directory server host system.
- **Port number—**Identify the port number on which the directory server is listening.
- **Root DN of the application partition**—Identify the root DN location of the application partition in the directory server where the policy store schema data must be installed.

  Example: dc=ca,dc=com
- **Administrator domain name**—Identify the full domain name, including the guid value, of the directory administrator.

  Example: CN=user1,CN=people,CN=Configuration,CN=*guid*
- **Administrator password**—Identify the password of the directory administrator.
- **Alternate user account**—By default, CA SiteMinder® uses the administrator account to communicate with the directory server. However, you can use a different user account to administer the policy store. Identify the complete administrator DN and password to configure CA SiteMinder® to use an alternative user account to administer the policy store.

  Note: This user must have the necessary permissions to modify attributes and change passwords.
- **CA SiteMinder® superuser password**—The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

  ```
  siteminder
  ```

  Limits:

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

Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

Oracle Directory Server Information

Gather the following required information to configure Oracle Directory Server to function as a policy store:

- **System IP address**—Determine the IP address of the Oracle Directory Server host system.
- **Directory instance port number**—Determine the port number for the Oracle Directory Server instance.

  Default: 389
- **Root DN—**Identify the root DN of the Oracle Directory Server.

  Example: o=yourorg.com
- **Administrator account**—Identify the user name (Bind DN) for the LDAP administrator account.

  Example: cn=Directory Manager
- **Administrator password**—Identify the password for the Oracle Directory Server administrator.
- **Alternate LDAP administrator**—By default, CA SiteMinder® uses the LDAP administrator account to communicate with the LDAP server. However, you can use a different LDAP user account to administer the policy store. Identify the complete administrator DN and password to configure CA SiteMinder® in this way.

  Note: This user must have the necessary permissions to modify attributes and change passwords.
- **CA SiteMinder® superuser password**—The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

  `siteminder`

  Limits:

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

  Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

Microsoft SQL Server Information

To configure Microsoft SQL Server as a policy store, gather the following required information:

Database server name

Identify the IP address or name of the database host system.

Note: For more information about IPv6 support, see the CA SiteMinder® Platform Support Matrix.

Database name

Identify the named instance or the name of the database that is to function as the policy store.

Database port

Identify the port on which the database is listening.

Database administrator user name and password

Identify the name and password of an administrator account with permission to do the following operations:

- Create schema
- Create, read, modify, and delete objects.

Note: If the CA SiteMinder® schema is already present in the database, the wizard does not require the credentials of a database administrator with **create** permission. For more information, see Configure a SQL Server Policy Store (see page 285).

CA SiteMinder® superuser password

The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

```
siteminder
```

Limits:

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

Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

Oracle RDBMS Information

Gather the following required information to configure Oracle RDBMS as a policy store.

Database server name

Identify the IP address or the name of the database host system.

Note: For more information about IPv6 support, see the CA SiteMinder® Platform Support Matrix.

Database service name

Identify the service name of the database that is to function as the policy store.

Database port

Identify the port on which the database is listening.

Database administrator user name

Identify the name of an administrator account with permission to do the following operations:

- Create schema
- Create, read, modify, and delete objects.

Database administrator password

Identify the password of the administrator account.

CA SiteMinder® superuser password

The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

```
siteminder
```

Limits:

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

Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

OneView Monitor Information

You only have to gather OneView Monitor information if you plan on configuring the OneView Monitor.

Gather the following required information to configure the OneView Monitor. You can use the OneView Monitor Information Worksheet to record your values.

- **JDK path**—Identify the path to the required JDK version.
- **ServletExec installation directory**—Identify ServletExec installation directory.

  Example: /usr/local/NewAtlanta/ServletExecAS
- **ServletExec port number**—Determine the port number for the ServletExec instance.
- **Sun Java System administrator directory**—Determine the following information:
  - The installed location of the Sun Java System.
  - The installed location of the Sun Java System Web servers.

  Example: /*sunjavasystem_home*/*location*

  sunjavasystem home

  Specifies the installed location of the Sun Java System.

  location

  Specifies the installed location of the Sun Java System Web servers.
- **Multiple ServletExec instances**—If you have multiple ServletExec instances, determine the instance to which you want to configure the OneView Monitor GUI.

Run the Configuration Wizard

To run the configuration wizard

1. Exit all applications that are running.
2. Navigate to *siteminder_home*\siteminder\install_config_info and double-click ca-ps-config.exe.

   The Policy Server configuration wizard starts.

   siteminder_home

   Specifies the Policy Server installation path.

   Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your CA SiteMinder® component.
3. Use the system and component information you have gathered to configure a policy store and individual components.

   Note: When prompted to initialize the LDAP instance do so only to configure a new policy store instance.

4. Review the installation settings and click Install.

   The wizard configures the selected components to work with the Policy Server.

   Note: This can take several minutes.

5. Click Done and reboot the system.

   The components you selected are configured.

Note: If you experience problems, you can locate the Policy Server installation log file and the policy store details file in *siteminder_home*\siteminder\install_config_info.

siteminder_home

Specifies the Policy Server installation path.

More information:

Troubleshoot the Policy Server Installation (see page 43)

Reinstall the Policy Server

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

To reinstall the Policy Server

1. Stop the Policy Server using the Policy Server Management Console.

   Note: More information on stopping and starting the Policy Server exists in the *Policy Server Administration Guide*.

2. Close the Policy Server Management Console.

3. Install the Policy Server.

4. Start the Policy Server using the Policy Server Management Console.

How to Uninstall the Policy Server

To uninstall the Policy Server complete the following procedures:

1. Set the JRE in the Path System Variable.

2. Shut down all instances of the Policy Server Management Console.

3. Remove Policy Server References from Agent Host Files.

4. Uninstall the Policy Server.

Set the JRE in the Path Variable

You set the JRE in path variable when uninstalling the Policy Server, Web Agent and SDK to prevent the uninstallation program from stopping and issuing one of the following error messages:

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

To set the JRE in the path variable

1. Open the Windows Control Panel.
2. Double-click System.
3. Add the location of the JRE to the Path system variable in the Environment Variables dialog.

Remove Policy Server References from Agent Host Files

You remove the Policy Server reference from the SmHost.conf file to prevent unexpected results from the Web Agent once the Policy Server is uninstalled.

To remove the Policy Server reference

1. Navigate to *web_agent_home*/config.

   web_agent_home

   Specifies the installation directory of the Web Agent.

2. Open the SmHost.conf file in a text editor.
3. Delete the line that begins with "policyserver=".

   Note: This line contains the IP address and port numbers for the Policy Server you are uninstalling.

4. Save SmHost.conf.

   The SmHost.conf file no longer references the Policy Server you are uninstalling.

Stop All CA SiteMinder® Processes

Before you uninstall the Policy Server, stop all CA SiteMinder® processes so that Policy Server files are safely removed.

Follow these steps:

1. Log in to the Windows system.
2. From the Administrative Tools, open the Services.
3. Scroll down to the SiteMinder Policy Server service and select Stop.

All CA SiteMinder® processes stop.

Uninstall the Policy Server

You uninstall the Policy Server when it is no longer required on the system.

Follow these steps:

1. Open the Windows Control Panel and go to the list of programs.
2. Right–click CA CA SiteMinder® Policy Server.
3. Click Uninstall/Change.
4. Follow the instructions of the wizard.

   Note: If you are prompted to remove a shared file, click No to All.
5. If requested, reboot the system.

   The Policy Server is uninstalled.

Remove Leftover Items

Manually remove the following folders, files, registry settings, and virtual directories after uninstalling the Policy Server:

- **Windows system**
  - *siteminder_home*\bin
  - *siteminder_home*\install_config_info
  - C:\Program Files\ZeroG Registry\com.zerog.registry.xml

  Important! Remove all items before reinstalling the Policy Server.

- **AdventNet software registry entry**—Delete the AdventNet software registry entry only if the software was not on the system before installing the Policy Server. This registry entry is located in HKEY_LOCAL_MACHINE\SOFTWARE\Advent,Inc.
- **IIS virtual directories**—Delete the following CA SiteMinder® virtual directories using the IIS Microsoft Management Console
  - 'CA SiteMinder®'
  - 'CA SiteMinder®Cgi'
  - 'CA SiteMinder®Monitor'
  - 'netegrity_docs'

Remove Leftover Services

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

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

To manually remove leftover services

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

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<Registry_Key_Name>
   ```

   Registry_Key_Name

   Specifies the registry key name of the service that is to be removed:

   - SMServMon (CA SiteMinder® Health Monitor Service)
   - SMPolicySrv (CA SiteMinder® Policy Server)
   - Agent Service (SNMP Agent)

   The leftover services are removed.

Scripting Interface

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

siteminder_installation

Specifies the installed location of CA SiteMinder®.

Example: /home/smuser/siteminder/CLI

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

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

Note: More information on the scripting interface exists in the *Programming Guide for Perl*

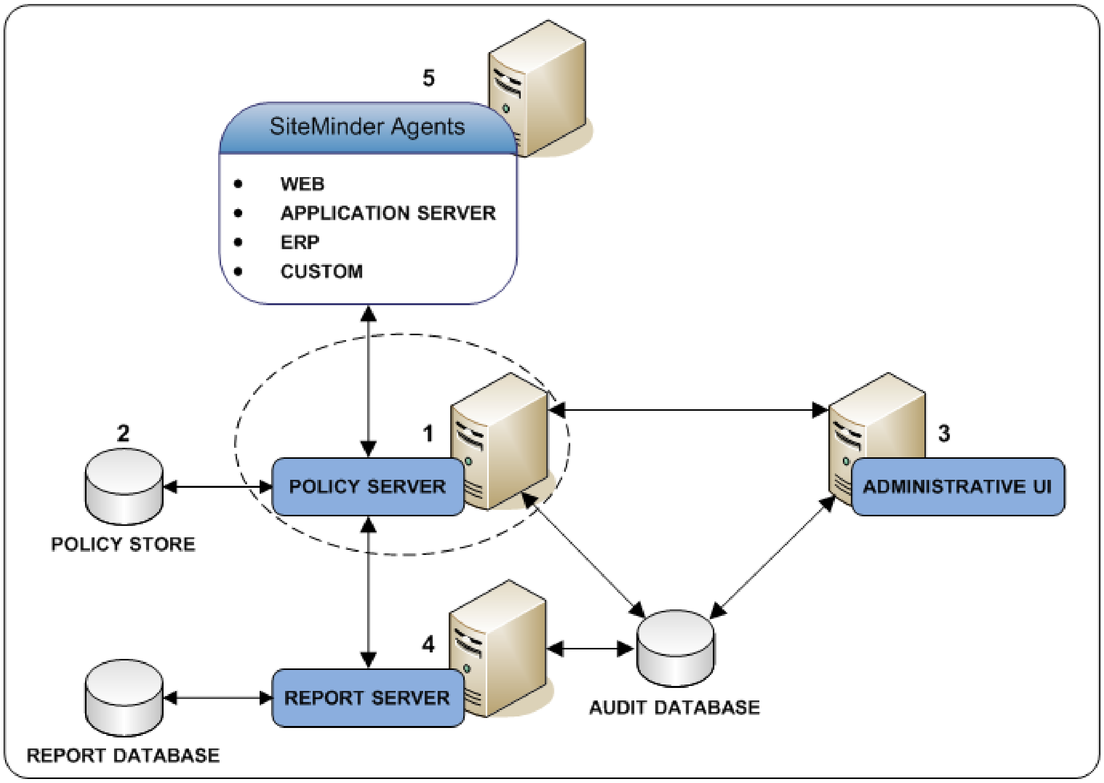
Chapter 5: Installing the Policy Server on UNIX Systems

Installation Road Map

The following diagram illustrates a sample CA SiteMinder® installation and lists the order in which you install and configure each component. Consider the following items:

- Confirm that the Policy Server host system meets the minimum system requirements. We recommend doing so before installing the Policy Server.
- A dotted line surrounds the Policy Server. Install this component now.

Figure 2: Installation Roadmap



More information:

Policy Server System Requirements (see page 19)

Solaris 10 Zone Support

A CA SiteMinder® Policy Server is supported in the following zones:

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

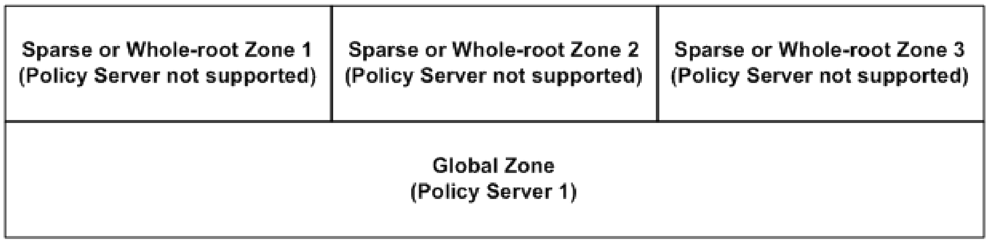
Consider the following scenarios when planning to run one or more Policy Servers in a Solaris 10 environment.

Global Zone Support

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

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

Example: Global zone support


Sparse or Whole-root Zone 1
(Policy Server not supported)
Sparse or Whole-root Zone 2
(Policy Server not supported)
Sparse or Whole-root Zone 3
(Policy Server not supported)
Global Zone
(Policy Server 1)

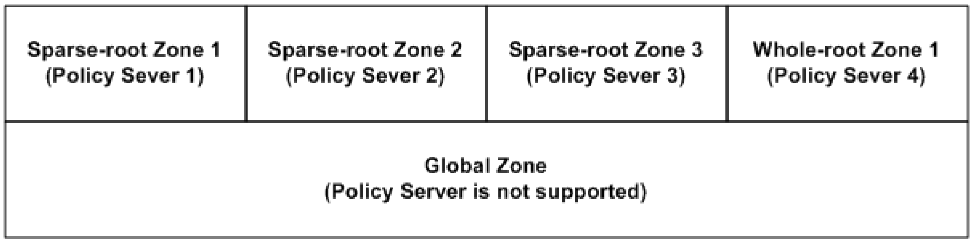
Note: Web Agents, however, may run concurrently in any zone.

Sparse-root Zone Support

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

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

Example: Sparse-root zone support



Sparse-root Zone 1
(Policy Sever 1)

Sparse-root Zone 2
(Policy Sever 2)

Sparse-root Zone 3
(Policy Sever 3)

Whole-root Zone 1
(Policy Sever 4)

Global Zone
(Policy Server is not supported)

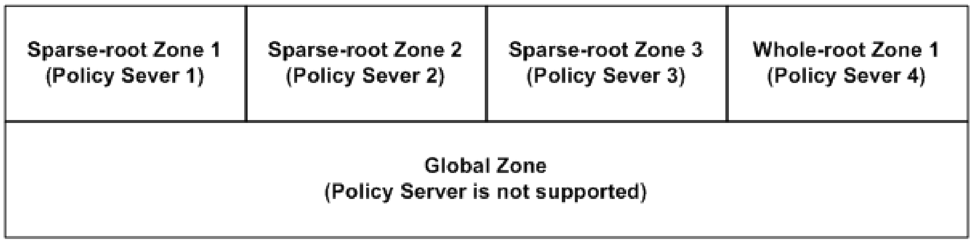
Note: Web Agents, however, may run concurrently in any zone.

Whole-root Zone Support

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

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

Example: Whole-root zone support



Sparse-root Zone 1
(Policy Sever 1)

Sparse-root Zone 2
(Policy Sever 2)

Sparse-root Zone 3
(Policy Sever 3)

Whole-root Zone 1
(Policy Sever 4)

Global Zone
(Policy Server is not supported)

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

How to Prepare for the Policy Server Installation

Before you install the Policy Server on a UNIX system, complete the following steps, if applicable:

1. Determine if the Policy Server host system meets the minimum operating system patch requirements. For more information, see the *Policy Server Release Notes*.
2. (Red Hat Linux) The Red Hat operating system relies on entropy for performance. Increase entropy before installing the component. Without sufficient entropy, the installation can take an exceedingly long time to complete. We recommend that you use the following command to set a symbolic link:

   ```
   mv /dev/random /dev/random.org
   ```

   ```
   ln –s /dev/urandom /dev/random
   ```
3. (Linux) Be sure that the required Linux libraries are installed to the Policy Server host system.
4. Create a New UNIX Account.
5. Modify the UNIX System Parameters.
6. Unset the Localization Variables.
7. Unset the LANG Environment Variable.

Required Linux Libraries

Certain library files are required for components operating on Linux operating environments. Failure to install the correct libraries can cause the following error:

```
java.lang.UnsatisfiedLinkError
```

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

Red Hat 5.x:

compat–gcc-34-c++-3.4.6-*patch_version*.I386

libstdc++-4.x.x-x.el5.i686.rpm

Red Hat 6.x:

libstdc++-4.x.x-x.el6.i686.rpm

Additionally, for Red Hat 6.x (64-bit):

Note: All the RPM packages that are required for 64-bit Red Hat 6.x are *32-bit* packages.

libXau-1.0.5-1.el6.i686.rpm

libxcb-1.5-1.el6.i686.rpm

compat-db42-4.2.52-15.el6.i686.rpm

compat-db43-4.3.29-15.el6.i686.rpm

libX11-1.3-2.el6.i686.rpm

libXrender-0.9.5-1.el6.i686.rpm

libexpat.so.1 (provided by expat-2.0.1-11.el6_2.i686.rpm)

libfreetype.so.6 (provided by freetype-2.3.11-6.el6_2.9.i686.rpm)

libfontconfig.so.1 (provided by fontconfig-2.8.0-3.el6.i686.rpm)

libICE-1.0.6-1.el6.i686.rpm

libuuid-2.17.2-12.7.el6.i686.rpm

libSM-1.1.0-7.1.el6.i686.rpm

libXext-1.1-3.el6.i686.rpm

compat-libstdc++-33-3.2.3-69.el6.i686.rpm

compat-db-4.6.21-15.el6.i686.rpm

libXi-1.3-3.el6.i686.rpm

libXtst-1.0.99.2-3.el6.i686.rpm

libXft-2.1.13-4.1.el6.i686.rpm

libXt-1.0.7-1.el6.i686.rpm

libXp-1.0.0-15.1.el6.i686.rpm

Korn Shell (ksh) Package Required on Linux

The ksh Korn shell is required during Policy Server installation and upgrade on Linux platforms. Verify that the appropriate version for your Linux environment is installed.

Red Hat 5.x 32-bit

ksh-20100621-12.el5.i386.rpm

Red Hat 5.x 64-bit

ksh-20100621-12.el5.x86_64.rpm

Red Hat 6.x 32-bit

ksh-20100621-16.el6.i686.rpm

Red Hat 6.x 64-bit

ksh-20100621-16.el6.x86_64.rpm

Create a New UNIX Account

Create a UNIX account with the default shell as ksh. Name the account as follows:

```
smuser
```

Important! Do not use the installer to configure the OneView Monitor UI on the following web servers:

- Oracle iPlanet
- Apache on Linux

The installer modifies the configuration files of the web server. The new UNIX account does not have the required root privileges.

After you install the Policy Server, use the Policy Server Configuration Wizard as root to configure the OneView Monitor UI.

Modify the UNIX System Parameters

When the Policy Server is placed under load, it opens a large number of sockets and files. If the default limit parameters are not adequate for the load, a large number of sockets and files can become a problem. Modify the default limit parameters to avoid associated problems.

To view the default limit parameters, type the following command in a shell window:

```
ulimit -a
```

The system displays a message similar to the following example:

```
$ ulimit -a

time(seconds)                               unlimited

file(blocks)                                unlimited

data(kbytes                                 2097148

stack(kbytes)                               8192

coredump(blocks)                            unlimited

nofiles(descriptor                          256
s)

vmemory(kbytes)                             unlimited
```

In the example, the nofiles parameter is set to 256. The parameter is the total number of files (sockets + files descriptors) that this shell and its descendants have been allocated. If this parameter is not set high enough, the Policy Server returns numerous socket errors. The most common socket error is 10024, or too many open files.

Increase the nofiles parameter value for proper Policy Server operation under load. You can change this value by running the following command:

```
ulimit -n
```

For example, to set the value to 1024, place the following command in the profile file of the smuser account:

```
ulimit -n 1024
```

The Policy Server is bound by the nofiles parameter in the smuser account ulimit for the number of connections to it.

Unset Localization Variables

The LC_* variables are sometimes set by default in the profile file of the smuser account. Use of the LC_* environment variables are not permitted. Unset them before installing the Policy Server.

To unset the LC_* environment variables, open the profile file of the smuser account and unset them.

Unset the LANG Environment Variable

The LANG environment variable is not permitted. Unset it before installing the Policy Server.

To unset the variable, add the unset LANG command to the profile file of the smuser account.

Before You Install the Policy Server

Consider the following items before installing the Policy Server:

- **Free space in /tmp**—The Policy Server installation requires 3 GB of free space in the /tmp directory.
- **System path length**—If the system path length exceeds 1024 characters, the Policy Server installation fails. The limitation applies to both included or excluded CA SiteMinder® added directories.

  Note: For best results, we recommend that you install CA SiteMinder® to a location such that the installation path does not exceed 700 characters.
- **Telnet or other terminal emulation software**—If you are going to install the Policy Server using Telnet or other terminal emulation software, complete the installation using a console window. If you install in GUI Mode, a Java exception occurs and the installer exits.
- **Exceed X-windows application**—Running the Policy Server installer or the Policy Server Configuration Wizard (ca-ps-config.bin) using an Exceed X-windows application can truncate text in the window. The limitation is due to unavailable fonts in Exceed and has no affect on the Policy Server installation or configuration.
- **Environment variables**—The Policy Server installation modifies environment variables.

How to Install the Policy Server

To install the Policy Server, complete the following steps:

1. Review the Policy Server component considerations.
2. Review the policy store considerations.
3. Review the FIPS considerations.
4. Gather information for the Policy Server installer.
5. Run the Policy Server installer.

6. (Linux) If Security–Enhanced Linux is enabled, add CA SiteMinder®–specific exceptions.

7. (Optional) If you configured SNMP, restart the SNMP daemon.

8. (Optional) If you do not use the Policy Server installer to configure a policy store, manually configure the policy store.

Policy Server Component Considerations

In addition to the Policy Server, the installer can install and configure the following components. Review the following items before installing the Policy Server:

- OneView Monitor UI

  The OneView Monitor enables the monitoring of CA SiteMinder® components.

  Note: To use the OneView Monitor, you must have the supported Java SDK and ServletExec/AS installed on the system.

- SNMP

  You must have the following items to enable SNMP support:

  - The password of the root user.
  - A native SunSolstice Master Agent.

- Policy store

  Note: The key store and certificate data store are automatically configured and collocated with the policy.

- Audit logs

  You can store audit logs in either a relational database or a text file. After you install the Policy Server, audit logging is set to a text file and not to ODBC by default.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

Policy Store Considerations

Consider the following items before running the Policy Server installer or the Policy Server Configuration wizard:

- The Policy Server installer and the Policy Server Configuration wizard can automatically configure one of the following stores as a policy store:

  - Microsoft Active Directory Lightweight Directory Services (AD LDS)

    Note: Be sure that you have met the prerequisites for configuring AD LDS as a policy store.

  - Oracle® Directory Enterprise Edition (formerly Sun Java™ System Directory Server)

    Important! The Policy Server installer and the Policy Server Configuration wizard cannot automatically configure a policy store that is being connected to using an SSL connection.

  - Microsoft SQL Server®
  - Oracle RDBMS

- (RDB policy store) The Policy Server installer or the Policy Server Configuration Wizard use specific database information to create the policy store data source. The Policy Server uses this data source to communicate with the policy store. Consider the following items:
  - The name of data source is CA CA SiteMinder® DSN.
  - The installer saves the data source to the system_odbc.ini file, which is located in *siteminder_home*/db.

    siteminder_home

    Specifies the Policy Server installation path.

- (RDB policy store) Verify that the database server that is to host the policy store is configured to store objects in UTF–8 form. This configuration avoids possible policy store corruption.
  - (Oracle) Be sure that the database is configured to store objects in UTF–8 form. Oracle supports unicode within many of their character sets. For more information about configuring your database to store objects in UTF–8 form, see your vendor–specific documentation.
  - (SQL Server) Be sure that the database is configured using the default collation (SQL_Latin1_General_CP1_CI_AS). Using a collation that is case–sensitive can result in unexpected behaviors. For more information about configuring your database to store objects using the default collation, see your vendor–specific documentation.
- The certificate data store is automatically collocated with the policy store.
- You manually configure any other supported directory server or relational database as a policy store after installing the Policy Server. Configuring a policy store manually is detailed in this document.

FIPS Considerations

The Policy Server uses certified Federal Information Processing Standard (FIPS) 140-2 compliant cryptographic libraries. FIPS is a US government computer security standard that is used to accredit cryptographic modules that meet the Advanced Encryption Standard (AES). The libraries provide a FIPS mode of operation when a CA SiteMinder® environment only uses FIPS-compliant algorithms to encrypt sensitive data.

You can install the Policy Server in one of the following FIPS modes of operation.

Note: The FIPS mode a Policy Server operates in is system-specific. For more information, see the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

- **FIPS-compatibility mode**—The default FIPS mode of operation during the installation is FIPS-compatibility mode. In FIPS-compatibility mode, the environment uses existing CA SiteMinder® algorithms to encrypt sensitive data and is compatible with previous versions CA SiteMinder®:
  - The use of FIPS-compliant algorithms in your environment is optional.
  - If your organization does not require the use of FIPS-compliant algorithms, install the Policy Server in FIPS-compatibility mode. No further configuration is required.
- **FIPS-migration mode**—FIPS-migration mode lets you transition an 12.52 environment running in FIPS-compatibility mode to FIPS-only mode.

  In FIPS-migration mode, the 12.52 Policy Server continues to use existing CA SiteMinder® encryption algorithms as you migrate the 12.52 environment to use only FIPS-compliant algorithms.

  Install the Policy Server in FIPS-migration mode if you are in the process of configuring the existing environment to use only FIPS-compliant algorithms.
- **FIPS-only mode**—In FIPS-only mode, the environment only uses FIPS-compliant algorithms to encrypt sensitive data.

  Install the Policy Server in FIPS-only mode if the existing environment is upgraded to 12.52 and the existing environment is configured to use only FIPS-compliant algorithms.

  Important! A 12.52 environment that is running in FIPS-only mode cannot operate with versions of CA SiteMinder® that do not also fully support FIPS (that is, versions before r12.0). This restriction applies to all agents, custom software using older versions of the Agent API, and custom software using PM APIs or any other API that the Policy Server exposes. Relink all such software with the 12.52 versions of the respective SDKs to achieve the required FIPS support.

Note: For more information about migrating an environment to use only FIPS-compliant algorithms, see the *Upgrade Guide*.

Gather Information for the Installer

The Policy Server installer requires specific information to install the Policy Server and any optional components.

Note: Installation worksheets are provided to help you gather and record information prior to installing or configuring Policy Server components using the Policy Server Installation Wizard or the Policy Server Configuration Wizard. You may want to print these worksheets and use them to record required information prior to running either wizard.

Required Information

Gather the following required information before running the Policy Server installer or the Configuration wizard.

- **JRE location**—Identify the folder in which the installer can locate the supported JRE. Verify that the JRE is set correctly in the PATH variable. If the JRE is not set correctly in the PATH variable, the installer cannot locate it.
- **Policy Server Installation location**—Determine where the installer must install the Policy Server.
- **Encryption key value**—Determine the encryption key value. An encryption key is a case-sensitive, alphanumeric key that secures the data sent between the Policy Server and the policy store. All Policy Servers that share a policy store are required to use the same encryption key. For stronger protection, define a long encryption key.

  Limits: 6 to 24 characters.
- **Advanced Authentication Server Encryption key value** - Determine the encryption key value. An encryption key is a case–sensitive, alphanumeric key that secures the data sent between the Policy Server and the advanced authentication server (running on the CA SiteMinder® SPS). The CA SiteMinder® SPS and all Policy Servers share the same key. For stronger protection, define a long encryption key.
  Limits: 6 to 24 characters.

Active Directory LDS Server Information

Gather the following required information to configure Microsoft Active Directory LDS as a policy store:

- **System IP address**—Identify the IP address of the directory server host system.
- **Port number—**Identify the port number on which the directory server is listening.
- **Root DN of the application partition**—Identify the root DN location of the application partition in the directory server where the policy store schema data must be installed.

  Example: dc=ca,dc=com

- **Administrator domain name**—Identify the full domain name, including the guid value, of the directory administrator.

  Example: CN=user1,CN=people,CN=Configuration,CN=*guid*

- **Administrator password**—Identify the password of the directory administrator.

- **Alternate user account**—By default, CA SiteMinder® uses the administrator account to communicate with the directory server. However, you can use a different user account to administer the policy store. Identify the complete administrator DN and password to configure CA SiteMinder® to use an alternative user account to administer the policy store.

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

- **CA SiteMinder® superuser password**—The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

  ```
  siteminder
  ```

  Limits:

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

  Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

Oracle Directory Server Information

Gather the following required information to configure Oracle Directory Server to function as a policy store:

- **System IP address**—Determine the IP address of the Oracle Directory Server host system.

- **Directory instance port number**—Determine the port number for the Oracle Directory Server instance.

  Default: 389

- **Root DN—**Identify the root DN of the Oracle Directory Server.

  Example: o=yourorg.com

- **Administrator account**—Identify the user name (Bind DN) for the LDAP administrator account.

  Example: cn=Directory Manager

- **Administrator password**—Identify the password for the Oracle Directory Server administrator.
- **Alternate LDAP administrator**—By default, CA SiteMinder® uses the LDAP administrator account to communicate with the LDAP server. However, you can use a different LDAP user account to administer the policy store. Identify the complete administrator DN and password to configure CA SiteMinder® in this way.

  Note: This user must have the necessary permissions to modify attributes and change passwords.
- **CA SiteMinder® superuser password**—The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

  ```
  siteminder
  ```

  Limits:

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

  Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

Microsoft SQL Server Information

To configure Microsoft SQL Server as a policy store, gather the following required information:

Database server name

Identify the IP address or name of the database host system.

Note: For more information about IPv6 support, see the CA SiteMinder® Platform Support Matrix.

Database name

Identify the named instance or the name of the database that is to function as the policy store.

Database port

Identify the port on which the database is listening.

Database administrator user name and password

Identify the name and password of an administrator account with permission to do the following operations:

- Create schema
- Create, read, modify, and delete objects.

Note: If the CA SiteMinder® schema is already present in the database, the wizard does not require the credentials of a database administrator with **create** permission. For more information, see Configure a SQL Server Policy Store (see page 285).

CA SiteMinder® superuser password

The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

```
siteminder
```

Limits:

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

Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

Oracle RDBMS Information

Gather the following required information to configure Oracle RDBMS as a policy store.

Database server name

Identify the IP address or the name of the database host system.

Note: For more information about IPv6 support, see the CA SiteMinder® Platform Support Matrix.

Database service name

Identify the service name of the database that is to function as the policy store.

Database port

Identify the port on which the database is listening.

Database administrator user name

Identify the name of an administrator account with permission to do the following operations:

- Create schema
- Create, read, modify, and delete objects.

Database administrator password

Identify the password of the administrator account.

CA SiteMinder® superuser password

The default CA SiteMinder® superuser account has maximum permissions. Determine the password for the default superuser account. The name of the default account is:

```
siteminder
```

Limits:

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

Note: We recommend that you do not use the default superuser for day-to-day operations. Rather, use the default superuser to access the Administrative UI for the first–time and then create an administrator with superuser permissions.

OneView Monitor Information

You only have to gather OneView Monitor information if you plan on configuring the OneView Monitor.

Gather the following required information to configure the OneView Monitor. You can use the OneView Monitor Information Worksheet to record your values.

- **JDK path**—Identify the path to the required JDK version.
- **ServletExec installation directory**—Identify ServletExec installation directory.

  Example: /usr/local/NewAtlanta/ServletExecAS
- **ServletExec port number**—Determine the port number for the ServletExec instance.
- **Sun Java System administrator directory**—Determine the following information:
  - The installed location of the Sun Java System.
  - The installed location of the Sun Java System Web servers.

  Example: /*sunjavasystem_home*/*location*

sunjavasystem home

Specifies the installed location of the Sun Java System.

location

Specifies the installed location of the Sun Java System Web servers.

- **Multiple ServletExec instances**—If you have multiple ServletExec instances, determine the instance to which you want to configure the OneView Monitor GUI.

Install the Policy Server in GUI Mode

Install the Policy Server using the installation media on the Technical Support site. Consider the following items:

- Be sure that you have executable permissions. To add executable permissions to the installation media, run the following command:

  ```
  chmod +x installation_media
  ```

  installation_media

  Specifies the Policy Server installer executable.

- If you execute the Policy Server installer across different subnets, it can crash. Install the Policy Server directly on the host system to avoid the problem.

Follow these steps:

1. Exit all foreground applications.
2. Open a shell and navigate to the installation media.
3. Enter the following command:

   ```
   ./ca-ps-12.5-cr-unix_version
   ```

   cr

   Specifies the cumulative release number. The base r12.5 release does not include a cumulative release number.

   unix_version

   Specifies the UNIX version: **sol** or **linux**.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.

4. Use the system and component information you have gathered to install the Policy Server.

Consider the following items when running the installer:

- If you are installing the Policy Server for the first–time on this system, do not configure the OneView Monitor UI. The installer modifies the configuration files of the web server that is to host the UI. The smuser account does not have the required root privileges. After you install the Policy Server, use the Policy Server Configuration Wizard as root to configure the OneView Monitor UI.
- The installer prompts you to select a FIPS mode of operation. For more information about which FIPS mode to select, see FIPS Considerations (see page 67).
- If you are configuring a policy store manually, clear the Policy Store option when selecting components. For more information about which stores can be automatically configured as a policy store, see Policy Store Considerations (see page 65).
- If you are initializing a policy store, you are prompted to enter a password for the default CA SiteMinder® user account. The default account name is:

  ```
  siteminder
  ```

- You are prompted to install the default certificate authority (CA) certificates to the certificate data store. You can add additional certificates and private keys to the certificate data store after installation.
- If you are using IPv6 addresses, surround entries with brackets.

  Example:

  ```
  [2001:db8::1428:57ab]
  ```

- If you cut and paste path information into the wizard, enter a character to enable the Next button.

5. Review the installation settings and click Install.

   The Policy Server and all selected components are installed and configured.

   Note: The installation can take several minutes.

6. Click Done.

   The installer closes.

7. (Optional) If you did not use the installer to configure a policy store, manually configure the policy.

Note: If you experience problems during the installation, you can locate the installation log file and the policy store details file in *siteminder_home/*siteminder/install_config_info.

siteminder_home

Specifies the Policy Server installation path.

More information:

Troubleshoot the Policy Server Installation (see page 77)

Install the Policy Server in Console Mode

Install the Policy Server using the installation media on the Technical Support site. Consider the following items:

- Be sure that you have executable permissions. To add executable permissions to the installation media, run the following command:

  ```
  chmod +x installation_media
  ```

  installation_media

  Specifies the Policy Server installer executable.

- If you execute the Policy Server installer across different subnets, it can crash. Install the Policy Server directly on the host system to avoid the problem.

Follow these steps:

1. Exit all applications that are running.
2. Open a shell and navigate to the installation media.
3. Run the following command:

   ```
   ./ca-ps-12.5-cr-unix_version -i console
   ```

   cr

   Specifies the cumulative release number. The base r12.5 release does not include a cumulative release number.

   unix_version

   Specifies the UNIX version: **sol** or **linux**.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.

4. Use the system and component information you have gathered to install the Policy Server.

   Consider the following items when entering information:

   - If you are installing the Policy Server for the first–time on this system, do not configure the OneView Monitor UI. The installer modifies the configuration files of the web server that is to host the UI. The smuser account does not have the required root privileges. After you install the Policy Server, use the Policy Server Configuration Wizard as root to configure the OneView Monitor UI.

- The installer prompts you to select a FIPS mode of operation. For more information about which FIPS mode to select, see FIPS Considerations (see page 67).
- The installer prompts you to select components you want to configure. Separate entries with commas (,). To select none of the features, enter only a comma.
- If you are configuring a policy store manually, do not select Policy Store. For more information about which stores can be automatically configured as a policy store, see Policy Store Considerations (see page 65).
- If you are initializing a policy store, you are prompted to enter a password for the default CA SiteMinder® user account. The default account name is:

  ```
  siteminder
  ```

- You are prompted to install the default certificate authority (CA) certificates to the certificate data store. You can add additional certificates and private keys to the certificate data store after installation.
- If you are using IPv6 addresses, surround entries with brackets.

  Example:

  ```
  [2001:db8::1428:57ab]
  ```

- Only initialize the policy store when configuring a new policy store instance.

5. Review the installation settings and press Enter.

   The Policy Server and all selected components are installed and configured.

   Note: The installation can take several minutes.

6. Press Enter.

   The installer closes.

7. (Optional) If you did not use the installer to configure a policy store, manually configure the policy.

Note: If you experience problems during the installation, you can locate the installation log file and the policy store details file in *siteminder_home/*siteminder/install_config_info.

siteminder_home

Specifies the Policy Server installation path.

More information:

Troubleshoot the Policy Server Installation (see page 77)

Add Exceptions to Security–Enhanced Linux

If Security–Enhanced Linux is enabled on the Policy Server host system, add CA SiteMinder®–exceptions to the environment. Adding the exceptions prevents Security–Enhanced Linux text relocation denials.

Follow these steps:

1. Log in to the Policy Sever host system.
2. Open a shell and run the following command:

   ```
   chcon -t textrel_shlib_t /siteminder_home/lib/*
   ```

   siteminder_home

   Specifies the Policy Server installation path.

3. Run the following command:

   ```
   chcon -t textrel_shlib_t /JDK_home/lib/i386/*
   ```

   JDK_home

   Specifies the required JDK installation path.

4. Run the following command:

   ```
   chcon -t textrel_shlib_t /JDK_home/lib/i386/server/*
   ```

   JDK_home

   Specifies the required JDK installation path.

   CA SiteMinder®–specific exceptions have been added.

Troubleshoot the Policy Server Installation

Use the following files to troubleshoot the Policy Server installation:

- CA_SiteMinder_Policy_Server_*release*_InstallLog.log

  The installation log contains a summary section that lists the number of successes, warnings, non–fatal errors, and errors that occurred during the installation. Individual installation actions are listed with the respective status.

  release

  Specifies the Policy Server release.

  Location: *siteminder_home*\siteminder\install_config_info

- ca-ps-details.log

  The policy store log details the policy store status.

  Location: *siteminder_home*\siteminder\install_config_info

- smps.log

  The smps.log is created when you start the Policy Server. This log contains the following line if the Policy Server installed successfully:

  ```
  [Info] Journaling thread started, will delete commands older than 60 minutes.
  ```

  Location: *siteminder_home*\siteminder\log

  siteminder_home

  Specifies the Policy Server installation path.

Restart the SNMP Daemon

You only have to restart the SNMP daemon if you configured SNMP during the Policy Server installation.

To restart the SNMP daemon

1. Enter S76snmpdx stop in /etc/rc3.d.

   The SNMP daemon stops.

2. Enter S76snmpdx start in /etc/rc3.d.

   The SNMP daemon starts.

Configure a Policy Store

If you did not use the Policy Server installer to configure a policy store automatically, manually configure a supported LDAP directory server or relational database as a policy store.

Configure Auto Startup

You configure auto startup to ensure that the Policy Server restarts automatically when the UNIX system is rebooted.

Follow these steps:

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

   Example: /export/ca/siteminder

2. Change the directory to the siteminder installation directory.

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

   Note: Do not use the suse command.

   You are prompted for a password.

4. Enter the root password and press ENTER.

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

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

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

Unattended Policy Server Installation

After the Policy Server is manually installed on one machine, you can reinstall it or install it on a separate machine using an unattended installation mode. An unattended installation lets you install or uninstall the Policy Server without any user interaction.

The installer provides a ca-ps-installer.properties template file that lets you define installation variables. The default parameters, passwords, and paths in this file reflect the information you entered during the initial Policy Server installation. In this file, you can either store encrypted or plain text passwords. If you are using encrypted passwords, for example, a shared secret and CA SiteMinder® Super User, you must use the same ones that you entered during the initial installation since they are encrypted in the file and cannot be modified. However, you can use plain text passwords by modifying the file.

More information:

How to Run an Unattended Policy Server Install (see page 499)

Policy Server Configuration Wizard

Use the Policy Server Configuration wizard to configure or reconfigure the following components after installing the Policy Server:

- A policy store.
- SNMP support.
- The OneView Monitor UI.

Note: You cannot change the Policy Server FIPS–mode of operation using the Policy Server Configuration Wizard. For more information about changing the Policy Server FIPS–mode of operation, see the *CA SiteMinder® Upgrade Guide*.

Important! If you configured an Oracle iPlanet web server instance for the OneView Monitor UI or SNMP, do not use the wizard to configure new instances. Configuring new web server instances can cause the existing web server instance to fail.

More information:

Policy Store Considerations (see page 33)

How to use the Configuration Wizard

Complete the following procedures to use the Policy Server Configuration wizard:

1. Review the configuration wizard requirements.
2. Review the policy store considerations (see page 65).
3. If you are configuring the OneView Monitor UI or one of the following stores as a policy store, gather information for the wizard (see page 46):
   - Active Directory LDS
   - Oracle Directory Server
   - SQL Server
   - Oracle RDBMS
4. Run the wizard.

Configuration Wizard Requirements

Meet the following requirements before using the Policy Server Configuration wizard:

- The Policy Server Configuration wizard requires at least 150 MB of free space in /tmp
- Run the wizard as a UNIX user with local administrator privileges.
- If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.

Run the Configuration Wizard in GUI Mode

You run the Policy Server Configuration wizard to configure individual Policy Server components.

Follow these steps:

1. Exit all running applications.
2. Execute the following script in a ksh shell from the CA SiteMinder® installation directory:

   ```
   . ./ca_ps_env.ksh
   ```

   Note: Be sure that there is a space between the periods (. .).
3. Open a shell and run the following command:

   ```
   ./ca-ps-config.bin gui
   ```

   The Configuration wizard starts.
4. Use the system and component information you have gathered to configure a policy store and individual components.

   Note: Only initialize the policy store instance to configure a new policy store instance.
5. Review the installation settings and click Install.

   The wizard configures the selected components to work with the Policy Server.

   Note: The installation can take several minutes.
6. Click Done.

   The selected components are configured.

Note: If you experience problems, you can locate the installation log file and the policy store details file in *siteminder_home/*siteminder/install_config_info.

siteminder_home

Specifies the Policy Server installation path.

More information:

Troubleshoot the Policy Server Installation (see page 77)

Run the Configuration Wizard in Console Mode

You run the Policy Server Configuration wizard to configure individual Policy Server components.

Follow these steps:

1. Exit all running applications.
2. Execute the following script in a ksh shell from the CA SiteMinder® installation directory:

   ```
   . ./ca_ps_env.ksh
   ```

   Note: Be sure that there is a space between the periods (. .).
3. Open a shell and run the following command:

   ```
   ./ca-ps-config.bin -i console
   ```

   The Configuration wizard starts.
4. Use the system and component information you have gathered to configure a policy store and individual components.

   Note: Only initialize the policy store instance to configure a new policy store instance.
5. Review the installation settings and click Enter.

   The wizard configures the selected components to work with the Policy Server.

   Note: The installation can take several minutes.
6. Press Enter

   The installer closes. The selected components are configured.

Note: If you experience problems, you can locate the installation log file and the policy store details file in *siteminder_home/*siteminder/install_config_info.

siteminder_home

Specifies the Policy Server installation path.

More information:

Troubleshoot the Policy Server Installation (see page 77)

How to Uninstall the Policy Server

Complete the following procedures to uninstall the Policy Server:

1. Shut down all instances of the Policy Server Management Console.

   Note: More information on shutting down the Policy Server Management Console exists in the *Policy Administration Guide*.

2. Set the JRE in the path variable.
3. Remove Policy Server references from agent host files.
4. Stop all CA SiteMinder® processes.
5. Uninstall the Policy Server.
6. Remove CA SiteMinder® references from IWS.
7. Remove CA SiteMinder® references from ServletExec/AS.
8. Remove leftover items.

Remove Policy Server References from Agent Host Files

You remove the Policy Server reference from the SmHost.conf file to prevent unexpected results from the Web Agent once the Policy Server is uninstalled.

To remove the Policy Server reference

1. Navigate to *web_agent_home*/config.

   web_agent_home

   Specifies the installation directory of the Web Agent.

2. Open the SmHost.conf file in a text editor.
3. Delete the line that begins with "policyserver=".

   Note: This line contains the IP address and port numbers for the Policy Server you are uninstalling.

4. Save SmHost.conf.

   The SmHost.conf file no longer references the Policy Server you are uninstalling.

Set the JRE in the PATH Variable

You set the JRE in the PATH variable when uninstalling the Policy Server, Web Agent, SDK, or documentation to prevent the uninstallation program from stopping and issuing error messages.

To set the JRE in the PATH variable

1. Run the following command:

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

   JRE

   Specifies the location of the JRE.

2. Run the following command:

   ```
   export PATH
   ```

   The JRE is set in the PATH variable.

Stop all CA SiteMinder® Processes

You stop all CA SiteMinder® processes to ensure that Policy Server files are safely removed.

To stop all CA SiteMinder® processes

1. Log into the UNIX system with the smuser account.
2. Run stop-all, which is located in the /siteminder directory.

   All CA SiteMinder® processes stop.

Uninstall the Policy Server

You uninstall the Policy Server when it is no longer required on the system.

Note: Do not manually remove the installation directories to uninstall this component. Execute the uninstall shell script. If you only remove the installation directories, related registries can be left behind. If you try to re–install this component on this host system, the entries can prevent a successful installation.

Follow these steps:

1. Log in to the Policy Server host system as the user who installed the Policy Server.

   Note: The user who installed the Policy Server should have the required CA SiteMinder® scripts sourced. If the CA SiteMinder® scripts are not sourced at login, or you logged in as another user, source the following scripts:

   ```
   smprofile.ksh
   ca_ps_env.ksh
   ```

2. Change to the following directory in a console window:

   ```
   siteminder_home/siteminder/install_config_info/ca-ps-uninstall
   ```

   siteminder_home

   Specifies the Policy Server installation path.

3. Run the following command:

   ```
   ./uninstall
   ```

   The uninstallation program appears.

4. Press Enter.

   A status indicator displays progress.

5. Change the directory to the one above the CA SiteMinder® installation directory.

   Example: If the CA SiteMinder® installation directory is /export/smuser/ca/siteminder, go to:

   ```
   /export/smuser/ca
   ```

6. Enter the following command and press Enter.

   ```
   $ rm -rf siteminder
   ```

   The CA SiteMinder® installation directory is removed.

7. Open the following file from the HOME directory:

   ```
   .profile
   ```

8. Locate and delete the line that contains smprofile.ksh.

   Example:

   ```
   ./export/smuser/siteminder/smprofile.ksh
   ```

9. Save the file.

   The Policy Server is uninstalled.

Remove CA SiteMinder® References from IWS

You manually remove CA SiteMinder® references from IWS after uninstalling the Policy Server. CA SiteMinder® references are left in the obj.conf file and the magnus.conf file.

To remove CA SiteMinder® references from IWS

1. Log into an account that has privileges to access and modify the Web server's configuration.
2. Go to the following at the Solaris command line.

   ```
   <SunJavaSystem_home>/https-<hostname>/config
   ```

   The obj.conf and magnus.conf files appear in the config folder.
3. Open obj.conf and remove the following lines:

   ```
   NameTrans fn="assign-name" from="/servlet/*" name="<ServletExec_instance name>"
   NameTrans fn="assign-name" from="*.jsp*" name="<ServletExec_instance name>"
   NameTrans fn="pfx2dir" from="/siteminder monitor"
   dir="/<siteminder_installation>/monitor"
   NameTrans fn="pfx2dir" from="/siteminder cgi"
   dir="/<siteminder_installation>/admin" name="cgi"
   NameTrans fn="pfx2dir" from="/siteminder"
   dir="/<siteminder_installation>/admin"
   NameTrans fn="pfx2dir" from="/netegrity_docs"
   dir="/netegrity/netegrity_documents"
   <Object name="<ServletExec_instance name>">
   Service fn="ServletExecService" group="<ServletExec_instance name>"
   </Object>
   ```
4. Save and close the obj.conf file.
5. Open magnus.conf and remove the following lines:

   ```
   Init fn="init-cgi" SM_ADM_UDP_PORT="44444" SM_ADM_TCP_PORT="44444"
   Init fn="load-modules"
   shlib="/<Servlet_Exec_Install>/bin/ServletExec_Adapter.so"
   funcs="ServletExecInit,ServletExecService"
   Init fn="ServletExecInit" <ServletExec_instance
   name>.instances="<IP_Address>:<port_number>"
   ```
6. Save and close magnus.conf.
7. Restart the Web server.

   CA SiteMinder® references are removed from IWS.

   The CA SiteMinder® references no longer appear in IWS.

Remove CA SiteMinder® References from StartServletExec

To remove references from StartServletExec

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

3. Remove the following lines from the StartServletExec script:

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

   siteminder_home

   Specifies the Policy Server installation path.

4. Save and close the StartServletExec script.

5. Restart ServletExec.

   The uninstallation is complete.

Remove Leftover Items

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

You can locate this file at one of the following:

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

Chapter 6: Configuring LDAP Directory Servers to Store CA SiteMinder® Data

LDAP Directory Servers as a Policy or Key Store

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

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

- Microsoft Active Directory Lightweight Directory Services (AD LDS)
- Oracle Directory Server (formerly Sun Java System Directory Server)

If you do not use the Policy Server to configure a policy store automatically, you can manually configure a policy store after installing the Policy Server. Additionally, after you install the Policy Server, you can use the Policy Server Management Console to point the Policy Server to an existing policy store.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

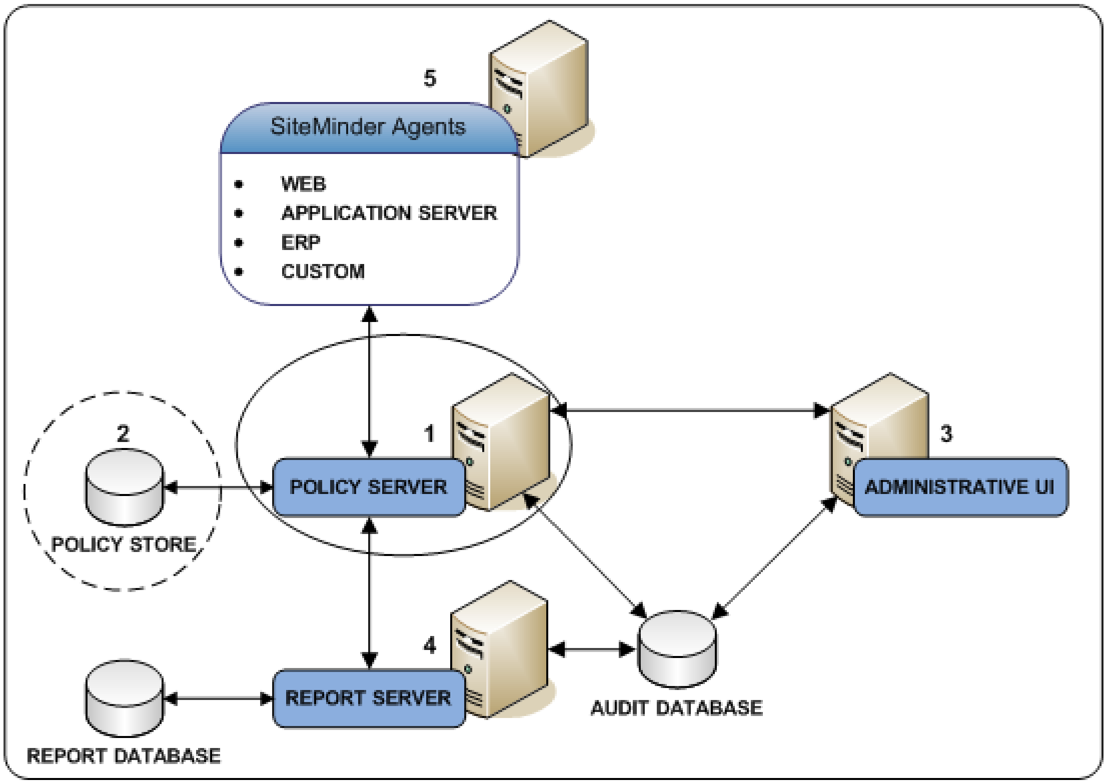
Installation Road Map

The following diagram illustrates a sample CA SiteMinder® installation and lists the order in which you install and configure each component.

- A solid line surrounds the Policy Server, which is required before configuring a policy store. If a Policy Server is not part of your environment, install it before continuing.
- The dotted line surrounds the policy store. Configure this component now.

The following figure depicts a single policy/key store instance. Although not illustrated, your environment can use separate instances for individual policy and key stores.

Equation 1: Installation Roadmap



Important Considerations

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

Default Policy Store Objects Consideration

When you configure a policy store, the following default policy store object files are available:

- smpolicy.xml
- smpolicy-secure.xml

Consider the following items when choosing a file to:

- Both files contain the default objects that the policy store requires.
  - If you use the Policy Server Configuration Wizard to configure the policy store automatically, the wizard only uses smpolicy.xml.
  - If you want to use smpolicy–secure.xml, configure the policy store manually.
- Both files provide default security settings. These settings are available in the default Agent Configuration Object (ACO) templates that are available in the Administrative UI.
- The smpolicy-secure file provides more restrictive default security settings.
- Choosing smpolicy does not limit you from using the more restrictive default security settings. You can modify the default ACO settings using the Administrative UI.

  Note: For more information, see the *Policy Server Configuration Guide*.

The following table summarizes the security settings for both files:

Parameter Name	smpolicy Values	smpolicy–secure Values
BadCssChars	No value	<, >, ', ;,), (, &, +, %00
BadQueryChars	No value	<, >, ', ;,), (, &, +, %00
BadUrlChars	//, ./, /., /*, *., ~, \, %00-%1f, %7f-%ff, %25	smpolicy.smdif values plus: <, >, ', ;,), (, &, +
EnableCookieProvider	Yes	No
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	All smpolicy values.
LimitCookieProvider	No	Yes
ValidTargetDomain	This file does not include this parameter.	This parameter does not have a default value. Provide a valid redirection domain. Example: validtargetdomain=".example.com"

CA Directory as a Policy Store

CA Directory can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key store.

Gather Directory Server Information

Configuring a CA Directory as a policy store requires specific directory server information.

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

Gather the following information before configuring the policy store. You can use the Policy Store Worksheets to record your values.

- **Host information—**Determine the fully qualified host name or the IP address of the system on which CA Directory is running.
- **DSA port number**—Determine the port on which the DSA is to listen.
- **Base DN**—Determine the distinguished name of the node in the LDAP tree in which policy store objects are to be defined.
- **Administrative DN**—Determine the LDAP user name of the account that CA SiteMinder® is to use manage objects in the DSA.
- **Administrative password**—Determine the password for the administrative user.

How to Configure the Policy Store

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

1. Create a DSA for the policy store (see page 93).
2. Create the policy store schema (see page 93).
3. Open the DSA (see page 95).
4. Create the base tree structure for policy store data (see page 96).
5. Create a superuser administrator for the DSA (see page 97).
6. Point the Policy Server to the policy store (see page 97).
7. Set the CA SiteMinder® superuser password (see page 98).
8. Verify the CA Directory cache configuration (see page 99).
9. Import the policy store data definitions (see page 100).

10. Import the default policy store objects (see page 100).
11. Prepare for the Administrative UI registration (see page 102).

Create a DSA for the Policy Store

Create the DSA by running the following command:

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

DSA_Name

Specifies the name of the DSA.

port

Specifies the port on which the DSA is to listen.

o=*DSA_Name*,c=*country_code*

Specifies the DSA prefix.

Example: "o=psdsa,c=US"

The dxnewdsa utility starts the new DSA.

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

```
dxserver start DSA_Name
```

Create the Policy Store Schema

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

Important! By default, CA Directory configuration files are read–only. Any CA Directory files that you are instructed to modify, must be updated for write permission. Once the files are updated, you can revert the permission to read–only. Also, all default.xxx files provided by CA Directory are overwritten during a CA Directory upgrade. Use caution when modifying any read-only files.

To create the Policy Store schema

1. Copy the following files into the CA Directory *DXHOME*\config\schema directory:
   - netegrity.dxc
   - etrust.dxc

   DXHOME

   Specifies the Directory Server installation path.

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

siteminder_home

Specifies the Policy Server installation path.

- Windows %*DXHOME*%
- Unix/Linux: $*DXHOME*

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

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

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

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

   ```
   #CA Schema

   source "netegrity.dxc";

   source "etrust.dxc";
   ```

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

   DSA_Name

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

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

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

   - **r12**

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

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

   - **r12 SP1 or later**

     ```
     # cache configuration
     set ignore-name-bindings = true;
     ```

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

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

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

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

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

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

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

8. Save the DXC file.

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

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

   DSA_Name

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

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

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

    ```
    dxserver stop DSA_Name
    dxserver start DSA_Name
    ```

    DSA_Name

    Specifies the name of the DSA.

    The policy store schema is created.

Open the DSA

You create a view into the directory server to manage objects.

Follow these steps:

1. Be sure that the database is configured for an anonymous login.
2. Launch the JXplorer GUI.

3. Select the connect icon.

   Connection settings appear.

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

   host_name_or_IP_address

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

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

   port_number

   Specifies the port on which the DSA is listening.

6. Enter o=*DSA_Name*,c=*country_code* in the Base DN field.

   Example: o=psdsa,c=US

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

   A view into DSA appears.

Create the Base Tree Structure for Policy Store Data

You create a base tree structure to hold policy store data. You use the JXplorer GUI to create the organizational units.

To create the base tree structure for policy store data

1. Select the root element of your DSA.
2. Create an organizational unit under the root element called:

   Netegrity

3. Create an organizational unit (root element) under Netegrity called:

   SiteMinder

4. Create an organizational unit (root element) under CA SiteMinder® called:

   PolicySvr4

5. Create an organizational unit (root element) under PolicySvr4 called:

   XPS

   The base tree structure is created.

Create a Superuser Administrator for the DSA

You only have to create a superuser administrator if you do not have an administrator account that CA SiteMinder® can use to access the DSA. The Policy Server requires this information to connect to the policy store.

Follow these steps:

1. Use the JXplorer GUI to access the DSA.
2. Create an administrator that CA SiteMinder® can use to connect to the policy store.

   Note: Create the user with the following object type:

   ```
   inetOrgPerson
   ```

3. Note the administrator DN and password. You use the credentials when pointing the Policy Server to the policy store.

Example:

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

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

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

   ```
   Policy Store
   ```

4. Select the following value from the Storage list:

   LDAP

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

- Confirm Password
- Root DN

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

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

   `Key Store`

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    `Use Policy Store database`

11. Click OK.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

`siteminder`

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

   – The password must contain at least six (6) characters and cannot exceed 24 characters.

   – The password cannot include an ampersand (&) or an asterisk (*).

   – If the password contains a space, enclose the passphrase with quotation marks.

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Verify the CA Directory Cache Configuration

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

Note: By default, the DxConsole is only accessible from localhost. For more about using the set dsa command to let the DxConsole accept a connection from a remote system, see the *Directory Configuration Guide*.

Follow these steps:

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

   ```
   telnet DSA_Host DXconsole_Port
   ```

   DSA_Host

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

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

   DXConsole_Port

   Specifies the port on which the DXconsole is listening. This value appears in the console-port parameter of the following file:

   DXHOME\config\knowledge\DSA_Name.dxc

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

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

   The DSA Management Console appears.

2. Enter the following command:

   ```
   get cache;
   ```

   The DSA Management Console displays the current DSA DXcache settings and specifies the directory caching status.

3. Enter the following command:

   ```
   logout;
   ```

   Closes the DXconsole and returns to the system prompt.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

   Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

CA Directory as a Session Store

You can configure CA Directory as a session store.

Note: For more information about supported versions, see the 12.52 CA SiteMinder® Platform Support Matrix.

How to Configure the Session Store

Complete the following tasks to configure CA Directory as a session store:

1. Obtain the session store schema files.
2. Create a DSA for the session store.
3. Add a session store administrative user and root DN.
4. Create the session store schema.
5. Point the Policy Server to the session store.

Obtain the Session Store Schema Files

All required session store schema files are installed with the Policy Server. Contact your CA SiteMinder® Administrator and request the following file:

netegrity.dxc

Creates the DSA session store schema. The schema lets the DSA store and retrieve the session information of CA SiteMinder® users.

The files reside in *siteminder_home*\eTrust.

siteminder_home

Specifies the Policy Server installation path.

Create a DSA for the Session Store

Create a DSA and dedicate its use to the session store only. A dedicated DSA helps to maximize session store performance.

Follow these steps:

1. Log in to the CA Directory host system.
2. Create a data DSA by running the following command:

   ```
   dxnewdsa dsa_name port prefix
   ```

   dsa_name

   Specifies the name of the session store DSA.

   port

   Specifies the port on which the session store must listen for requests.

   prefix

   Specifies the namespace prefix. Use LDAP syntax to specify the prefix.

Example: Create a data DSA for the session store.

```
dxnewdsa smsessionstore 1234 o=forwardinc,c=us
```

Note: Forward, Inc. is a fictitious company name that is used strictly for instructional purposes only and is not meant to reference an existing company.

Add a Session Store Administrative User and Root DN

The Policy Server requires:

- The complete distinguished name (DN) and password of a user in the DSA. The Policy Server uses these credentials to manage the session store.
- A root DN to which session information can be written.

Follow these steps:

1. Access the DSA using anonymous authentication with *one* of the following methods:
   - Use the JXplorer tool.
   - Use the CA Directory command-line interface.
2. Create a user that CA SiteMinder® can use to manage the session store.
   - Be sure to create the user with only the following OBJECT CLASS:

     inetOrgPerson
   - Note the credentials. The credentials are required to point the Policy Server to the session store DSA.
3. Disconnect from JXplorer.
4. Start JXplorer.
5. Log in to the DSA using the complete DN of the administrative user you created to verify that you can access the DSA.

   Example: cn=admin,o=forwardinc,c=us
6. Manually create an organizational unit that serves as the root DN of the session store.

   Example: ou=sessionstore
7. Disconnect from JXplorer.

Note: We recommend that you disable the anonymous authentication to prevent unauthorized access to the session store.

Command-line Procedure for CA Directory

Create the Session Store Schema

The DSA requires the schema to store and retrieve the session information of CA SiteMinder® users.

Follow these steps:

1. Log in to the CA Directory host system.
2. Stop the DSA using the following command:

   ```
   dxserver stop DSA_Name
   ```

3. Add the CA SiteMinder® session store schema file (netegrity.dxc) in to *DXHOME*\config\schema.
4. Navigate to *DXHOME*\config\schema.
5. Create the session store schema by copying the default schema file of the DSA (default.dxg), removing the read–only attribute, and renaming it.

   Example: Copy default.dxg and rename the copy to smsession.dxg.

6. Edit the session store schema file:
   a. Add the following lines to the bottom of the file:

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

   b. Save the file.
   c. Apply the read–only attribute.
7. Navigate to *DXHOME*\dxserver\config\limits.
8. Create a session store limits file by copying the default limits file (default.dxc), removing the read–only attribute, and renaming it.

   Example: Copy default.dxc and rename the copy smsession.dxc.

9. Edit the session store default limits file:
   a. Edit the max–local–ops attribute to match the following value:

      ```
      set max-op–size = 1000;
      ```

      The attribute is in the size limits section and represents a high limit. The session store is not expected to return more than 1,000 objects per search query.

   b. Save the file.
   c. Apply the read–only attribute.

10. Navigate to *DXHOME*\config\servers and open the session store initialization file (*DSA_name*.dxi).

    DSA_name

    Specifies the name of the session store DSA.

11. Edit the session store initialization file:

    a. Edit the schema reference from default.dxg to the session store schema file.

       The reference is in the schema section.

       Example: Change default.dxg to smsession.dxg.

    b. Edit the service limits reference from default.dxc to the session store limits file.

       The reference is in the service limits section.

       Example: Change default.dxc to smsession.dxc.

    c. Edit the set–cache index attribute to match the following setting:

       ```
       set cache-index–all–except = smVariableValue,smsessionblob;
       ```

       Note: Be sure that the cache index all attribute is set before the following attribute:

       ```
       set lookup-cache = true;
       ```

       The attribute is in the grid configuration section.

    d. (Optional) Compress the following attribute to store more session objects in memory:

       smVariableValue

    e. (Optional) Disable transaction logging to improve performance.

       Important! Consider the effects disabling transaction logging has on data recovery. For more information, see the CA Directory documentation.

12. Start the DSA using the following command:

    ```
    dxserver start DSA_Name
    ```

    The session store schema is created.

Point the Policy Server to the Session Store

Point the Policy Server to the session store DSA to let CA SiteMinder® manage the session store.

Follow these steps:

1. Open the Policy Server Management Console.

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

2. Click the Data tab.
3. Select Session Store from the Database list.
4. Select CA Directory from the Storage list.
5. Select the Session Store Enabled option.
6. Under LDAP Session Store section:
   a. Enter the IP address and port of the session store DSA.
   b. Enter the root DN of the session store DSA.

      Example: ou=sessionstore,o=fowardinc,c=us

   c. Enter the complete DN of an administrative user in the DSA.

      Example: cn=admin,o=forwardinc,c=us

   d. Enter the password of the administrative user.
7. Click Test LDAP Connection to verify the connection.
8. Click OK.

   CA SiteMinder® is configured to manage the session store.

Active Directory as a Policy Store

Active Directory can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key store.

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

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 CA SiteMinder® data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Store

To configure an Active Directory directory server as a policy store, complete the following procedures:

1. (Optional) If applicable, use the vendor–specific software to create an LDAP Directory Server instance.
2. (Optional) If applicable, use the vendor–specific software to create a user with the following privileges:

   - create
   - read
   - modify
   - delete

   Create this user in the LDAP tree underneath the policy store root object.
3. Point the Policy Server to the directory server.
4. Create the policy store schema.
5. Set the CA SiteMinder® superuser password.
6. Import the policy store data definitions.
7. Import the default policy store objects.
8. Restart the Policy Server.
9. Prepare for the Administrative UI registration.

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut with Administrator permissions. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.
2. Click the Data tab.
3. Select the following value from the Database list:

   `Policy Store`
4. Select the following value from the Storage list:

   LDAP

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

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

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

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

   ```
   Key Store
   ```

9. Select the following value from the Storage list:

   ```
   LDAP
   ```

10. Select the following option:

    ```
    Use Policy Store database
    ```

11. Click OK.

Create the Policy Store Schema

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

Important! The Active Directory schema is owned by the root domain. All schema changes must be made on the root domain controller that holds the Schema Master using an account with SchemaAdmins permissions. Schema changes cannot be made from child domains (replicas).

Follow these steps:

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

   ```
   smldapsetup ldgen -ffile_name
   ```

   file_name

   Specifies the name of the LDIF file you are creating.

   An LDIF file with the CA SiteMinder® schema is created.

2. Run the following command:

   ```
   smldapsetup ldmod -ffile_name
   ```

   file_name

   Specifies the name of the LDIF you created.

   The utility imports the policy store schema.

3. Navigate to *policy_server_home*\xps\db and open the following file:

   ```
   ActiveDirectory.ldif
   ```

4. Manually replace each instance of <RootDN> with the DN that represents the policy store schema location, not the policy store object location.

   Example: If the following root DN represents the policy store object:

   ```
   ou=policystore,dc=domain,dc=com
   ```

   Replace each instance of <RootDN> with the following DN:

   ```
   dc=domain,dc=com
   ```

5. Run the following command:

   ```
   smldapsetup ldmod
   -fpolicy_server_home\xps\db\ActiveDirectory.ldif
   ```

   policy_server_home

   Specifies the Policy Server installation path.

   The policy store schema is extended. You have created the policy store schema.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

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

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

   Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

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

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Support for Active Directory ObjectCategory Indexing Attribute

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

Enable or Disable ObjectCategory Attribute Support

On Windows Systems:

To enable or disable ObjectCategory attribute support

1. Launch the Windows Registry Editor.
2. Locate the key HKLM\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\DS\LDAP Provider.
   a. To enable support, set the EnableObjectCategory value to 1.
   b. To disable support, set the EnableObjectCategory value to 0.

      Note: The default value is 0.

On UNIX systems:

To enable or disable ObjectCategory attribute support

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

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\Current Version\Ds\LDAPProvider.

   a. To enable support, set the EnableObjectCategory value to 1.

   b. To disable support, set the EnableObjectCategory value to 0.

   Note: The default value is 0.

Domino Directory Server as a Policy Store

Domino Directory Server can function as a policy store. A single directory server instance can function as a:

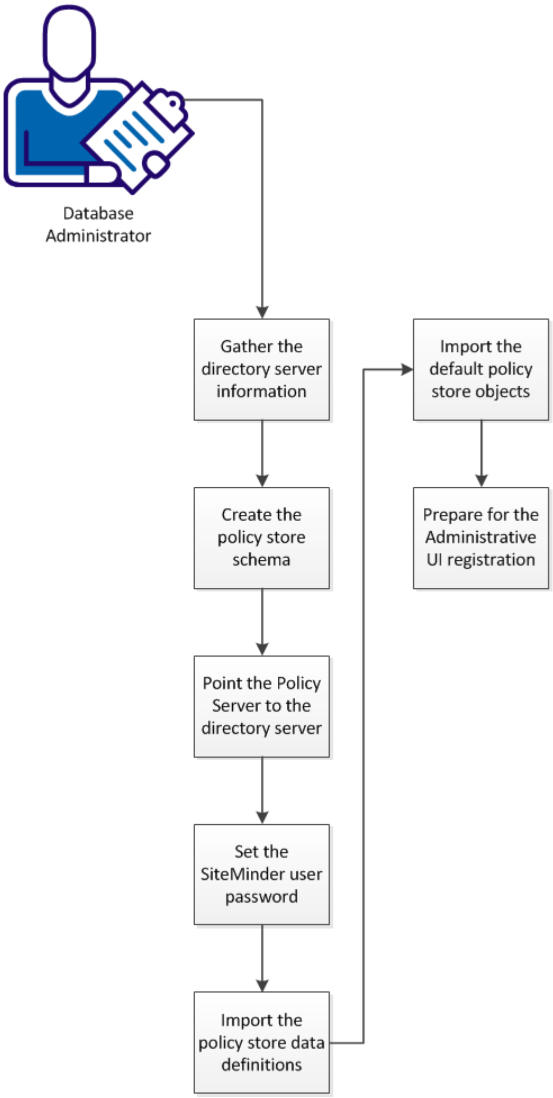
- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key store.

How to Configure a Domino Directory Server as a Policy Store

This scenario describes how a database administrator configures a Domino directory server version 8.5 as a CA SiteMinder® policy store.

This configuration process contains several separate procedures. The following illustration describes the workflow:


Database Administrator
Gather the directory server information
Create the policy store schema
Point the Policy Server to the directory server
Set the SiteMinder user password
Import the policy store data definitions
Import the default policy store objects
Prepare for the Administrative UI registration

To configure a Domino directory server version 8.5 as a CA SiteMinder® policy store, Follow these steps:

1. Gather the directory server information (see page 110).
2. Create the policy store schema (see page 123).
3. Point the Policy Server to the directory server (see page 97).
4. Set the CA SiteMinder® superuser password (see page 98).
5. Import the policy store data definitions (see page 100).
6. Import the default policy store objects (see page 100).
7. Prepare for the Administrative UI registration (see page 102).

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 CA SiteMinder® data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

Create the Policy Store Schema

You create the policy store schema so that the Domino directory server can operate as a policy store.

Follow these steps:

1. Stop the domino directory service.
2. Create a backup copy of the following file in your Domino directory server:

   domino_home\data\schema.nsf

3. Locate the following file on your Policy Server:

   policy_server_home\db\tier2\IBM_Lotous_Domino_DirectoryServer\schema.nsf

4. Copy the file from Step 3 to the following folder of your Domino directory server:

   domino_home\data

5. Start the Domino directory service.
6. Open the schema.nsf file on your Domino directory server.
7. Verify that all the xps and CA SiteMinder® objects and attributes exist.
8. Use an LDAP browser to connect to the Domino LDAP directory.
9. Create the following base DN for CA SiteMinder®:

   ```
   Netegrity/SiteMinder/PolicySvr4
   ```

10. Restart the Domino directory service.
11. Open the service in console mode.
12. Update the indices in the directory with the following command:

    ```
    load updall -r
    ```

13. Restart the domino directory service.

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

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

   `Policy Store`

4. Select the following value from the Storage list:

   LDAP

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

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

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

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

   `Key Store`

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    `Use Policy Store database`

11. Click OK.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

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

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

IBM Tivoli Directory Server as a Policy Store

IBM Tivoli Directory Server can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key 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 CA SiteMinder® data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Store

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

1. Verify that you have gathered the required information.
2. Create a directory entry and root nodes.
3. Point the Policy Server to the policy store.
4. Create the policy store schema.
5. Set the CA SiteMinder® superuser password.
6. Import the policy store data definitions.
7. Import the default policy store objects.
8. Restart the Policy Server.
9. Prepare for the Administrative UI registration.

Create a Directory Entry and Root Nodes

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

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

Follow these steps:

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

   Example:

   ```
   ou=Nete
   ```

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

   Example:

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

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

2. Click the Data tab.

3. Select the following value from the Database list:

   ```
   Policy Store
   ```

4. Select the following value from the Storage list:

   LDAP

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

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

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

6. Click Apply.

7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.

8. Select the following value from the Database list:

   ```
   Key Store
   ```

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    ```
    Use Policy Store database
    ```

11. Click OK.

Create the Policy Store Schema

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

To create the policy store schema

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

   policy_server_home

   Specifies the Policy Server installation path.

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

   release

   Specifies the CA SiteMinder® release.

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

   IBMDirectoryServer.ldif

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

   The policy store schema is created.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

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

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

   Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

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

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Microsoft Active Directory LDS as a Policy Store

Microsoft Active Directory LDS can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key store.

Note: You can use the Policy Server Configuration wizard to configure this type of LDAP directory server as a policy store automatically.

Active Directory LDS Prerequisite

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

Follow these steps:

1. Open the ADSI Edit console.

2. Navigate to the following in the configuration partition:

   ```
   cn=directory service, cn=windows nt,
   cn=services, cn=configuration, cn={guid}
   ```

3. Locate the msDS-Other-Settings attribute.

4. Add the following new value to the msDS-Other-Settings attribute:

   ```
   ADAMAllowADAMSecurityPrincipalsInConfigPartition=1
   ```

5. In the configuration and policy store application partitions:

   a. Navigate to CN=Administrators, CN=Roles.

   b. Open the properties of CN=Administrators.

   c. Edit the member attribute.

   d. Click Add DN and paste the full DN of the user you created in the configuration partition.

   e. Go to the properties of the user you created and verify the value for the following object:

      ```
      msDS-UserAccountDisabled
      ```

      Be sure that the value is set false.

   The administrative user has rights over the configuration partition and all application partitions, including the policy store partition.

Gather Directory Server Information

Configuring Active Directory LDS as a policy store requires specific directory server information. Gather the following information before configuring the policy store.

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

- **Host information**—Determine the fully qualified name or the IP address of the directory server host system.
- **Port information**—Determine if the directory server is listening on a non–standard port. If you do not provide port information, the CA SiteMinder® utilities you use to configure the policy store default to port 389 (non-SSL) and 636 (SSL).
- **Administrator DN**—Determine the full domain name, including the guid value, of the directory server administrator.

  Example: CN=user1,CN=People,CN=Configuration,CN,{guid}
- **Administrator password**—Determine the password for the directory server administrator.

- **Root DN of the application partition**—Identify the root DN location of the application partition in the directory server where the policy store schema data must be installed.
- (Optional) **SSL client certificate**—If the directory connection is made over SSL, determine the path of the directory that contains the SSL client certificate database.

How to Configure the Policy Store

To configure Active Directory LDS as a policy store, complete the following procedures:

1. Be sure that you have met the Active Directory LDS prerequisite.
2. Be sure that you have gathered the required information.
3. Point the Policy Server to the directory server.
4. Create the policy store schema.
5. Set the CA SiteMinder® superuser password.
6. Import the policy store data definitions.
7. Import the default CA SiteMinder® objects.
8. Restart the Policy Server.
9. Prepare for the Administrative UI registration.

Point the Policy Server to the Policy Store

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

Note: The Policy Server can bind to an AD LDS policy store using a proxy object. A proxy object is created on AD LDS and is associated with an Active Directory account through the Security Identifier of the account. For more information about binding to an AD LDS instance using a proxy object, see the Microsoft documentation. If you configure a Policy Server connection using a proxy object and plan on using password policies, configure AD LDS for SSL.

Follow these steps:

1. Open the Policy Server Management Console.

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

2. Click the Data tab.

3. Select the following value from the Database list:

   `Policy Store`

4. Select the following value from the Storage list:

   LDAP

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

   ■ LDAP IP Address

   ■ Admin Username

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

   ■ Password

   ■ Confirm Password

   ■ Root DN

     Specifies the existing root DN location of the application partition in the AD LDS server. The existing root DN location is where the policy store schema is imported.

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

6. Click Apply.

7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.

8. Select the following value from the Database list:

   `Key Store`

9. Select the following option:

   `Use Policy Store database`

10. Click OK.

Create the Policy Store Schema

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

Follow these steps:

1. Run the following command:

   ```
   smldapsetup ldgen -ffile_name
   ```

   file_name

   Specifies the name of the LDIF file you are creating.

   An LDIF file with the CA SiteMinder® schema is created.

2. Run the following command:

   ```
   smldapsetup ldmod -ffile_name
   ```

   file_name

   Specifies the name of the LDIF you created.

   smldapsetup imports the policy store schema.

3. Navigate to *siteminder_home*\xps\db and open the following file:

   ```
   ADLDS.ldif
   ```

   siteminder_home

   Specifies the Policy Server installation path.

4. Replace each instance of {guid} with the actual value of guid in braces and save the file.

   Example: {CF151EA3-53A0-44A4-B4AC-DA0EBB1FF200}

5. Run the following command:

   ```
   smldapsetup ldmod -fsiteminder_home\xps\db\ADLDS.ldif
   ```

   The policy store schema is extended. You have created the policy store schema.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

   – The password must contain at least six (6) characters and cannot exceed 24 characters.

   – The password cannot include an ampersand (&) or an asterisk (*).

   – If the password contains a space, enclose the passphrase with quotation marks.

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

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

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Novell eDirectory as a Policy Store

Novell eDirectory can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key store.

Be sure that you have the following installed before beginning:

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

Limitations of Policy Store Objects in Novell eDirectory

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

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

  A Novell eDirectory DN cannot exceed 256 characters. Some CA SiteMinder® objects can reach 241 characters. If your root DN is longer than 15 characters, some objects can exceed the 256–byte limit.
- When the policy store resides in Novell eDirectory, policy store objects cannot have names longer than 64 characters. eDirectory does not allow an attribute to be set to a value longer than 64. The limitation affects Certificate Maps particularly because they routinely have long names by design.
- The Policy Server does not support LDAP referrals for policy stores residing in Novell eDirectory.

Gather Directory Server Information

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

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

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Store

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

1. Edit the policy store schema files.
2. Point the Policy Server to the policy store.
3. Set the CA SiteMinder® super user password.

   Note: You do not have to complete this procedure if you already have a CA SiteMinder® super user password.
4. Create the policy store schema.
5. Import the policy store data definitions.
6. Import the default policy store objects.
7. Refresh the LDAP Server.
8. Restart the Policy Server.
9. Prepare for the Administrative UI Registration.

Edit the Policy Store Schema Files

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

Follow these steps:

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

   policy_server_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   ldapsearch -hhost -pport -bbasedn -ssub -Dadmin_DN -wAdminPWd
   objectclass=ncpServer dn
   ```

   -h*host*

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

   -p*port*

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

   -b*basedn*

   Specifies the base DN for the search.

   -D*admin_dn*

   Specifies the DN of the administrator account that can bind to the directory server.

   -w*admin_pw*

   Specifies the password for the administrator account.

   Example:

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

   The Novell server DN opens.

3. Navigate to *policy_server_home*\novell.

4. Open the Novell policy store schema file.

5. Manually edit the policy store schema file by replacing every <ncpserver> 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 <ncpserver> with cn=servername,o=servercontainer.

6. Save and close the policy store schema file.

7. Navigate to *policy_server_home*\xps\db.

8. Open the following Novell policy store schema file:

   `Novell.ldif`

9. Manually edit the policy store schema file by replacing every <ncpserver> 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 <ncpserver> with cn=servername,o=servercontainer.

The Novell policy store schema files contain your Novell server DN information.

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

2. Click the Data tab.

3. Select the following value from the Database list:

   `Policy Store`

4. Select the following value from the Storage list:

   LDAP

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

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

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

6. Click Apply.

7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.

8. Select the following value from the Database list:

   ```
   Key Store
   ```

9. Select the following value from the Storage list:

   ```
   LDAP
   ```

10. Select the following option:

    ```
    Use Policy Store database
    ```

11. Click OK.

Create the Policy Store Schema

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

Follow these steps:

1. Run the following command:

   ```
   smldapsetup ldmod -v

   -fpolicy_server_home\novell\Novell_Add_release.ldif
   ```

   -fpolicy_server_home

   Specifies the Policy Server installation path.

   -v

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

   release

   Specifies the CA SiteMinder® release.

2. Run the following command:

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

   The policy store schema is created.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

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

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

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.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.

4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.

5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

   The Policy Server stops as indicated by the red stoplight.

3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

OpenLDAP as a Policy Store

OpenLDAP can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key 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 CA SiteMinder® data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Store

Complete the following procedures to configure an OpenLDAP directory server as a policy store:

1. Configure the sldap configuration file.
2. Create the database.
3. Point the Policy Server to the directory server.
4. Set the CA SiteMinder® superuser password.
5. Import the policy store data definitions.
6. Import the default policy store objects.
7. Prepare for the Administrative UI registration.

How to Configure the Slapd Configuration File

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

1. Specify the CA SiteMinder® schema files.
2. Specify policy store indexing.
3. Enable user authentication.
4. Specify database directives.
5. Support Client-Side Sorting
6. Test the configuration file.
7. Restart the OpenLDAP server.

Specify the SiteMinder Schema Files

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

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to *siteminder_home*/db/tier2/OpenLDAP and copy the following files to the schema folder in the OpenLDAP installation directory:

   - openldap_attribute.schema
   - openldap_object.schema

   siteminder_home

   Specifies the Policy Server installation path.

3. Navigate to *siteminder_home*/xps/db and copy the following files to the schema folder in the OpenLDAP installation directory:

   - openldap_attribute_XPS.schema
   - openldap_object_XPS.schema

4. Type the following entries 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 in /usr/local/etc/openldap and that the schema files are located in the schema subdirectory.

   The CA SiteMinder® schema files are specified.

Specify Policy Store Indexing

Specify indexing in the slapd.conf file to use OpenLDAP as a policy store.

Follow these steps:

1. Stop the slapd instance.
2. Open the slapd.conf file with a text editor.
3. Locate the following lines:

   ```
   # Indices to maintain
   index   objectClass     eq
   ```

4. Insert a new line in the file, and then add the following lines:

   ```
   index smAdminOID4 pres,eq
   index smAuthDirOID4 pres,eq
   index smAzDirOID4 pres,eq
   index smcertmapOID4 pres,eq
   index smIsRadius4 pres,eq
   index smIsAffiliate4 pres,eq
   index smParentRealmOID4 pres,eq
   index smPasswordPolicyOID4 pres,eq
   index smAgentGroupOID4 pres,eq
   index smKeyManagementOID4 pres,eq
   index smAgentOID4 pres,eq
   index smAgentKeyOID4 pres,eq
   index smRootConfigOID4 pres,eq
   index smAGAgents4 pres,eq
   index smDomainAdminOIDs4 pres,eq
   index smDomainOID4 pres,eq
   index smvariableoid5 pres,eq
   index smNestedVariableOIDs5 pres,eq
   index smvariabletypeoid5 pres,eq
   index smActiveExprOID5 pres,eq
   index smDomainUDs4 pres,eq
   index smVariableOIDs5 pres,eq
   index smusractiveexproid5 pres,eq
   index smPropertyOID5 pres,eq
   index smPropertySectionOID5 pres,eq
   index smPropertyCollectionOID5 pres,eq
   index smFilterClass4 pres,eq
   index smTaggedStringOID5 pres,eq
   index smNoMatch5 pres,eq
   index smTrustedHostOID5 pres,eq
   index smIs4xTrustedHost5 pres,eq
   index smDomainMode5 pres,eq
   # index smImsEnvironmentOIDs5 pres,eq
   index smSecretRolloverEnabled6 pres,eq
   index smSecretGenTime6 pres,eq
   ```

```
index smSecretUsedTime6 pres,eq
index smSharedSecretPolicyOID6 pres,eq
index smFilterPath4 pres,eq
index smPolicyLinkOID4 pres,eq
index smIPAddress4 pres,eq
index smRealmOID4 pres,eq
index smSelfRegOID4 pres,eq
index smAzUserDirOID4 pres,eq
index smResourceType4  pres,eq
index smResponseAttrOID4 pres,eq
index smResponseGroupOID4  pres,eq
index smResponseOID4     pres,eq
index smRGResponses4 pres,eq
index smRGRules4     pres,eq
index smRuleGroupOID4 pres,eq
index smRuleOID4   pres,eq
index smSchemeOID4 pres,eq
index smisTemplate4  pres,eq
index smisUsedbyAdmin4 pres,eq
index smSchemeType4   pres,eq
index smUserDirectoryOID4 pres,eq
index smODBCQueryOID4 pres,eq
index smUserPolicyOID4 pres,eq
index smAgentTypeAttrOID4 pres,eq
index smAgentTypeOID4 pres,eq
index smAgentTyperfcid4 pres,eq
index smAgentTypeType4 pres,eq
index smAgentCommandOID4 pres,eq
index smTimeStamp4     pres,eq
index smServerCommandOID4 pres,eq
index smAuthAzMapOID4 pres,eq
index xpsParameter pres,eq
index xpsValue  pres,eq
index xpsNumber pres,eq
index xpsCategory pres,eq
index xpsGUID pres,eq
index xpsSortKey pres,eq
index xpsIndexedObject pres,eq
```

5. Save the file and close the text editor.

6. Run the following command:

   ```
   slapindex -f slapd.conf
   ```

7. Restart the slapd instance.

   The policy store indexing for OpenLDAP is specified.

Enable User Authentication

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

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

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

Specify Database Directives

The slapd configuration file requires values for additional database directives.

To specify the directives, edit the following:

database

Specify any supported backend type.

Example: bdb

suffix

Specify the database suffix.

Example: dc=example,dc=com

rootdn

Specify the DN of root.

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

rootpw

Specify the password to root.

directory

Specify the path of the database directory.

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

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

Support Client-Side Sorting

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

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

- Enable reading of the Root DSE.

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

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

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

- Allow a simple V2 bind.

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

To support client-side sorting

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

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

   ACL

   Specifies an access control list or list of permissions.

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

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

   ```
   sizelimit 500
   ```

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

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

   ```
   allow bind_v2
   ```

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

Test the Configuration File

Testing the configuration file ensures that it is correctly formatted.

To test the configuration file

1. Change the directory to the OpenLDAP server directory.

2. Run the following command:

   ```
   ./slapd
   ```

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

3. Run the following command:

   ```
    ./slapd -Tt
   ```

   The slapd configuration file is tested.

Restart the OpenLDAP Server

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

To restart the directory server

1. Stop the directory server using the following command:

   ```
   kill -INT 'cat path_of_var/run_directory/slapd.pid`
   ```

   path_of_var/run_directory

   Specifies the path of the database directory.

   Example: kill -INT `cat /usr/local/var/run/slapd.pid`

2. Start the directory server using the following command:

   ```
   ./slapd
   ```

How to Create the Database

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

1. Create the base tree structure.

2. Add entries.

Create the Base Tree Structure

You can create a base tree structure to store policy store objects.

Specify the following entry under the root DN:

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

The base tree structure is created.

Add Entries

Add entries to the directory server so that CA SiteMinder® has the necessary organization and organizational role information.

To add database entries

1. Create an LDIF file.

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

   ```
   # CA, example.com
   dn: ou=Netegrity,dc= example,dc=com
   ou: CA
   objectClass: organizationalUnit
   objectClass: top


   # SiteMinder, CA, example.com
   dn: ou=SiteMinder,ou=CA,dc= example,dc=com
   ou: SiteMinder
   objectClass: organizationalUnit
   objectClass: top


   # PolicySvr4, SiteMinder, CA, example.com
   dn: ou=PolicySvr4,ou=SiteMinder,ou=CA,dc= example,dc=com
   ou: PolicySvr4
   objectClass: organizationalUnit
   objectClass: top


   # XPS, policysvr4, siteminder, ca, example.com
   dn: ou=XPS,ou=policysvr4,ou=siteminder,ou=ca,dc= example,dc=com
   ou: XPS
   objectClass: organizationalUnit
   objectClass: top
   ```

2. Use the following command to add the entries.

   ```
   ldapadd -f <file_name.ldif> -D "cn=Manager,dc=example,dc=com"

   -w<password>
   ```

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

2. Click the Data tab.

3. Select the following value from the Database list:

   `Policy Store`

4. Select the following value from the Storage list:

   LDAP

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

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

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

6. Click Apply.

7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.

8. Select the following value from the Database list:

   `Key Store`

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    `Use Policy Store database`

11. Click OK.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

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

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

   passphrase

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

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

   -adminui–setup

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

   -t *timeout*

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

   Unit of measurement: minutes

   Default: 240 (4 hours)

   Minimum Limit: 15

   Maximum Limit: 1440 (24 hours)

   -r *retries*

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

   Default: 1

   Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Oracle Directory Server as a Policy Store

Oracle Directory Server (formerly Sun Java System Directory Server) can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key store.

Note: You can use the Policy Server Configuration wizard to configure this type of LDAP directory server as a policy store automatically.

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 CA SiteMinder® data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Store

To configure Oracle Directory Sever Enterprise Edition (formerly Sun Directory Server Enterprise Edition) as a policy store, complete the following procedures:

1. (Optional) If applicable, use the vendor–specific software to create an LDAP directory server instance.
2. (Optional) If applicable, use the vendor–specific software to create an administrative user with the following privileges:
   - create
   - read
   - modify
   - delete

   Create this user in the LDAP tree underneath the policy store root object.
3. Review the Oracle Directory Server considerations.
4. Point the Policy Server to the directory server.
5. Create the policy store schema.
6. Set the CA SiteMinder® superuser password.
7. Import the policy store data definitions.
8. Import the default CA SiteMinder® objects.
9. Restart the Policy Server.
10. Prepare for the Administrative UI registration.

Oracle Directory Server Enterprise Edition Considerations

If you are using Oracle Directory Server Enterprise Edition as a policy store, consider the following.

smldapsetup and Oracle Directory Enterprise Edition

The smldapsetup utility creates the ou=Netegrity, *root* sub suffix and PolicySvr4 database.

root

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

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

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

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

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

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

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

Replicate an Oracle Directory Server Enterprise Edition Policy Store

CA SiteMinder® 12.52 creates a UserRoot and a PolicySvr4 database. The PolicySvr4 database has suffix mappings pointing to it. To replicate this policy store, set up a replication agreement for the PolicySvr4 database directory.

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

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

To replicate CA SiteMinder® indexes

1. Generate the CA SiteMinder® indexes:

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

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

2. Set up the indexes on a replica server:

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

   host

   Specifies the replica host.

   replicaport

   Specifies the replica port number.

   AdminDN

   Specifies the replica administrator DN.

   Example: cn=directory manager

   AdminPW

   Specifies the replica administrator password.

   The CA SiteMinder® indexes are replicated.

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

2. Click the Data tab.

3. Select the following value from the Database list:

   ```
   Policy Store
   ```

4. Select the following value from the Storage list:

   LDAP

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

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

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

6. Click Apply.

7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.

8. Select the following value from the Database list:

   `Key Store`

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    `Use Policy Store database`

11. Click OK.

Create the Policy Store Schema

You create the policy store schema so the directory server can function as a policy store and store CA SiteMinder® objects. Use this procedure for the following directory server products:

- Oracle 10g, 11g (32-bit)
- Sun Java System 6.1, 7.0

Perform the following prerequisites:

- Create an LDAP instance.
- Open the SiteMinder Management console, click the Data tab, and then enter the policy store and key store information for your LDAP instance.

Follow these steps:

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

   ```
   smldapsetup ldgen -ffile_name
   ```

   file_name

   Specifies the name of the LDIF file you are creating.

   An LDIF file with the CA SiteMinder® schema is created.

2. Run the following command:

   ```
   smldapsetup ldmod -ffile_name
   ```

   file_name

   Specifies the name of the LDIF you created.

3. Run the following command:

   ```
   smldapsetup ldmod -fpolicy_server_home\xps\db\OracleDirectoryServer.ldif
   ```

   policy_server_home

   Specifies the Policy Server Installation path.

4. Have the administrator of your directory server run the following command:

   ```
   dsconf reindex -h localhost -p port_number -e "ou=Netegrity,root_dn"
   ```

5. Edit the following ldif file:

   ```
   policy_server_home/xps/db/OracleDirectoryServerBrowse.ldif
   ```

6. Replace the Root_DN shown in the following line:

   ```
   vlvBase: ou=xps,ou=PolicySvr4,ou=siteminder,ou=netegrity,Root_DN
   ```

   ...with the base dn of your policy store, as shown in the following line:

   ```
   vlvBase:ou=xps,ou=PolicySvr4,ou=siteminder,ou=netegrity,base_dn_of_your_p
   olicy_store
   ```

7. Run the following command:

   ```
   smldapsetup ldmod -fOracleDirectoryServerBrowse.ldif -v
   ```

8. Stop the database and re-index the vlv indexes with the following commands:

   ```
   dsadm stop Instance_Path
   ```

   ```
   dsadm reindex -bl -t "Sort xpsSortKey" Instance_Path policysvr4
   ```

   ```
   dsadm reindex -bl -t "Sort modifyTimestamp" Instance_Path policysvr4
   ```

9. Start the database with the following command:

   ```
   dsadm start Instance_Path
   ```

   The policy store schema is extended. You have created the policy store schema.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

   – The password must contain at least six (6) characters and cannot exceed 24 characters.

   – The password cannot include an ampersand (&) or an asterisk (*).

   – If the password contains a space, enclose the passphrase with quotation marks.

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:

   – To import smpolicy.xml, run the following command:

   ```
   XPSImport smpolicy.xml -npass
   ```

   – To import smpolicy–secure.xml, run the following command:

   ```
   XPSImport smpolicy–secure.xml -npass
   ```

   npass

   Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

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

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Oracle Internet Directory as a Policy Store

Oracle Internet Directory (OID) can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key 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 CA SiteMinder® data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Store

Complete the following procedures to configure OID as a policy store:

1. Index a required attribute.
2. Configure a domain in Oracle Internet Directory.
3. Point the Policy Server to the directory server.
4. Create the policy store schema.
5. Set the CA SiteMinder® superuser password.

6. Import the policy store data definitions.
7. Import the default policy store objects.
8. Restart the Policy Server.
9. Prepare for the Administrative UI registration.

Index a Required Attribute

Indexing the following attribute prevents an error from occurring when you import the default policy store objects:
`modifyTimestamp`

Follow these steps:

1. Log in to the Oracle Internet Directory host system.
2. Use the Oracle catalog command line tool to run the following command:

   ```
   oracle_home/ldap/bin/catalog connect=conn_str add=TRUE
   attribute=modifyTimestamp
   ```

   oracle_home

   Specifies the Oracle Internet Directory installation path.

   conn_str

   Specifies the directory database connect string. If you have configured a tnsnames.ora file, then enter the net service name specified in the file.

   The attribute is indexed.

Note: For more information about the catalog command line tool, see the Oracle documentation.

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 Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

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

   ```
   Policy Store
   ```

4. Select the following value from the Storage list:

   LDAP

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

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

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

   ```
   Key Store
   ```

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    ```
    Use Policy Store database
    ```

11. Click OK.

Create the Policy Store Schema

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

Follow these steps:

1. Run the following command:

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

   -f*file_name*

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

2. Run the following command:

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

   -f*file_name*

   Specifies the name of the schema file that you created.

3. Run the following command:

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

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

   -h*host*

   Specifies the IP address of the LDAP directory server.

   Example: 123.123.12.12

   -p*port*

   Specifies the port number of the LDAP directory server.

   Example: 3500

   -d*AdminDN*

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

   -w*AdminPW*

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

-c

Specifies continuous mode (do not stop on errors).

-f*siteminder_home*

Specifies the Policy Server installation path.

-Z

(Optional) Specifies an SSL-encrypted connection.

-P cert

(Optional) Specifies the path of the SSL client certificate database file (cert8.db).

Example:

If cert8.db exists in app/siteminder/ssl, specify:

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

The policy store schema is created.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

Limits:

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

Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

     Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

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

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

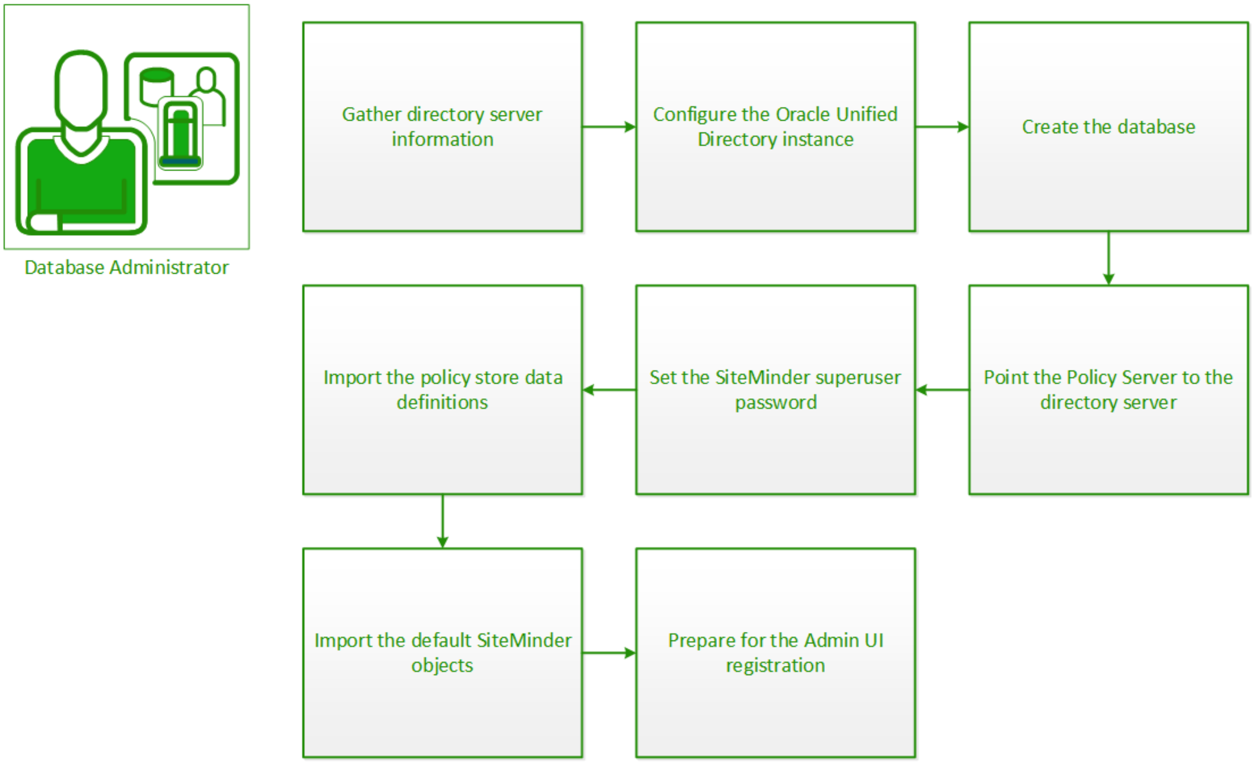
How to Configure Oracle Unified Directory as a Policy Store

Oracle Unified Directory (OUD) can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. This scenario describes how to configure a single directory server instance to store policy data and encryption keys.

Note: If your implementation requires, you can configure a separate key store.


Database Administrator
Gather directory server information
Configure the Oracle Unified Directory instance
Create the database
Point the Policy Server to the directory server
Set the SiteMinder superuser password
Import the policy store data definitions
Import the default SiteMinder objects
Prepare for the Admin UI registration

To configure Oracle Unified Directory as a policy store, complete the following procedures:

1. Gather directory server information (see page 110)
2. Configure the Oracle Unified Directory instance (see page 201).
3. Create the database (see page 205).
4. Point the Policy Server to the directory server (see page 97).
5. Set the CA SiteMinder® superuser password (see page 98).

6. Import the policy store data definitions (see page 100).
7. Import the default CA SiteMinder® objects (see page 100).
8. Prepare for the Administrative UI registration (see page 102).

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 CA SiteMinder® data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Oracle Unified Directory Instance

Oracle Unified Directory requires more configuration before you can use it as a policy store. The following process lists the configuration steps:

1. Specify the CA SiteMinder® schema files on Windows (see page 201) or UNIX (see page 202).
2. Configure policy store indexing on Windows (see page 202) or UNIX (see page 203).

Specify the CA SiteMinder® Schema Files on Windows

Specify the CA SiteMinder® schema files.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to *ps_home*\db\tier2\OUD and copy the following file to the schema folder (*oud_instance*\config\schema) in the Oracle Unified Directory installation directory:

   oud_sm_schema.ldif

   ps_home

   Specifies the Policy Server installation path.

   oud_instance

   Specifies the name of the Oracle Unified Directory instance.
3. Navigate to *ps_home*\xps\db\schema_extension\db\OUD and copy the following file to the schema folder (*oud_instance*\config\schema) in the Oracle Unified Directory installation directory:

   oud_XPS_schema.ldif

The CA SiteMinder® schema files are specified.

Specify the CA SiteMinder® Schema Files on UNIX

Specify the CA SiteMinder® schema files.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to *ps_home*/db/tier2/OUD and copy the following file to the schema folder (*oud_instance*/config/schema) in the Oracle Unified Directory installation directory:

   oud_sm_schema.ldif

   ps_home

   Specifies the Policy Server installation path.

   oud_instance

   Specifies the name of the Oracle Unified Directory instance.
3. Navigate to *ps_home*/xps/db/schema_extension/db/OUD and copy the following file to the schema folder (*oud_instance*/config/schema) in the Oracle Unified Directory installation directory:

   oud_XPS_schema.ldif

The CA SiteMinder® schema files are specified.

Configure Policy Store Indexing on Windows

Specify indexing in the Oracle Unified Directory instance config file (*oud_instance*\config\config.ldif) to use Oracle Unified Directory as a policy store.

Follow these steps:

1. Stop the Oracle Unified Directory instance.
2. Open the *oud_instance*\config\config.ldif file with a text editor.

   oud_instance

   Specifies the name of the Oracle Unified Directory instance.
3. Locate the following lines:

   ```
   dn: cn=Index,cn=userRoot,cn=Workflow Elements,cn=config
   objectClass: top
   objectClass: ds-cfg-branch
   cn: Index
   ```
4. Insert a new line in the file, and then add the contents from the following files:

   - *ps_home*\db/tier2\OUD\oud_sm_indexes.ldif
   - *ps_home*\xps\db\ schema_extension\db\OUD\oud_xps_index.ldif.

5. Save the file and close the text editor.

6. To rebuild the indexes, navigate to *oud_instance*\bat and run the following command .

```
rebuild-index.bat -b base_dn --rebuildAll -h hostname -p OUD_administration_port
-D "cn=Directory Manager" -j <bindpasswordfile> -X -t 0 --completionNotify
emailAddress
```

base_dn

Specifies the base DN of a back end that supports indexing. The index is rebuilt within the scope of the given base DN.

hostname

Specifies the fully qualified hostname or IP address of the directory server. If not provided, defaults to localhost.

OUD_administration_port

Specifies the administration port of the directory server. If not provided, the default administration port (44444) is used.

bindpasswordfile

Specifies the file that contains the bind password to use when authenticating to the directory server.

completionNotify

Specifies the email address of a recipient to be notified when the task completes. This option can be specified more than once in a single command.

7. Restart the Oracle Unified Directory instance after the rebuild task is completed.

Policy store indexing for Oracle Unified Directory is specified.

Specify Policy Store Indexing on UNIX

Specify indexing in the Oracle Unified Directory instance config file (*oud_instance/*config/config.ldif) to use Oracle Unified Directory as a policy store.

Follow these steps:

1. Stop the Oracle Unified Directory instance.

2. Open the *oud_instance*/config/config.ldif file with a text editor.

oud_instance

Specifies the name of the Oracle Unified Directory instance.

3. Locate the following lines:

   ```
   dn: cn=Index,cn=userRoot,cn=Workflow Elements,cn=config
   objectClass: top
   objectClass: ds-cfg-branch
   cn: Index
   ```

4. Insert a new line in the file, and then add the contents from the following files:

   - *ps_home*/db/tier2/OUD/oud_sm_indexes.ldif
   - *ps_home*/xps/db/ schema_extension/db/OUD/oud_xps_index.ldif.

   ps_home

   Specifies the Policy Server installation path.

5. Save the file and close the text editor.

6. Navigate to *oud_instance/*bin and run the following command to rebuild the indexes.

   ```
   rebuild-index -b base_dn --rebuildAll -h hostname -p OUD_administration_port -D
   "cn=Directory Manager" -j bindpasswordfile -X -t 0 --completionNotify
   emailAddress
   ```

   base_dn

   Specifies the base DN of a back end that supports indexing. The index is rebuilt within the scope of the given base DN.

   hostname

   Specifies the fully qualified hostname or IP address of the directory server. If not provided, defaults to localhost.

   OUD_administration_port

   Specifies the administration port of the directory server. If not provided, the default administration port (44444) is used.

   bindpasswordfile

   Specifies the file that contains the bind password to use when authenticating to the directory server.

   completionNotify

   Specifies the email address of a recipient to be notified when the task completes. This option can be specified more than once in a single command.

7. Restart the Oracle Unified Directory instance after the rebuild task is completed.

The policy store indexing for Oracle Unified Directory is specified.

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

To create a base tree structure to store policy store objects, specify the following entry under the root DN:

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

Add Entries to the Database

Add entries to the directory server so that CA SiteMinder® has the necessary organization and organizational role information.

Follow these steps:

1. Create an LDIF file.

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

   ```
   # CA, example.com
   dn: ou=Netegrity,dc= example,dc=com
   ou: CA
   objectClass: organizationalUnit
   objectClass: top

   # SiteMinder, CA, example.com
   dn: ou=SiteMinder,ou=CA,dc= example,dc=com
   ou: SiteMinder
   objectClass: organizationalUnit
   objectClass: top
   ```

```
# PolicySvr4, SiteMinder, CA, example.com
dn: ou=PolicySvr4,ou=SiteMinder,ou=CA,dc= example,dc=com
ou: PolicySvr4
objectClass: organizationalUnit
objectClass: top
```

2. Run the following command to add the entries.

   ```
   ldapmodify –h hostname -p port -D bindDN -j pwd_file -a -f LDIF_file_name
   ```

   hostname

   Specifies the fully qualified hostname or IP address of the directory server.

   Default: localhost.

   port

   Specifies the port on which to contact the directory server.

   Default: 389

   BindDN

   Specifies the bind DN to authenticate to the directory server.

   Default: cn=Directory Manager

   pwd_file

   Specifies the file that contains the bind password for authenticating to the directory server.

   LDIF_file_name

   Specifies the LDIF file that you created in Step 1.

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

2. Click the Data tab.

3. Select the following value from the Database list:

   ```
   Policy Store
   ```

4. Select the following value from the Storage list:

   LDAP

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

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

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

6. Click Apply.

7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.

8. Select the following value from the Database list:

   `Key Store`

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    `Use Policy Store database`

11. Click OK.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

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

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

   Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

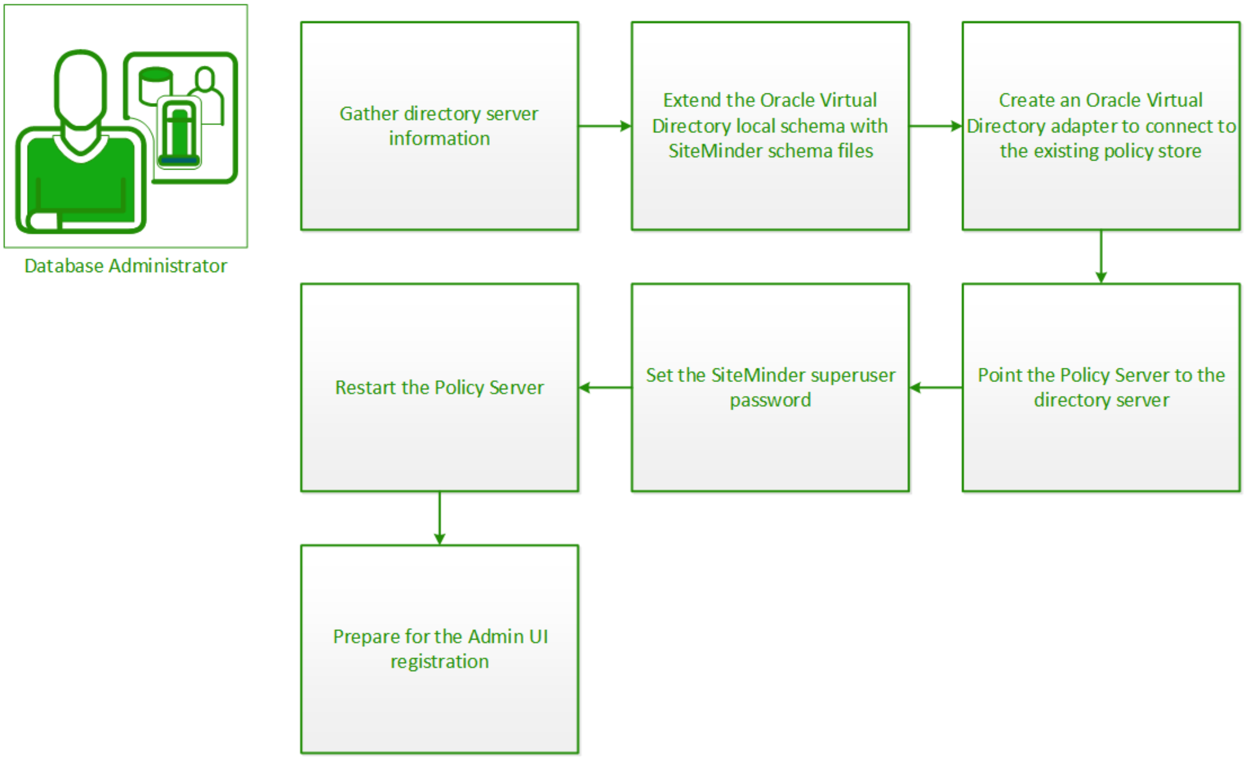
How to Configure Oracle Virtual Directory as a Policy Store

Oracle Virtual Directory (OVD) can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. This scenario describes how to configure a single directory server instance to store policy data and encryption keys.

Note: If your implementation requires, you can configure a separate key store.


Database Administrator
Gather directory server information
Extend the Oracle Virtual Directory local schema with SiteMinder schema files
Create an Oracle Virtual Directory adapter to connect to the existing policy store
Point the Policy Server to the directory server
Set the SiteMinder superuser password
Restart the Policy Server
Prepare for the Admin UI registration

To configure Oracle Virtual Directory as a policy store, do the following procedures:

1. Gather directory server information (see page 110)
2. Extend the Oracle Virtual Directory local schema with CA SiteMinder® schema files (see page 215).
3. Create an Oracle Virtual Directory adapter to connect to the existing policy store (see page 216).
4. Point the Policy Server to the directory server (see page 97).

5. Set the CA SiteMinder® superuser password (see page 98).
6. Restart the Policy Server (see page 116).
7. Prepare for the Administrative UI registration (see page 102).

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 CA SiteMinder® data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

Extend the OVD Local Schema With the CA SiteMinder® Schema Files

Extend the Oracle Virtual Directory with the following CA SiteMinder® schema files:

- ovd_sm_schema.ldif
- ovd_xps_schema.ldif

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to *siteminder_home*/db/tier2/Oracle Virtual Directory and copy the following file to the OVD host system:

   ```
   ovd_sm_schema.ldif
   ```

3. Navigate to *siteminder_home*/xps/db/schema_extension/db/Oracle Virtual Directory and copy the following file to the OVD host system.

   ```
   ovd_xps_schema.ldif
   ```

4. Log in to the Oracle Virtual Directory system.
5. Have the administrator of your directory server run the following commands to extend the local schema with the CA SiteMinder® schema files:

   ```
   ldapmodify -h OVD_Host –p OVD_Port -D cn=Admin -w Admin_Password -v -a -f
   ovd_sm_schema.ldif
   ```

   ```
   ldapmodify -h OVD_Host –p OVD_Port -D cn=Admin -w Admin_Password -v -a -f
   ovd_xps_schema.ldif
   ```

   ```
   dsconf reindex -h localhost -p OVD_Port -e "ou=Netegrity,root_database"
   ```

   OVD_Host

   Specifies the OVD system IP Address or fully qualified domain name.

   OVD_Port

   Specifies the port on which the OVD instance is running.

   cn=Admin

   Specifies the OVD server admin with rights to modify the schema.

   Admin_Password

   Specifies the server admin password.

Create an Oracle Virtual Directory Adapter to Connect to Existing Policy Store

To create an Oracle Virtual Directory LDAP adapter to connect to your existing policy store, use the Oracle Directory Services Manager.

Follow these steps:

1. Log in to Oracle Directory Services Manager.
2. Select Adapter from the task selection bar. The Adapter navigation tree appears.
3. Click the Create Adapter button. The New Adapter Wizard appears.
4. Specify the following values on the Type screen:

   Adapter Type

   Select LDAP.

   Adapter Name

   Enter a unique name for the LDAP adapter.

   Adapter Template

   Select an adapter template that corresponds to the directory type of the existing policy store.

5. Click Next.
6. Enter the following values on the Connection screen (accept the defaults for all other settings):

   Use DNS for Auto Discovery

   Select No.

   Host

   Enter the hostname or IP address of the remote host.

   Port

   Enter the port at which the remote host instance is running.

   Server proxy Bind DN

   Enter the credentials of a directory user who has permission to modify directory contents.

   Proxy Password

   Password for the user that is specified in the Secure proxy Bind DN field.

7. Click Next.

8. On the Connection Test screen, click Next if the connection status is OK. Otherwise, click Back and troubleshoot your connection settings.

9. Enter the following values on the Namespace screen (accept the defaults for all other settings):

   Remote Base:

   Click Browse and select the DN at which the policy data is stored.

   Mapped Namespace

   Enter a local DN at which to map the policy data.

10. Review the Summary page and click Finish.

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

2. Click the Data tab.

3. Select the following value from the Database list:

   ```
   Policy Store
   ```

4. Select the following value from the Storage list:

   LDAP

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

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

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

6. Click Apply.
7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.
8. Click OK.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

   – The password must contain at least six (6) characters and cannot exceed 24 characters.

   – The password cannot include an ampersand (&) or an asterisk (*).

   – If the password contains a space, enclose the passphrase with quotation marks.

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.

4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.

5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

   The Policy Server stops as indicated by the red stoplight.

3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Red Hat Directory Server as a Policy Store

Red Hat Directory Server can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key 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 CA SiteMinder® data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Store

Complete the following procedures to configure Red Hat Directory Server as a policy store:

1. Point the Policy Server to the policy store.
2. Create the policy store schema.
3. Set the CA SiteMinder® superuser password.
4. Import the policy store data definitions.
5. Import the default policy store objects.
6. Restart the Policy Server.
7. Prepare for the Administrative UI registration.

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

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

   `Policy Store`

4. Select the following value from the Storage list:

   LDAP

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

   ■ LDAP IP Address

   ■ Admin Username

   ■ Password

   ■ Confirm Password

   ■ Root DN

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

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

   `Key Store`

9. Select the following value from the Storage list:

   LDAP

10. Select the following option:

    `Use Policy Store database`

11. Click OK.

Create the Policy Store Schema

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

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command:
   ```
   smldapsetup ldgen -fschema_file
   ```
   schema_file

      Specifies the name of the LDIF file you are creating.

   An LDIF file is created using the policy store schema.
3. Run the following command:
   ```
   smldapsetup ldmod -fschema_file
   ```
   schema_file

      Specifies the name of the LDIF file you created.

   The policy store schema is imported.
4. Complete the following steps:
   a. Restart the directory server. Restarting the directory server is required to save the policy store schema correctly.

   b. Repeat step 3. Restarting the directory server removed the policy store root. Importing the policy store schema again is required to create the policy store root.
5. Run the following command:
   ```
   smldapsetup ldmod

   -fsiteminder_home/xps/db/RedHat_7_1.ldif
   ```
   -fsiteminder_home

      Specifies the Policy Server installation path.

   The policy store schema is extended for XPS.

The policy store schema is created.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

   – The password must contain at least six (6) characters and cannot exceed 24 characters.

   – The password cannot include an ampersand (&) or an asterisk (*).

   – If the password contains a space, enclose the passphrase with quotation marks.

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

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

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Siemens DirX as a Policy Store

Siemens DirX can function as a policy store. A single directory server instance can function as a:

- Policy store
- Key store

Using a single directory server simplifies administration tasks. The following sections provide instruction on how to configure a single directory server instance to store policy data and encryption keys. If your implementation requires, you can configure a separate key 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 CA SiteMinder® data store. You can print the applicable worksheet and can use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

How to Configure the Policy Store

Complete the following procedures to configure Siemens DirX as a policy store:

1. Create the policy store schema.
2. Point the Policy Server to the policy store.
3. Set the CA SiteMinder® superuser password.
4. Import the policy store data definitions.

5. Import the default policy store objects.
6. Prepare for the Administrative UI registration.

Create the Policy Store Schema

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

Prerequisite

Certain policy store operations require searches on CA SiteMinder® attributes. The DirX directory must index the attributes to perform search operations.

By default, the DirX directory indexes 20 attributes. CA SiteMinder® contains more attributes than this default limit. Increase the number of attributes that the directory can index to a maximum. We recommend a value of 800.

To increase the attribute indexing limit, use the following command while initializing the database profile.

```
dbamboot -Pdatabase_profile_name -aindexing_value
```

Example:

```
dbamboot -Pprofile1 -a800
```

Create the Schema

Follow these steps:

1. Create the following directory structure on the directory server host system:

   DirX_installation\scripts\security\CA\SiteMinder

   DirX_installation

   Specifies the DirX installation path.

2. Log in to the Policy Server host system.

3. Navigate to *siteminder_home*\db\tier2\SiemensDirx and copy the following files to *DirX_installation*\scripts\security\CA\SiteMinder:

   - dirxabbr-ext.SiteMinder*release*
   - schema_ext_for_SiteMinder*release*.adm
   - bind.tcl
   - l-bind.cp
   - GlobalVar.tcl

siteminder_home

Specifies the Policy Server installation path.

release

Specifies the CA SiteMinder® release.

4. Navigate to *siteminder_home*\xps\db\Siemens_DirX and copy the following files to *DirX_installation*\scripts\security\CA\SiteMinder:
   - dirxabbr-ext.XPS
   - schema_ext_for_XPS.adm
5. Rename the following files:
   - schema_ext_for_SiteMinder*release*.adm to schema_ext_for_SiteMinder.adm
   - dirxabbr-ext.SiteMinder*release* to dirxabbr-ext.SiteMinder

   siteminder_home

   Specifies the Policy Server installation path.

   release

   Specifies the CA SiteMinder® release.
6. Copy the following files to *DirX_installation*\client\conf:
   - dirxabbr-ext.SiteMinder
   - dirxabbr-ext.XPS
7. Restart the DirX service.
8. Go to *DirX_installation*\scripts\security\CA\SiteMinder and edit the GlobalVar.tcl file to update the global variables that the DirX scripts reference.

   Default values:
   - LDAP port: 389
   - Root DN: o=My-Company
   - Admin username: cn=admin,o=My-Company
   - Admin password: dirx
9. From a command prompt, navigate to *DirX_installation*\scripts\security\CA\SiteMinder and execute the following commands:
   - dirxadm schema_ext_for_siteminder.adm
   - dirxadm schema_ext_for_XPS.adm
10. Restart the DirX service.

11. On the system where DirX is installed, index the attribute modifyTimestamp. Do this task manually or through the DirX Manager.

    The steps using the DirX Manager are as follows:

    a. Rebind to the DSA.

    b. Click on Schema on the left panel.

    c. Click on Database.

    d. Uncheck "Hide attributes with no index assigned".

    e. Click Edit.

    f. Under Index row, select the attribute modifyTimestamp.

    g. Save the changes.

    h. Right click on the Database and check consistence for attribute indexes.

12. Complete the following items using the DirX manage tool:

    a. Rebind to the DSA.

    b. Create the following base tree structure:

       - Under o=My-Company, create ou=Netegrity.
       - Under ou=Netegrity, create ou=SiteMinder.
       - Under ou=SiteMinder, create ou=PolicySvr4
       - Under ou=PolicySvr4, create ou=XPS

The policy store schema is created.

Point the Policy Server to the Policy Store

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

Follow these steps:

1. Open the Policy Server Management Console.

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

2. Click the Data tab.

3. Select the following value from the Database list:

   `Policy Store`

4. Select the following value from the Storage list:

   LDAP

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

   Note: You can click Help for a description of fields, controls, and their respective requirements.
6. Click Apply.
7. Click Test LDAP Connection to verify that the Policy Server can access the policy store.
8. Select the following value from the Database list:

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

   ```
   LDAP
   ```
10. Select the following option:

    ```
    Use Policy Store database
    ```
11. Click OK.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

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

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

   Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

   passphrase

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

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

   -adminui–setup

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

   -t *timeout*

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

   Unit of measurement: minutes

   Default: 240 (4 hours)

   Minimum Limit: 15

   Maximum Limit: 1440 (24 hours)

   -r *retries*

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

   Default: 1

   Maximum Limit: 5

   -c *comment*

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

   Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Configure a Separate Key Store

If you have a collocated policy/key store, you can configure the Policy Server to use a separate key store.

The type of directory server that is to function as a separate key store determines how you configure the store:

- If you can use the CA SiteMinder® smldapsetup utility to configure a policy store, you can configure a separate key store using key store–specific schema. The following directory servers can be configured this way:
  - Microsoft Active Directory
  - Microsoft AD LDS
  - Oracle Directory Server Enterprise Edition
  - Oracle Internet Directory Server
  - Red Hat Directory Server
- If you cannot use the CA SiteMinder® smldapsetup utility to configure a policy store, then you must:
  a. Configure a separate directory server instance with the policy store schema only. The policy store schema includes the key store schema. You do not have to:
     - Set the CA SiteMinder® superuser password.
     - Import the default policy store objects.
     - Import the policy store data definitions.

     A separate key store does not require these objects.

  b. Configure the Policy Server to use this policy store instance as a key store only.

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

Microsoft Active Directory as a Key Store

You can configure Microsoft Active Directory as a separate key store.

How to Configure the Key Store

Complete the following tasks to create the key store:

1. Create a directory server instance that is to function as the key store. Be sure to create a root suffix and root object to store the CA SiteMinder® keys.

   Note: For more information, see your vendor–specific documentation.

2. Create an LDAP user with privileges to create the schema, and read, modify, and delete objects in the LDAP tree underneath the key store root object.

   Note: For more information, see your vendor–specific documentation.

3. Register the key store.
4. Create the key store schema.
5. Import the key store schema.
6. Restart the Policy Server.

Gather Directory Server Information

Specific information is required to configure a separate key store. Gather the following information:

Host

The fully qualified name or the IP Address of the directory server host system.

Port

The port on which the directory server instance is listening. This value is only required if the instance is listening on a non–standard port.

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

Administrative DN

Specifies the LDAP user name of a user that has privileges to:

- create schema

Note: This permission is only required to import the key store schema. After you deploy the key store, you can configure the Policy Server with a user that does not have the permission.

- read
- write
- modify
- delete

Administrative password

Specifies the password for the Administrative DN.

Key store root DN

Specifies the distinguished name of the node in the LDAP tree where the key store objects must be imported.

SSL client certificate

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

Limit: SSL only

Register the Key Store

Registering the key store configures a connection between the key store and the Policy Server. The Policy Server uses the credentials that you supply to manage the key store.

Important! Registration does not configure the Policy Server to use the separate key store. The settings do not take effect until the Policy Server is restarted. Do not restart the Policy Server until the key store is configured and you are ready to deploy it.

Follow these steps:

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

   ```
   smldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot
   -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: For more information about these modes and arguments, see the *Policy Server Administration Guide*.

   Example:

   ```
   smldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager"
   -wpassword -r"dc=test" -k1
   ```

3. Start the Policy Server Management Console and open the Data tab.
4. Complete one of the following procedures:
   - If the Policy Server is configured to use a data relational database:
     a. Select Keystore from the Database list.
     b. Select LDAP from the Storage list to display the connection settings and administrative credentials.

c. Verify that the connection settings and administrative user setting appear.

d. Click test LDAP Connection to verify that the Policy Server can communicate with the key store instance.

- If the Policy Server is configured to use a directory server:

  a. Select Keystore from the Database list.

  b. Verify that the connection settings and the administrative user settings appear.

  c. Click test LDAP Connection to verify that the Policy Server can communicate with the key store instance.

Note: The Use Policy Store database setting is cleared. The cleared setting is expected normal behavior. The Policy Server continues to use the key store that is collocated with the policy store.

5. Exit the Policy Server Management Console.

   The separate key is registered with the Policy Server.

Create the Key Store Schema

The key store instance requires the schema to store and retrieve CA SiteMinder® web agent keys. Use the smldapsetup utility to create the key store schema file.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to create the key store schema file:

   ```
   smldapsetup ldgen -ffile_name -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: For more information about these modes and arguments, see the *Policy Server Administration Guide*.

   Example: smldapsetup ldgen -fkeystoreschema -k1

   The key store schema file is created.

Import the Key Store Schema

The key store instance requires the schema to store and retrieve CA SiteMinder® web agent keys. Use the smldapsetup utility to import the key store schema file.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to import the key store schema:

   ```
   smldapsetup ldmod -ffile_name -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Consider the following items:

   - For more information about these modes and arguments, see the *Policy Server Administration Guide*.
   - Standard out displays all policy store schema being imported. The behavior is normal and expected. The utility only imports the key–store specific schema.

   Example: smldapsetup ldmod -fkeystoreschema -k1

   The key store–specific schema is imported.

Restart the Policy Server

The Policy Server continues to use the collocated key store until you restart the Policy Server. Restart the Policy Server to begin using the separate key store.

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

Microsoft AD LDS as a Key Store

You can configure Microsoft AD LDS as a separate key store.

How to Configure the Key Store

Complete the following tasks to create the key store:

1. Create a directory server instance that is to function as the key store. Be sure to create a root suffix and root object to store the CA SiteMinder® keys.

   Note: For more information, see your vendor–specific documentation.

2. Create an LDAP user with privileges to create the schema, and read, modify, and delete objects in the LDAP tree underneath the key store root object.

   Note: For more information, see your vendor–specific documentation.

3. Be sure that the directory server meets the key store prerequisites.
4. Register the key store.
5. Create the key store schema.
6. Import the key store schema.
7. Restart the Policy Server.

Key Store Prerequisites

Be sure that you meet the following prerequisites before configuring the key store:

1. Create a key store partition.
2. Be sure that users can be created in the configuration partition. Only an administrative user in the configuration partition can import the key store schema.

Allow User Creation in the Configuration Partition

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

Follow these steps:

1. Open the ADSI Edit console.
2. Navigate to the following in the configuration partition:

   ```
   cn=directory service, cn=windows nt,
   cn=services, cn=configuration, cn={guid}
   ```

3. Locate the msDS-Other-Settings attribute.

4. Add the following new value to the msDS-Other-Settings attribute:

   ```
   ADAMAllowADAMSecurityPrincipalsInConfigPartition=1
   ```

5. In the configuration and policy store application partitions:

   a. Navigate to CN=Administrators, CN=Roles.

   b. Open the properties of CN=Administrators.

   c. Edit the member attribute.

   d. Click Add DN and paste the full DN of the user you created in the configuration partition.

   e. Go to the properties of the user you created and verify the value for the following object:

      ```
      msDS-UserAccountDisabled
      ```

      Be sure that the value is set false.

   The administrative user has rights over the configuration partition and all application partitions, including the key store partition.

Gather Directory Server Information

Specific information is required to configure a separate key store. Gather the following information:

Host

The fully qualified name or the IP address of the directory server host system.

Port

The port on which the directory server instance is listening. This value is only required if the instance is listening on a non–standard port.

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

- **Administrator DN**

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

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

  This user requires the following privileges:

  – create schema

    Note: This permission is only required to import the key store schema. After you deploy the key store, you can configure the Policy Server with a user that does not have the permission.

  – read

  – write

- modify
- delete

Administrator password

The password for the directory server administrator.

Root DN of the application partition

The root DN location of the application partition where the key store schema must be imported.

(Optional) SSL client certificate

If the directory connection is made over SSL, the path of the directory that contains the SSL client certificate database.

Register the Key Store

Registering the key store configures a connection between the key store and the Policy Server. The Policy Server uses the credentials that you supply to manage the key store.

Important! Registration does not configure the Policy Server to use the separate key store. The settings do not take effect until the Policy Server is restarted. Do not restart the Policy Server until the key store is configured and you are ready to deploy it.

Follow these steps:

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

   ```
   smldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot
   -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: For more information about these modes and arguments, see the *Policy Server Administration Guide*.

   Example:

   ```
   smldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager"
   -wpassword -r"dc=test" -k1
   ```

3. Start the Policy Server Management Console and open the Data tab.
4. Complete one of the following procedures:
   - If the Policy Server is configured to use a data relational database:
     a. Select Keystore from the Database list.
     b. Select LDAP from the Storage list to display the connection settings and administrative credentials.
     c. Verify that the connection settings and administrative user setting appear.
     d. Click test LDAP Connection to verify that the Policy Server can communicate with the key store instance.
   - If the Policy Server is configured to use a directory server:

     a. Select Keystore from the Database list.

     b. Verify that the connection settings and the administrative user settings appear.

     c. Click test LDAP Connection to verify that the Policy Server can communicate with the key store instance.

   Note: The Use Policy Store database setting is cleared. The cleared setting is expected normal behavior. The Policy Server continues to use the key store that is collocated with the policy store.
5. Exit the Policy Server Management Console.

   The separate key is registered with the Policy Server.

Create the Key Store Schema

The key store instance requires the schema to store and retrieve CA SiteMinder® web agent keys. Use the smldapsetup utility to create the key store schema file.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to create the key store schema file:

   ```
   smldapsetup ldgen -ffile_name -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: For more information about these modes and arguments, see the *Policy Server Administration Guide*.

   Example: smldapsetup ldgen -fkeystoreschema -k1

   The key store schema file is created.

Import the Key Store Schema

The key store instance requires the schema to store and retrieve CA SiteMinder® web agent keys. Use the smldapsetup utility to import the key store schema file.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to import the key store schema:

   ```
   smldapsetup ldmod -ffile_name -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Consider the following items:

   - For more information about these modes and arguments, see the *Policy Server Administration Guide*.
   - Standard out displays all policy store schema being imported. The behavior is normal and expected. The utility only imports the key–store specific schema.

   Example: smldapsetup ldmod -fkeystoreschema -k1

   The key store–specific schema is imported.

Restart the Policy Server

The Policy Server continues to use the collocated key store until you restart the Policy Server. Restart the Policy Server to begin using the separate key store.

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

Oracle Directory Server Enterprise Edition as a Key Store

You can configure Oracle Directory Server Enterprise Edition as a separate key store.

How to Configure the Key Store

Complete the following tasks to create the key store:

1. Create a directory server instance that is to function as the key store. Be sure to create a root suffix and root object to store the CA SiteMinder® keys.

   Note: For more information, see your vendor–specific documentation.

2. Create an LDAP user with privileges to create the schema, and read, modify, and delete objects in the LDAP tree underneath the key store root object.

   Note: For more information, see your vendor–specific documentation.

3. Review the key store consideration.
4. Gather directory server information.
5. Register the key store.
6. Create the key store schema.
7. Import the key store schema.
8. Restart the Policy Server.

Key Store Considerations

The smldapsetup utility creates the ou=Netegrity, *root* sub suffix and PolicySvr4 database.

root

The directory root you specify when registering the key store. This variable has to be either an existing root suffix or sub suffix.

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

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

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

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

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

Note: For more information about root and sub suffixes, see your vendor–specific documentation.

Gather Directory Server Information

Specific information is required to configure a separate key store. Gather the following information:

Host

The fully qualified name or the IP Address of the directory server host system.

Port

The port on which the directory server instance is listening. This value is only required if the instance is listening on a non–standard port.

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

Administrative DN

Specifies the LDAP user name of a user that has privileges to:

- create schema

  Note: This permission is only required to import the key store schema. After you deploy the key store, you can configure the Policy Server with a user that does not have the permission.

- read
- write
- modify
- delete

Administrative password

Specifies the password for the Administrative DN.

Key store root DN

Specifies the distinguished name of the node in the LDAP tree where the key store objects must be imported.

SSL client certificate

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

Limit: SSL only

Register the Key Store

Registering the key store configures a connection between the key store and the Policy Server. The Policy Server uses the credentials that you supply to manage the key store.

Important! Registration does not configure the Policy Server to use the separate key store. The settings do not take effect until the Policy Server is restarted. Do not restart the Policy Server until the key store is configured and you are ready to deploy it.

Follow these steps:

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

   ```
   smldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot
   -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: For more information about these modes and arguments, see the *Policy Server Administration Guide*.

   Example:

   ```
   smldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager"
   -wpassword -r"dc=test" -k1
   ```

3. Start the Policy Server Management Console and open the Data tab.
4. Complete one of the following procedures:
   - If the Policy Server is configured to use a data relational database:
     a. Select Keystore from the Database list.
     b. Select LDAP from the Storage list to display the connection settings and administrative credentials.

c. Verify that the connection settings and administrative user setting appear.

d. Click test LDAP Connection to verify that the Policy Server can communicate with the key store instance.

- If the Policy Server is configured to use a directory server:

  a. Select Keystore from the Database list.

  b. Verify that the connection settings and the administrative user settings appear.

  c. Click test LDAP Connection to verify that the Policy Server can communicate with the key store instance.

Note: The Use Policy Store database setting is cleared. The cleared setting is expected normal behavior. The Policy Server continues to use the key store that is collocated with the policy store.

5. Exit the Policy Server Management Console.

   The separate key is registered with the Policy Server.

Create the Key Store Schema

The key store instance requires the schema to store and retrieve CA SiteMinder® web agent keys. Use the smldapsetup utility to create the key store schema file.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to create the key store schema file:

   ```
   smldapsetup ldgen -ffile_name -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: For more information about these modes and arguments, see the *Policy Server Administration Guide*.

   Example: smldapsetup ldgen -fkeystoreschema -k1

   The key store schema file is created.

Import the Key Store Schema

The key store instance requires the schema to store and retrieve CA SiteMinder® web agent keys. Use the smldapsetup utility to import the key store schema file.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to import the key store schema:

   ```
   smldapsetup ldmod -ffile_name -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Consider the following items:

   - For more information about these modes and arguments, see the *Policy Server Administration Guide*.
   - Standard out displays all policy store schema being imported. The behavior is normal and expected. The utility only imports the key–store specific schema.

   Example: smldapsetup ldmod -fkeystoreschema -k1

   The key store–specific schema is imported.

Restart the Policy Server

The Policy Server continues to use the collocated key store until you restart the Policy Server. Restart the Policy Server to begin using the separate key store.

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

Replicate an Oracle Directory Server Key Store

CA SiteMinder® creates a UserRoot and a PolicySvr4 database. Suffix mappings point to the PolicySvr4 database. Replicating a key store requires that you set up a replication agreement for the PolicySvr4 database directory.

Follow these steps:

1. Configure a replication agreement as detailed by your vendor–specific documentation.
2. Log in to the Policy Server host system.

3. Run the following command to generate the CA SiteMinder® indexes:

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

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

4. Set up the indexes on a replica server:

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

   host

   Specifies the replica host.

   replicaport

   Specifies the replica port number.

   AdminDN

   Specifies the replica administrator DN.

   Example: cn=directory manager

   AdminPW

   Specifies the replica administrator password.

   The CA SiteMinder® indexes are replicated.

Oracle Internet Directory Server as a Key Store

You can configure Oracle Internet Directory Server as a separate key store.

How to Configure the Key Store

Complete the following tasks to create the key store:

1. Create a directory server instance that is to function as the key store. Be sure to create a root suffix and root object to store the CA SiteMinder® keys.

   Note: For more information, see your vendor–specific documentation.

2. Create an LDAP user with privileges to create the schema, and read, modify, and delete objects in the LDAP tree underneath the key store root object.

   Note: For more information, see your vendor–specific documentation.

3. Register the key store.

4. Create the key store schema.

5. Import the key store schema.
6. Restart the Policy Server.

Gather Directory Server Information

Specific information is required to configure a separate key store. Gather the following information:

Host

The fully qualified name or the IP Address of the directory server host system.

Port

The port on which the directory server instance is listening. This value is only required if the instance is listening on a non–standard port.

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

Administrative DN

Specifies the LDAP user name of a user that has privileges to:

- create schema

Note: This permission is only required to import the key store schema. After you deploy the key store, you can configure the Policy Server with a user that does not have the permission.

- read
- write
- modify
- delete

Administrative password

Specifies the password for the Administrative DN.

Key store root DN

Specifies the distinguished name of the node in the LDAP tree where the key store objects must be imported.

SSL client certificate

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

Limit: SSL only

Register the Key Store

Registering the key store configures a connection between the key store and the Policy Server. The Policy Server uses the credentials that you supply to manage the key store.

Important! Registration does not configure the Policy Server to use the separate key store. The settings do not take effect until the Policy Server is restarted. Do not restart the Policy Server until the key store is configured and you are ready to deploy it.

Follow these steps:

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

   ```
   smldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot
   -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: For more information about these modes and arguments, see the *Policy Server Administration Guide*.

   Example:

   ```
   smldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager"
   -wpassword -r"dc=test" -k1
   ```

3. Start the Policy Server Management Console and open the Data tab.
4. Complete one of the following procedures:
   - If the Policy Server is configured to use a data relational database:
     a. Select Keystore from the Database list.
     b. Select LDAP from the Storage list to display the connection settings and administrative credentials.
     c. Verify that the connection settings and administrative user setting appear.
     d. Click test LDAP Connection to verify that the Policy Server can communicate with the key store instance.
   - If the Policy Server is configured to use a directory server:

     a. Select Keystore from the Database list.

     b. Verify that the connection settings and the administrative user settings appear.

     c. Click test LDAP Connection to verify that the Policy Server can communicate with the key store instance.

Note: The Use Policy Store database setting is cleared. The cleared setting is expected normal behavior. The Policy Server continues to use the key store that is collocated with the policy store.

5. Exit the Policy Server Management Console.

   The separate key is registered with the Policy Server.

Create the Key Store Schema

The key store instance requires the schema to store and retrieve CA SiteMinder® web agent keys. Use the smldapsetup utility to create the key store schema file.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to create the key store schema file:

   ```
   smldapsetup ldgen -ffile_name -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: For more information about these modes and arguments, see the *Policy Server Administration Guide*.

   Example: smldapsetup ldgen -fkeystoreschema -k1

   The key store schema file is created.

Import the Key Store Schema

The key store instance requires the schema to store and retrieve CA SiteMinder® web agent keys. Use the smldapsetup utility to import the key store schema file.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to import the key store schema:

   ```
   smldapsetup ldmod -ffile_name -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

Consider the following items:

- For more information about these modes and arguments, see the *Policy Server Administration Guide*.
- Standard out displays all policy store schema being imported. The behavior is normal and expected. The utility only imports the key–store specific schema.

Example: smldapsetup ldmod -fkeystoreschema -k1

The key store–specific schema is imported.

Restart the Policy Server

The Policy Server continues to use the collocated key store until you restart the Policy Server. Restart the Policy Server to begin using the separate key store.

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

Red Hat Directory Server as a Key Store

You can configure Red Hat Directory Server as a separate key store.

How to Configure the Key Store

Complete the following tasks to create the key store:

1. Create a directory server instance that is to function as the key store. Be sure to create a root suffix and root object to store the CA SiteMinder® keys.

   Note: For more information, see your vendor–specific documentation.

2. Create an LDAP user with privileges to create the schema, and read, modify, and delete objects in the LDAP tree underneath the key store root object.

   Note: For more information, see your vendor–specific documentation.

3. Register the key store.
4. Create the key store schema.
5. Import the key store schema.
6. Restart the Policy Server.

Register the Key Store

Registering the key store configures a connection between the key store and the Policy Server. The Policy Server uses the credentials that you supply to manage the key store.

Important! Registration does not configure the Policy Server to use the separate key store. The settings do not take effect until the Policy Server is restarted. Do not restart the Policy Server until the key store is configured and you are ready to deploy it.

Follow these steps:

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

   ```
   smldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot
   -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: For more information about these modes and arguments, see the *Policy Server Administration Guide*.

   Example:

   ```
   smldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager"
   -wpassword -r"dc=test" -k1
   ```

3. Start the Policy Server Management Console and open the Data tab.
4. Complete one of the following procedures:
   - If the Policy Server is configured to use a data relational database:
     a. Select Keystore from the Database list.
     b. Select LDAP from the Storage list to display the connection settings and administrative credentials.
     c. Verify that the connection settings and administrative user setting appear.
     d. Click test LDAP Connection to verify that the Policy Server can communicate with the key store instance.
   - If the Policy Server is configured to use a directory server:

     a. Select Keystore from the Database list.

     b. Verify that the connection settings and the administrative user settings appear.

     c. Click test LDAP Connection to verify that the Policy Server can communicate with the key store instance.

   Note: The Use Policy Store database setting is cleared. The cleared setting is expected normal behavior. The Policy Server continues to use the key store that is collocated with the policy store.

5. Exit the Policy Server Management Console.

   The separate key is registered with the Policy Server.

Create the Key Store Schema

The key store instance requires the schema to store and retrieve CA SiteMinder® web agent keys. Use the smldapsetup utility to create the key store schema file.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to create the key store schema file:

   ```
   smldapsetup ldgen -ffile_name -k1
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: For more information about these modes and arguments, see the *Policy Server Administration Guide*.

   Example: smldapsetup ldgen -fkeystoreschema -k1

   The key store schema file is created.

Import the Key Store Schema

The key store instance requires the schema to store and retrieve CA SiteMinder® web agent keys. Use the smldapsetup utility to import the key store schema file.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to import the key store schema:

   ```
   smldapsetup ldmod -ffile_name -k1
   ```

   Note:

   - For more information about these modes and arguments, see the *Policy Server Administration Guide*.
   - Standard out displays all policy store schema being imported. The behavior is normal and expected. The utility only imports the key–store specific schema. The utility only imports the key–store specific schema.

   Example:

   ```
   smldapsetup ldmod -fkeystoreschema -k1
   ```

   The key store–specific schema is imported.

3. Complete the following steps:

   a. Restart the directory server. Restarting the directory server is required to save the key store schema correctly.

   b. Repeat step 2. Restarting the directory server removed the key store root. Importing the key store schema again is required to create the key store root.

   The key store–specific schema is imported.

Restart the Policy Server

The Policy Server continues to use the collocated key store until you restart the Policy Server. Restart the Policy Server to begin using the separate key store.

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

Chapter 7: Configuring CA SiteMinder® Data Stores in a Relational Database

Relational Databases as a Policy or Key Store

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

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

- Microsoft SQL Server
- Oracle RDBMS

If you do not use the Policy Server installer to configure a policy store automatically, you can manually configure a policy store after installing the Policy Server. Additionally, after you install the Policy Server, you can use the Policy Server Management Console to point the Policy Server to an existing policy store.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

In addition to policy store support, you can use a relational database to store CA SiteMinder® keys, audit logs, and session data.

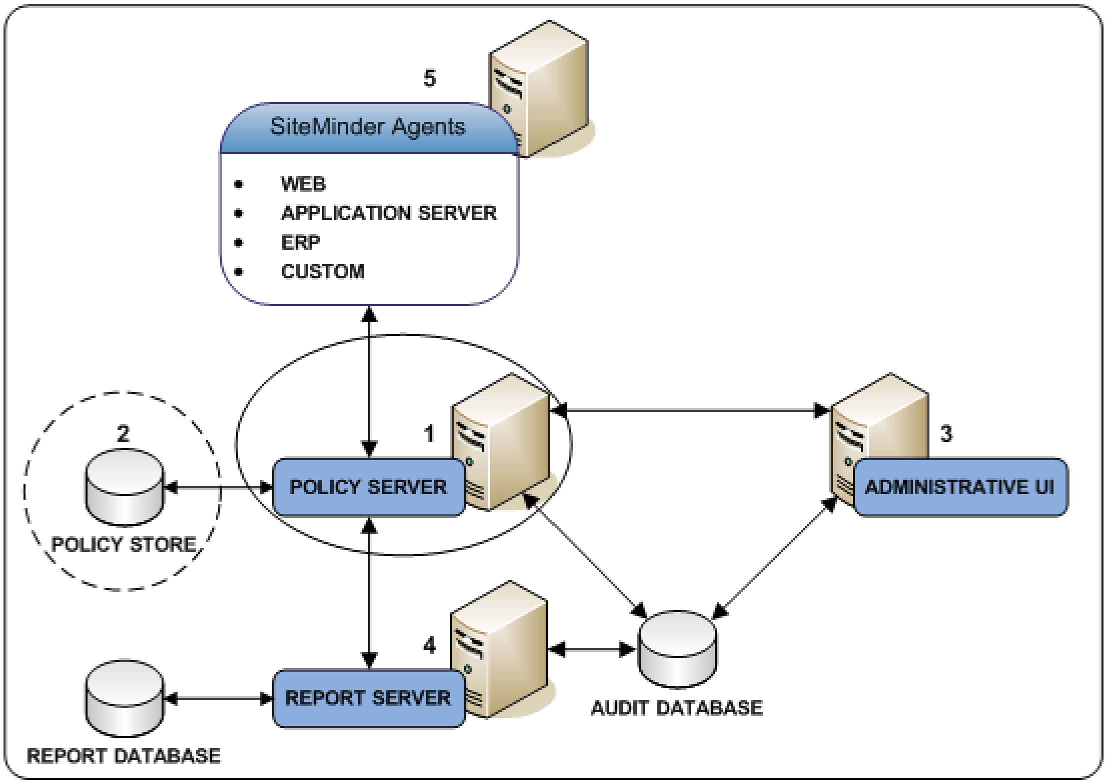
Installation Road Map

The following diagram illustrates a sample CA SiteMinder® installation and lists the order in which you install and configure each component.

- A solid line surrounds the Policy Server, which is required before configuring a policy store. If a Policy Server is not part of your environment, install it before continuing.
- The dotted line surrounds the policy store. Configure this component now.

The following figure depicts a single policy/key store instance. Although not illustrated, your environment can use separate instances for individual policy and key stores.

Equation 2: Installation Roadmap



Important Considerations

Consider the following before configuring a policy store:

- Avoid possible policy store corruption—Be sure that the database server that is to host the policy store is configured to store objects in UTF-8 form:
  - (Oracle) Be sure that the database is configured to store objects in UTF-8 form. Oracle supports unicode within many of their character sets. For more information about configuring your database to store objects in UTF-8 form, see your vendor-specific documentation.
  - (SQL Server) Be sure that the database is configured using the default collation (SQL_Latin1_General_CP1_CI_AS). Using a collation that is case sensitive can result in unexpected behaviors. For more information about configuring your database to store objects using the default collation, see your vendor-specific documentation.

- Do not use brackets around the IP address when using IPv6 ODBC data sources or the connection fails.

  Example: Use fec0::9255:20c:29ff:fe47:8089 instead of [fec0::9255:20c:29ff:fe47:8089]

  Note: For more information about IPv6-supported databases, see the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

Default Policy Store Objects Consideration

When you configure a policy store, the following default policy store object files are available:

- smpolicy.xml
- smpolicy-secure.xml

Consider the following items when choosing a file to:

- Both files contain the default objects that the policy store requires.
  - If you use the Policy Server Configuration Wizard to configure the policy store automatically, the wizard only uses smpolicy.xml.
  - If you want to use smpolicy–secure.xml, configure the policy store manually.
- Both files provide default security settings. These settings are available in the default Agent Configuration Object (ACO) templates that are available in the Administrative UI.
- The smpolicy-secure file provides more restrictive default security settings.
- Choosing smpolicy does not limit you from using the more restrictive default security settings. You can modify the default ACO settings using the Administrative UI.

  Note: For more information, see the *Policy Server Configuration Guide*.

The following table summarizes the security settings for both files:

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

Parameter Name	smpolicy Values	smpolicy–secure Values
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	All smpolicy values.
LimitCookieProvider	No	Yes
ValidTargetDomain	This file does not include this parameter.	This parameter does not have a default value. Provide a valid redirection domain. Example: validtargetdomain=".example.com"

Schema Files for Relational Databases

CA SiteMinder® provides schema files for configuring the following CA SiteMinder® data stores:

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

Note: The CA SiteMinder® schema files are installed with the Policy Server. If the Policy Server is installed on a UNIX system, copy the schema files from *siteminder_home*/db/SQL directory to a temporary directory (C:\temp) on the Windows system to which the database is installed.

siteminder_home

Specifies the Policy Server installation path.

IBM DB2 Schema Files

The following SQL Server schema files are provided in the *siteminder_home*\db\tier2\DB2 directory.

siteminder_home

Specifies the Policy Server installation path.

sm_db2_ps.sql

Creates the schema for a policy store and key store.

Note: If you are storing keys in a different database, this schema file creates the schema for the key store data.

sm_db2_logs.sql

Creates the schema for CA SiteMinder® audit logs. For 12.52 edit this script (see page 344) before using it to create an audit store.

sm_db2_ss.sql

Creates the schema for a CA SiteMinder® session store.

smsampleusers_db2.sql

Creates the schema for a CA SiteMinder® sample users database and populates the database with sample users.

The following IBM DB2 schema file is provided in the *siteminder_home*\xps\db directory.

DB2.sql

Creates the XPS schema for a policy store.

MySQL Schema Files

The following SQL Server schema files are provided in the *siteminder_home*\db\tier2\MySQL directory.

siteminder_home

Specifies the Policy Server installation path.

sm_mysql_ps.sql

Creates the schema for a policy store and key store.

Note: If you are storing keys in a different database, this schema file creates the schema for the key store data.

sm_mysql_logs.sql

Creates the schema for CA SiteMinder® audit logs.

sm_mysql_ss.sql

Creates the schema for a CA SiteMinder® session store.

smsampleusers_mysql.sql

Creates the schema for a CA SiteMinder® sample users database and populates the database with sample users.

The following MySQL schema file is provided in the *siteminder_home*\xps\db directory.

MySQL.sql

Creates the XPS schema for a policy store.

SQL Server Schema Files

The following SQL Server schema files are provided in the *siteminder_home*\db\SQL directory:

siteminder_home

Specifies the Policy Server installation path.

sm_mssql_ps.sql

Creates the schema for a policy store and key store.

Note: If you are storing keys in a different database, this schema file creates the schema for the key store data.

sm_mssql_logs.sql

Creates the schema for CA SiteMinder® audit logs.

sm_mssql_ss.sql

Creates the schema for a CA SiteMinder® session store.

Note: If you do not plan on storing Unicode characters in the session store, use this file.

sm_mssql_ss.sql.unicode

Creates the schema for the CA SiteMinder® session store.

Note: If you plan on storing Unicode characters in the session store, use this file.

smsampleusers_sqlserver.sql

Creates the schema for the CA SiteMinder® sample users database and populates the database with sample users.

The following SQL Server schema file is provided in *siteminder_home*\xps\db:

SQLServer.sql

Creates the XPS schema for a policy store.

Oracle Schema Files

The following Oracle schema files are provided in the *siteminder_home*\db\SQL directory.

siteminder_home

Specifies the Policy Server installation path.

sm_oracle_ps.sql

Creates the schema for a policy store and key store.

Note: If you are storing keys in a different database, this schema file creates the schema for the key store data.

sm_oracle_logs.sql

Creates the schema for CA SiteMinder® audit logs.

sm_oracle_ss.sql

Creates the schema for a CA SiteMinder® session store.

smsampleusers_oracle.sql

Creates the schema for a CA SiteMinder® sample users database and populates the database with sample users.

The following Oracle schema file is provided in the *policy_server_home*\xps\db directory.

Oracle.sql

Creates the XPS schema for a policy store.

Configure a MySQL Policy Store

A MySQL policy store can also function as:

- A key store
- An audit logging database

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

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

Gather Database Information

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

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

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

How to Configure the Policy Store

You can configure MySQL Server as a policy store.

Note: Gather the required database information before beginning the policy store setup.

Follow these steps:

1. Verify that MySQL is installed using the Latin1 or UTF8 character set. Use the UTF8 character set to support Unicode characters.

   Note: If MySQL is not installed using one of these character sets, reinstall MySQL with the appropriate character set before configuring the CA SiteMinder® data store.

2. Confirm that the MySQL database acting as the policy store is accessible from the Policy Server host system.

3. Create the database instance for the CA SiteMinder® data store, using the vendor–specific user interface.

   - To create a database instance for Unicode characters, use the character set and collation for UTF8.
   - To create a database instance for non-Unicode characters, use the character set and collation for Latin1.

4. Create the CA SiteMinder® schema.

5. Configure a MySQL data source for CA SiteMinder®.
   - (Windows) Create a MySQL data source.
   - (UNIX) Create a MySQL data source on UNIX systems.
   - (UNIX) Configure the MySQL wire protocol driver.
6. Point the Policy Server to the database.
7. Set the CA SiteMinder® superuser password.
8. Import the policy store data definitions.
9. Import the default policy store objects.
10. Restart the Policy Server.
11. Prepare for the Administrative UI registration.

Create the CA SiteMinder® Schema

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

Follow these steps:

1. Start the Query Browser and log in as the person who administers the Policy Server database.
2. Select the database instance from the database list.
3. Navigate to the following location:

   siteminder_home\db\tier2\MySQL.

   siteminder_home

   Specifies the Policy Server installation path.
4. Open *one* of the following files in a text editor:
   - To store Unicode characters in the policy store, open sm_mysql_ps.sql.unicode.
   - To store non-Unicode characters in the policy store, open sm_mysql_ps.sql.
5. Locate the following lines in the sm_mysql_ps file:

   ```
   DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
   CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
   ```
6. Replace each instance of 'databaseName' with the name of the database functioning as the policy store.
7. After you replace the databaseName instances, copy the contents of the entire file.
8. Paste the file contents into a query and execute the query.

   The policy and key store schema are added to the database.

9. Navigate to the following location:

   siteminder_home\xps\db\Tier2DirSupport\MySQL

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

    - To store Unicode characters in the policy store, open MySQL.sql.unicode.
    - To store non-Unicode characters in the policy store, open MySQL.sql.

11. Paste the schema from the appropriate MySQL file into a query and execute the query.

    The policy store schema is extended.

12. To use the policy store as an audit logging database, repeat steps three and four but use the following logging schema file:

    sm_mysql_logs.sql

    The database can store CA SiteMinder® data.

    Note: You are not required to configure the policy store to store more CA SiteMinder® data. You can configure individual databases to function as a separate audit log database, key store, and session store.

Configure a MySQL Data Source for CA SiteMinder®

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

Note: If you are using MySQL 5.1.x, ensure that you assign the TRIGGER permission to the user name that is used to create the DSN.

Create a MySQL Data Source on Windows

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

Follow these steps:

1. Log in to the Policy Server host system.
2. Do one of the following steps:

   - If you are using a supported 32–bit Windows operating system, click Start and select Programs, Administrative Tools, ODBC Data Sources.
   - If you are using a supported 64–bit Windows operating system:

     a. Navigate to the *install_home*\Windows\SysWOW64.

     b. Double–click odbcad32.exe.

   The ODBC Data Source Administrator appears.

3. Click System DSN.

   System Data Sources lists all available data sources.

4. Click Add.

   The Create New Data Source dialog appears.

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

   The ODBC MySQL Wire Protocol Driver Setup dialog appears.

6. Complete the following steps in the General tab:

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

      Example:

      ```
      CA SiteMinder® MySQL Wire Data Source
      ```

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

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

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

7. Click Test Connect.

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

8. Click OK.

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

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

Create a MySQL Data Source on UNIX Systems

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

siteminder_home

Specifies the Policy Server installation path.

This system_odbc.ini file contains all of the names of the available ODBC data sources and the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for CA SiteMinder®.

The first section of the system_odbc.ini file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the “=” refers to a subsequent section of the file describing each individual data source. After the “=” is a comment field.

Note: If you modify of the first line of data source entry, which is [CA SiteMinder® Data Source], take note of the value. The value is required when you configure the database as a policy store.

Each data source has a section in the system_odbc.ini file describing its attributes. The first attribute is the ODBC driver that is loaded when CA SiteMinder® uses this data source. The remaining attributes are specific to the driver.

Adding a MySQL Server Data source involves:

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

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

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

Create the MySQL Wire Protocol Driver

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

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

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

These files are located in *siteminder_home*/db

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

[SiteMinder Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

Follow these steps:

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

   ```
   SiteMinder Data Source=DataDirect 7.1 MySQL Wire Protocol
   ```

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

   ```
   Driver=nete_ps_root/odbc/lib/NSmysql27.so
   Description=DataDirect 7.1 MySQL Wire Protocol
   Database=database_name
   HostName=host_name
   LogonID=root_user
   Password=root_user_password
   PortNumber=mysql_port
   ```

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

   nete_ps_root

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

   Example: /export/smuser/siteminder

   database_name

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

   host_name

   Specifies the name of the MySQL database host system.

   root_user

   Specifies the login ID of the MySQL root user.

root_user_password

Specifies the password for the MySQL root user.

mysql_port

Specifies the port on which the MySQL database is listening.

4. Save the file.

   The wire protocol driver is configured.

Point the Policy Server to the Database

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

Follow these steps:

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

   `ODBC`

3. Select the following value from the Database list:

   `Policy Store`

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

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

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

   `Key Store`

9. Select the following value from the Storage list:

   `ODBC`

10. Select the following option:

    `Use the Policy Store database`

11. Select the following value from the Database list:

    `Audit Logs`

12. Select the following value from the Storage list:

    `ODBC`

13. Select the following option:

    `Use the Policy Store database`

14. Click Apply to save the settings.

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

16. Click OK.

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

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

`siteminder`

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

Limits:

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

Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

     Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

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

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

   passphrase

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

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

   -adminui–setup

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

   -t *timeout*

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

   Unit of measurement: minutes

   Default: 240 (4 hours)

   Minimum Limit: 15

   Maximum Limit: 1440 (24 hours)

   -r *retries*

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

   Default: 1

   Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Configure a SQL Server Policy Store

A single SQL Server database can function as a:

- policy store
- key store
- logging database

  Note: Store CA SiteMinder® session information in a separate database. Do not use the policy store to store session information.

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

Consider the following items:

- You can configure a SQL Server policy store manually or you can use the Policy Server installer to configure the policy store automatically.
- The database must be installed on a Windows system. Additionally, the CA SiteMinder® schema files are installed with the Policy Server. If the Policy Server is installed on a UNIX system, copy the schema files from the *policy_server_home*/db/SQL directory to a temporary directory on the Windows system.

Gather Database Information

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

Note: Information prefixed with (W) indicates that the information is only required if the Policy Server is installed on a Windows system; (U) indicates that the information is only required if the Policy Server is installed on a UNIX system. Different information is required when configuring the SQL Server data source.

Gather the following information before configuring the policy store or any other type of CA SiteMinder® data store. You can use the SQL Server Information Worksheet to record your values.

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

Database instance name

Determine the name of the database instance that is to function as the policy store or data store.

Administrative account name and password

Determine the user name and password of an account with privileges to create, read, modify, and delete objects in the database.

(W) Data source name

Determine the name you will use to identify the data source.

Example: SM SQL Server Wire DS.

(W) SQL Server name

Determine the name of the SQL Server database that contains the instance that is to function as the policy store.

(U) Policy Server root

Determine the explicit path to where the Policy Server is installed.

(U) IP Address

Determine the IP Address of the SQL Server database.

How to Configure the Policy Store

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

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

1. Be sure that the SQL Server database instance that is to contain the CA SiteMinder® data is accessible from the Policy Server system.
2. Using the SQL Server Enterprise Manager, create the database instance for the CA SiteMinder® data store.

   Example:

   ```
   smdatastore
   ```

3. Create the CA SiteMinder® Schema.

4. Configure a SQL Server data source for CA SiteMinder®.
   - (Windows) Create a SQL Server data source.
   - (UNIX) Create a SQL Server data source on UNIX systems.
   - (UNIX) Configure the SQL Server wire protocol driver.
5. Point the Policy Server to the database.
6. Set the CA SiteMinder® superuser password.
7. Import the policy store data definitions.
8. Import the default CA SiteMinder® objects.
9. Restart the Policy Server.
10. Prepare for the Administrative UI registration.

Create the CA SiteMinder® Schema

You create the CA SiteMinder® schema so that SQL Server database can store policy, key, and audit logging information.

The following warnings are displayed when running the policy store and audit logging schema files. The warnings do not affect the policy store configuration:

- Warning: The table 'smvariable5' has been created but its maximum row size (8746) exceeds the maximum number of bytes per row (8060). INSERT or UPDATE of a row in this table will fail if the resulting row length exceeds 8060 bytes.
- Warning: The table 'smodbcquery4' has been created but its maximum row size (64635) exceeds the maximum number of bytes per row (8060). INSERT or UPDATE of a row in this table will fail if the resulting row length exceeds 8060 bytes.
- Warning: The table 'smaccesslog4' has been created but its maximum row size (9668) exceeds the maximum number of bytes per row (8060). INSERT or UPDATE of a row in this table will fail if the resulting row length exceeds 8060 bytes.

Follow these steps:

1. Start the Query Analyzer and log in as the person who administers the Policy Server database.
2. Select the database instance from the database list.
3. Open sm_mssql_ps.sql in a text editor and copy the contents of the entire file.
4. Paste the schema from sm_mssql_ps.sql into the query and execute the query.

   The policy and key store schema is added to the database.
5. Open SQLServer.sql in a text editor and copy the contents of the entire file.

6. Paste the schema from SQLServer.sql into the query, and execute the query.

   The policy store schema is extended.

7. Repeat steps three and four to use the policy store as an audit logging database. Use the following schema file:

   sm_mssql_logs.sql

   Note: You are not required to configure the policy store to store additional CA SiteMinder® data. You can configure individual databases to function as a separate audit log database, key store, and session store.

   The database can store CA SiteMinder® data.

Configure a SQL Server Data Source for CA SiteMinder®

If you are using ODBC, you need to configure a data source to let CA SiteMinder® communicate with the CA SiteMinder® data store.

More information:

SQL Server Authentication Mode Considerations (see page 288)

SQL Server Authentication Mode Considerations

CA SiteMinder® data sources do not support Windows authentication. Configure the CA SiteMinder® data source with the credentials of a user that is stored in the database.

Note: For more information about SQL Server authentication modes, see the vendor–specific documentation.

Create a SQL Server Data Source on Windows

ODBC requires that you configure a data source for the SQL Server wire protocol.

Note: This procedure only applies if the Policy Server is installed on a Windows System.

Follow these steps:

1. Complete one of the following steps:

   - If you are using a supported 32–bit Windows operating system, click Start and select Programs, Administrative Tools, ODBC Data Sources.
   - If you are using a supported 64–bit Windows operating system:

     a. Navigate to C:\Windows\SysWOW64.

     b. Double–click odbcad32.exe.

   The ODBC Data Source Administrator appears.

2. Click the System DSN tab.

   System data source settings appear.

3. Click Add.

   The Create New Data Source dialog appears.

4. Select CA SiteMinder® SQL Server Wire Protocol and click Finish.

   The ODBC SQL Server Wire Protocol Driver Setup dialog appears.

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

   Example: CA SiteMinder® Data Source.

   Note: Take note of your data source name. This information is required as you configure your database as a policy store.

6. Enter the name of the SQL Server host system in the Server field.

7. Enter the database name in the Database Name field.

8. Click Test.

   The connection settings are tested and a prompt appears specifying that the connection is successful.

9. Click OK.

   The SQL Server data source is configured and appears in the System Data Sources list.

Create a SQL Server Data Sources on UNIX Systems

The CA SiteMinder® ODBC data sources are configured using a system_odbc.ini file, which you create by renaming sqlserverwire.ini, located in *policy_server_installation*/db, to system_odbc.ini. This system_odbc.ini file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for CA SiteMinder®.

The first section of the system_odbc.ini file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [CA SiteMinder® Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the system_odbc.ini file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by CA SiteMinder®. The remaining attributes are specific to the driver.

Adding a MS SQL Server Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the system_odbc.ini file if you create a new service name or want to use a different driver. You should have entries for the Oracle or SQL drivers under [CA SiteMinder® Data Source].

Again, to configure a MS SQL Server data source, you must first create a system_odbc.ini file in the *policy_server_installation*/db directory. To do this, you need to rename sqlserverwire.ini, located in *policy_server_installation*/db, to system_odbc.ini.

Configure the SQL Server Wire Protocol Driver

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

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

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

These files are located in *siteminder_home*/db

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

[SiteMinder Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

Follow these steps:

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

   ```
   SiteMinder Data Source=DataDirect 7.1 SQL Server Wire Protocol
   ```

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

   ```
   Driver=nete_ps_root/odbc/lib/NSsqls27.so
   Description=DataDirect 7.1 SQL Server Wire Protocol
   Database=SiteMinder Data
   Address=myhost, 1433
   QuotedId=No
   AnsiNPW=No
   ```

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

   nete_ps_root

   Specifies the explicit path of the Policy Server installation, rather than a path with an environment variable.

   Example: export/smuser/siteminder

   CA SiteMinder® Data

   Specifies the SQL Server database instance name.

   myhost

   Specifies the IP Address of the SQL Server database.

   1433

   Represents the default listening port for SQL Server.

4. If you are using Microsoft SQL Server 2008 to function as any CA SiteMinder® store, edit the [ODBC] section as follows:

   ```
   TraceFile=nete_ps_root/db/odbctrace.out
   TraceDll=nete_ps_root/odbc/lib/NStrc27.so
   InstallDir=nete_ps_root/odbc
   ```

   nete_ps_root

   Specifies the explicit path to the Policy Server installation directory. This path cannot contain an environment variable.

5. Save the file.

   The wire protocol driver is configured.

Point the Policy Server to the Database

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

Follow these steps:

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

   `ODBC`

3. Select the following value from the Database list:

   `Policy Store`

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

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

7. Click Apply to save the settings.

8. Select the following value from the Database list:

   `Key Store`

9. Select the following value from the Storage list:

   `ODBC`

10. Select the following option:

    `Use the Policy Store database`

11. Select the following value from the Database list:

    `Audit Logs`

12. Select the following value from the Storage list:

    `ODBC`

13. Select the following option:

    `Use the Policy Store database`

14. Click Apply to save the settings.

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

16. Click OK.

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

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

`siteminder`

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

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

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

   Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

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

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

   passphrase

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

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

   -adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Configure an Oracle Policy Store

A single Oracle database can function as a:

- policy store
- key store
- logging database

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

You can configure an Oracle policy store manually or use the Policy Server installer to configure the policy store automatically.

Prerequisites for an Oracle 10g Database

After installing the Oracle 10g database, complete the following prerequisites:

- Create a table space for the policy store.
- Create a user with appropriate privileges to manage this table space in the database.

Create an Oracle 10g Table Space for the Policy Store

Creating a table space for the policy store is a prerequisite for an Oracle 10g database only.

To create an Oracle 10g table space for the policy store

1. In the Oracle Enterprise Manager 10g Database Control, log in as the SYSDBA user with appropriate privileges to manage the Oracle database.
2. On the Oracle global database's configuration screen, select Administration, Tablespaces.
3. On the Tablespaces screen, click Create.
4. On the Create Tablespaces screen, enter a table space name, and click ADD.

   Example: NETE_TB
5. On the Create Tablespaces: Add Datafile screen:
   a. Enter a file name.

      Example: NETE_TB

   b. Specify the file size.

      Example: 100 MB

   c. Click Continue.

   Oracle creates the table space and displays it on the Tablespaces screen.

Complete the prerequisites by creating a user to manage the table space for the policy store.

More Information:

SM--Create an Oracle 10g User to Manage the Policy Store's Table Space (see page 300)

SM--Create an Oracle 10g User to Manage the Policy Store's Table Space

Creating a user to manage table space for the policy store is a prerequisite for an Oracle 10g database only.

To create a user to manage table space for the policy store

1. On the Oracle global database's configuration screen, select Administration, Users.
2. On the Create Tablespaces screen, click Create.

3. On the Create User screen, enter the:
   - Name for the user.

     Example: NETE
   - Password for the user.
   - Default Tablespace that you created.
   - Temporary tablespace.

     Example: TEMP
4. Click Roles.
5. Select Modify.
6. On the Modify Roles screen:
   a. Select CONNECT and RESOURCE as a roles for this user.
   b. Click Apply.
7. Start sqlplus in a command window, by entering:
   a. sqlplus
   b. the credentials for the policy store user created on the Create User screen.

   You have completed the prerequisites for an Oracle 10g database, and can now configure a CA SiteMinder® data store for the database.

Gather Database Information

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

Information prefixed with (U) indicates that the information is only required if the Policy Server is installed on a UNIX system. This information is required when configuring Oracle data source for UNIX.

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

Required Information

Gather the following required information before configuring a supported Oracle or Oracle RAC database as a policy store or any other type of CA SiteMinder® data store:

- (U) **Policy Server installation path**—Identify the explicit path to where the Policy Server is installed.
- **Data source**—Determine the name you will use to identify the Oracle data source.

  Example: SM Oracle Server Wire DS.
- **Database administrative account**—Determine the user name of an account with privileges to create, read, modify, and delete objects in the database.

  Note: Ensure the administrative account does not have the DB role. Audit-based reports will not return correct results if the administrative account has the DB role.
- **Database administrative Password**—Determine the password for the Administrative account.

Oracle Database Information

Gather the following information only if you are configuring a supported Oracle database as a policy store or any other type of CA SiteMinder® data store:

- **Oracle machine name**—Determine the name of the machine on which the Oracle database is installed.
- **Oracle instance service name**—Determine the service name of the database instance to which you will connect. The tnsnames.ora file specifies service names.
- **Oracle port number**—Determine the port number on which the Oracle database is listening.

Oracle RAC Database (without SCAN) Information

Gather the following information if you are configuring a supported Oracle RAC database (without SCAN functionality configured) as a policy store or any other CA SiteMinder® data store:

- **Oracle RAC system service name—**Determine the service name for the entire system.

  Example: In the following tnsnames.ora file, SMDB is the service name for the entire system:

  ```
  SMDB=
  (Description =
  (ADDRESS = PROTOCOL = TCP)(HOST = nete_servername1)(PORT=1521
  (ADDRESS = PROTOCOL = TCP)(HOST = nete_servername2)(PORT=1521)
  (ADDRESS = PROTOCOL = TCP)(HOST = nete_servername3)(PORT=1521))
  (LOAD_BALANCE = yes)
  (CONNECT_DATA=
  (SERVER = DEDICATED)
  (SERVER_NAME = SMDB))
  )
  ```

- **Oracle RAC node service names**—Determine the service names for each node in the system.
- **Oracle RAC node IP addresses**—Determine the IP Address of each node in the Oracle RAC system.

  Note: If you are using Oracle RAC 10g, determine the virtual IP address of each node in the system.

- **Oracle RAC node port numbers**—Determine the port number for each node in the Oracle RAC system.

Oracle RAC Database (Using SCAN) Information

The Oracle RAC Single Client Access Name (SCAN) feature provides a single name for clients to access any Oracle Database running in a cluster.

Gather the following information if you are configuring an Oracle RAC database with SCAN functionality as a policy store or any other CA SiteMinder® data store:

- **Oracle RAC system service name**—Determine the service name for the entire system.

  Example: In the following tnsnames.ora file, SMDB is the service name for the entire system:

  ```
  SMDB=
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = clus-scan.example.com)(PORT = 1521))
      (CONNECT_DATA =
        (SERVER = DEDICATED)
        (SERVICE_NAME = SMDB)
      )
    )
  ```

- **Oracle RAC SCAN Address**—Determine the FQDN of the Oracle RAC system SCAN.
- **Oracle RAC SCAN port number**—Determine the port number for the Oracle RAC system SCAN.

How to Configure the Policy Store

To configure a single Oracle database as a policy store, key store, and logging database, complete the following procedures:

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

1. Be sure that the Oracle database instance that is to contain the CA SiteMinder® data is accessible from the Policy Server system. Test the communication using tnsping or sqlplus.
2. Create the CA SiteMinder® Schema.
3. Configure an Oracle data source for CA SiteMinder®:
   - (Windows) Create an Oracle data source on Windows systems.
   - (Windows) Create an Oracle RAC data source on Windows systems.
   - (UNIX) Create an Oracle data source on UNIX.
   - (UNIX) Configure the wire protocol driver.
   - (UNIX) Configure the Oracle wire protocol driver.
   - (UNIX) Configure the Oracle RAC wire protocol driver.
4. Point the Policy Server to the database.

5. Set the CA SiteMinder® superuser password.
6. Import the policy store data definitions.
7. Import the default policy store objects.
8. Restart the Policy Server.
9. Prepare for the Administrative UI registration.

Create the CA SiteMinder® Schema

You create the CA SiteMinder® schema so a single Oracle database can store policy, key, and audit logging information.

Follow these steps:

1. Log in to Oracle with sqlplus or some other Oracle utility as the user who administers the Policy Server database information.

   Note: We recommend that you do not create the CA SiteMinder® schema with the SYS or SYSTEM users. If necessary, create an Oracle user, such as SMOWNER, and create the schema with that user.

2. Import the following script:

   ```
   $NETE_PS_ROOT/db/sql/sm_oracle_ps.sql
   ```

   Note: Environment variables may not function in the SQL utility of Oracle. If you experience problems importing the script using the utility, specify an explicit path.

   The policy store and key store schema is added to the database.

3. Import the following script

   ```
   $NETE_PS_ROOT/xps/db/Oracle.sql
   ```

   The policy store schema is extended.

4. Import the following script to use the policy store as an audit logging database:

   ```
   sm_oracle_logs.sql.
   ```

   Note: You are not required to configure the policy store to store additional CA SiteMinder® data. You can configure individual databases to function as a separate audit log database, key store, and session store.

   The database can store CA SiteMinder® data.

Configure an Oracle Data Source for CA SiteMinder®

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

Create an Oracle Data Source on Windows

Create an ODBC data source for an Oracle database.

Follow these steps:

1. Do one of the following:

   - If you are using a supported 32–bit Windows operating system, click Start and select Programs, Administrative Tools, ODBC Data Sources.

   - If you are using a supported 64–bit Windows operating system:

     a. Navigate to the *install_home*\Windows\SysWOW64.

     b. Double–click odbcad32.exe

   The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

   The Create New Data Source dialog appears

3. Select CA SiteMinder® Oracle Wire Protocol, and click Finish.

   The ODBC Oracle Wire Protocol Driver Setup dialog appears. The General tab is pulled to the front.

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

   Note: Record this name. You will need the data source name when pointing the Policy Server to the database.

5. Enter the machine name where the Oracle database is installed in the Host Name field.

6. Enter the port number where the Oracle database is listening on the machine in the Port Number field.

7. Enter the name of the Oracle instance to which you want to connect in the SID field.

   Note: The service name is specified in the tnsnames.ora file. The SID is the system identifier for the database instance. The tnsnames.ora file contains service names and details that Oracle uses to identify and connect to Oracle instances.

   Example: if the tnsnames.ora file contains the following entry for an Oracle instance, you enter instance1 in the SID field:

   ```
   instance1 =
       (Description=
       (Address = (PROTOCOL = TCP)(Host = myhost)(Port=1521))
       (Connect_DATA_ = (SID = SIDofinstance1))
       )
   ```

8. Click Test Connection.

   The connection settings are tested and a prompt appears specifying that the connection is successful.

9. Click OK.

   The Oracle data source is configured for the wire protocol driver.

Create an Oracle RAC (no SCAN) Data Source on Windows

Create an ODBC data source for an Oracle RAC database that does not use the SCAN feature.

Follow these steps:

1. Do one of the following:

   - If you are using a supported 32–bit Windows operating system, click Start and select Programs, Administrative Tools, ODBC Data Sources.

   - If you are using a supported 64–bit Windows operating system:

     a. Navigate to the C:\Windows\SysWOW64.

     b. Double–click odbcad32.exe

   The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

   The Create New Data Source dialog appears.

3. Select CA SiteMinder® Oracle Wire Protocol, and click Finish.

   The ODBC Oracle Wire Protocol Driver Setup dialog appears. The General tab is pulled to the front.

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

   Note: Record this name. You will need the data source name when pointing the Policy Server to the database.

5. Enter the IP Address of the first node in the Oracle RAC system in the Host field.

   Oracle RAC 10g: Enter the virtual IP Address.

6. Enter the service name for the entire Oracle RAC system in the Service Name field.

   Example: In the following tnsnames.ora file, the SMDB value is the service name for the entire Oracle RAC system, which contains 3 nodes:

   ```
   SMDB=
       (Description =
   (ADDRESS = (Protocol = TCP)(HOST = nete_servername1)(PORT = 1521))
   (ADDRESS = (Protocol = TCP)(HOST = nete_servername2)(PORT = 1521))
   (ADDRESS = (Protocol = TCP)(HOST = nete_servername3)(PORT = 1521))
   (LOAD_BALANCE = yes)
   (CONNECT_DATA =
   (SERVER = DEDICATED)
   (SERVICE_NAME = SMDB)
   )
   ```

7. Click the Failover tab.

   Failover settings appear.

8. Specify the host name or virtual IP Address, port number, and service name for the remaining Oracle RAC nodes in the environment in the Alternate Servers field.

   Note: The ServiceName is the service name for the entire Oracle RAC system.

9. Specify the AlternateServers to provide connection failover to the other Oracle nodes if the primary server is not accepting connections. The entry should have the following format:

   (HostName=nete_servername2:PortNumber=1521:ServiceName=nete_servicename[,...])

10. Select LoadBalancing.

11. Click OK

    The Oracle RAC data source is configured for the wire protocol driver.

Create an Oracle RAC SCAN Data Source on Windows

Create an ODBC data source for an Oracle RAC database that uses the SCAN feature.

Follow these steps:

1. Do one of the following:

   - If you are using a supported 32–bit Windows operating system, click Start and select Programs, Administrative Tools, ODBC Data Sources.
   - If you are using a supported 64–bit Windows operating system:

     a. Navigate to the C:\Windows\SysWOW64.

     b. Double–click odbcad32.exe

   The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

   The Create New Data Source dialog appears.

3. Select CA SiteMinder Oracle Wire Protocol, and click Finish.

   The ODBC Oracle Wire Protocol Driver Setup dialog appears. The General tab is pulled to the front.

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

   Note: Record this name. You will need the data source name when pointing the Policy Server to the database.

5. Enter the FQDN or IP Address of the SCAN in the Host field.

6. Enter the port number of the SCAN in the Port Number field.

7. Enter the service name for the entire Oracle RAC system in the Service Name field.

   Example: In the following tnsnames.ora file, the SMDB value is the service name for the entire Oracle RAC system, which contains the SCAN:

   ```
   SMDB =
     (DESCRIPTION =
       (ADDRESS = (PROTOCOL = TCP)(HOST = clus-scan.rac.com)(PORT = 1521))
       (CONNECT_DATA =
         (SERVER = DEDICATED)
         (SERVICE_NAME = ORCL)
       )
     )
   ```

8. Click OK

   The Oracle RAC data source is configured for the wire protocol driver.

Create an Oracle Data Source on UNIX Systems

You configure the names of available ODBC data sources and the attributes that are associated with these data sources in the system_odbc.ini file.

To create the system_odbc.ini file:

1. Navigate to *policy_server_installation*/db
2. Rename oraclewire.ini to "system_odbc.ini".

Customize the system_odbc.ini file for each site. You can also add more data sources to this file, such as defining extra ODBC user directories for CA SiteMinder®.

The first section of the system_odbc.ini file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the “=” refers to a subsequent section of the file describing each individual data source. After the “=” is a comment field.

Note: If you modify of the first line of the data source entry ([CA SiteMinder® Data Source]), take note of the change. This value is required to configure your ODBC database as a policy store.

Each data source has a section in the system_odbc.ini file describing its attributes. The first attribute is the ODBC driver to be loaded when CA SiteMinder® uses this data source. The remaining attributes are specific to the driver.

To add an Oracle Data source:

1. Define a new data source name in the [ODBC Data Sources] section of the file.
2. Add a section that describes the data source using the same name as the data source.

To create a service name or use a different driver, edit the system_odbc.ini file. Entries for the SQL Server or Oracle drivers belong under [CA SiteMinder® Data Source].

Configure the Oracle Wire Protocol Driver

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

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

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

These files are located in *siteminder_home*/db

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

[SiteMinder Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

Follow these steps:

1. Open the system_odbc.ini file.
2. Depending on the data source you are configuring, edit the applicable data source sections with the following information:

```
Driver=nete_ps_root/odbc/lib/NSora27.so
Description=DataDirect 7.1 Oracle Wire Protocol
LoginID=uid
Password=pwd
HostName=nete_servername
PortNumber=1521
SID=nete_serverid
CatalogOptions=0
ProcedureResults=0
EnableDisableParam=0
EnableStaticCursorsForLongData=0
ApplicationUsingThreads=1
```

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

nete_ps_root

Specifies the explicit path of the Policy Server installation.

uid

Specifies the user name of the database account that has full access rights to the database.

pwd

Specifies the password for the database account that has full access rights to the database.

nete_servername

Specifies the name of the Oracle database host system.

nete_serverid

Specifies the Oracle instance service name (SID). The SID is the system identifier for the database instance.

Example: In the following sample tnsnames.ora file, the value instance1 is the SID.

```
instance1 =

(Description =

(ADDRESS = (Protocol = TCP)(Host = myhost)(Port = 1521)

(CONNECT_DATA = (SID = instance1))

)
```

3. Save the file.

   The Oracle wire protocol driver is configured.

Configure the Oracle Wire Protocol Driver for Oracle RAC without SCAN

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

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

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

These files are located in *siteminder_home*/db

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

[SiteMinder Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

Follow these steps:

1. Open the system_odbc.ini file.
2. Depending on the data source you are configuring, edit the applicable data source sections with the following information:
   - Add ServiceName=*nete_servicename*
   - Add AlternateServers=
   - Add Loadbalancing=1
   - Remove or comment SID=nete_serverid

   The modified text for the data source should appear as follows:

   ```
   Driver=nete_ps_root/odbc/lib/NSora27.so
   Description=DataDirect 7.1 Oracle Wire Protocol
   Logon=uid
   Password=pwd
   HostName=nete_servername1
   PortNumber=1521
   ServiceName=nete_servicename
   CatalogOptions=0
   ProcedureRetResults=0
   EnableDescribeParam=0
   EnableStaticCursorsForLongData=0
   ApplicationUsingThreads=1
   AlternateServers=
   LoadBalancing=1
   ```

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

nete_ps_root

Specifies an explicit path to the directory where Policy Server is installed.

uid

Specifies the user name of the database account that has full access rights to the database.

pwd

Specifies the password for the database account that has full access rights to the database.

nete_servername1

Specifies the IP Address of the first Oracle RAC node.

(Oracle 10g) Specifies the virtual IP Address of the first Oracle RAC node.

nete_servicename

Specifies the Oracle RAC system service name for the entire RAC system.

AlternateServers=

If the primary server is not accepting connections, specifies the connection failover to the other Oracle nodes.

Example:
(HostName=nete_servername2:PortNumber=1521:ServiceName=nete_servicename[,...])

LoadBalancing=1

Turns on client load balancing, which helps to distribute new connections to keep RAC nodes from being overwhelmed with connection requests. When enabled, the order in which primary and alternate database servers are accessed is random.

3. Save the file.

   The Oracle wire protocol driver is configured.

Point the Policy Server to the Database

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

Follow these steps:

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

   `ODBC`

3. Select the following value from the Database list:

   `Policy Store`

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

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

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

6. Specify the maximum number of database connections that are allocated to CA SiteMinder®.

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

7. Click Apply to save the settings.

8. Select the following value from the Database list:

   `Key Store`

9. Select the following value from the Storage list:

   `ODBC`

10. Select the following option:

    `Use the Policy Store database`

11. Select the following value from the Database list:

    `Audit Logs`

12. Select the following value from the Storage list:

    `ODBC`

13. Select the following option:

    `Use the Policy Store database`

14. Click Apply to save the settings.

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

16. Click OK.

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

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

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

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

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

   siteminder_home

   Specifies the Policy Server installation path.

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

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

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

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

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

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:
   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Restart the Policy Server

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

Follow these steps:

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

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

   The Policy Server starts as indicated by the green stoplight.

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

Prepare for the Administrative UI Registration

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

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

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui–setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 15

Maximum Limit: 1440 (24 hours)

-r *retries*

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

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log path*

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

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

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

Configure an IBM DB2 Policy Store

A single IBM DB2 database can function as a:

- policy store
- key store
- logging database

  Note: Store CA SiteMinder® session information in a separate database. Do not use the policy store to store session information.

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

Gather Database Information

Configuring a single IBM DB2 database to function as a policy store or any other type of CA SiteMinder® data store requires specific database information.

Consider the following items:

- Information that is prefixed with a W represents a Windows requirement.
- Information that is prefixed with a U represents a UNIX requirement.

Gather the following information before configuring the policy store or any other type of CA SiteMinder® data store. You can use the IBM DB2 Information Worksheet to record your values.

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

- **Database instance name** —Determine the name of the database instance that is to function as the policy store or data store.
- **Administrative account** —Determine the user name of an account with privileges to create, read, modify, and delete objects in the database.
- **Administrative password** —Determine the password for the Administrative account.
- **IP address**—Determine the IP address of the database host system.
- **Tcp port**—Determine the port on which the database is listening.
- (W) **Data source name** —Determine the name that is to identify the data source.
- (U) **Policy Server root** —Determine the explicit path to where the Policy Server is installed.
- (U) **Package** —Determine the name of the package that is to process dynamic SQL.
- (U) **Package owner**—Determine the AuthID assigned to the package. The AuthID must have the authority to execute all SQLs in the package.
- (U) **Grant AuthID**—If you want to restrict execute privileges for the package, determine the AuthID that is granted execute permissions for the package.

  Default wire protocol setting: Public

(U) **Isolation level**—Determine the method by which the system acquires and releases locks.

Default wire protocol setting: CURSOR_STABILTY

- (U) **Dynamic sections**—Determine the number of sections that the wire protocol driver package can prepare for a single user.

  Default wire protocol setting: 100

How to Configure the Policy Store

Complete the following procedures to configure a single IBM DB2 database as a policy store, key store, and logging database.

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

1. Be sure that the IBM DB2 database instance that is to contain the CA SiteMinder® data is accessible from the Policy Server system.
2. Verify the following database instance settings:
   - If you are configuring a policy store only, the tablespace page size (page_size) and the buffer pool page size settings must each be set to at least 16k.

     The default DB2 value for each setting is not sufficient for the CA SiteMinder® policy store schema.
   - If you are configuring a policy store and an audit store, the table space page size (page_size) and the buffer pool page size settings must each be set to at least 32k.

     The default DB2 value for each setting is not sufficient for the CA SiteMinder® policy store and audit store schema.
3. Create the CA SiteMinder® schema.
4. Configure a DB2 data source for CA SiteMinder®.
5. Point the Policy Server to the database.
6. Set the CA SiteMinder® superuser password.
7. Import the policy store data definitions.
8. Import the default policy store objects.
9. Restart the Policy Server.
10. Prepare for the Administrative UI registration.

Create the CA SiteMinder® Schema

Follow these steps:

1. Navigate to *siteminder_home*\db\tier2\DB2.

   siteminder_home

   Specifies the Policy Server 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 and key store schema is created in the DB2 database.

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

   sm_db2_logs.sql

   Specifies the schema for an audit log store in a DB2 database. For 12.52 edit this script (see page 344) before creating an audit store.

   smsampleusers_db2.sql

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

   The corresponding CA SiteMinder® schema is created in the DB2 database.

   Note: Using the policy store to store key, audit, and sample users is optional. You can use separate databases to function as these types of CA SiteMinder® data stores individually.

5. Copy the following schema file to the DB2 host system:

   siteminder_home\xps\db\DB2.sql

   siteminder_home

   Specifies the Policy Server installation path.

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

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

   path

   Specifies the path to the DB2 schema file.

   The policy store schema is created.

Configure an IBM DB2 Data Source for CA SiteMinder®

If you are using ODBC, configure a data source to let CA SiteMinder® communicate with the CA SiteMinder® data store.

Create a DB2 Data Source on Windows Systems

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

Follow these steps:

1. Complete one of the following steps:

   - If you are using a supported 32–bit Windows operating system, click Start and select Programs, Administrative Tools, ODBC Data Sources.
   - If you are using a supported 64–bit Windows operating system:

     a. Navigate to the *install_home*\Windows\SysWOW64.

     b. Double–click odbcad32.exe

   The ODBC Data Source Administrator appears.

2. Click the System DSN tab and click Add.

3. Scroll down and select CA SiteMinder® DB2 Wire Protocol and click Finish.

4. In the ODBC DB2 Wire Protocol Driver Setup dialog, under the General tab, complete the following steps:

   a. In the Data Source Name field, enter any name.

      Example:

      ```
      SiteMinder DB2 Wire Data Source
      ```

   b. (Optional) In the Description field, enter a description of the DB2 wire protocol data source.

   c. In the IP Address field, enter the IP Address where the DB2 database is installed.

   d. In the Tcp Port field, enter the port number where DB2 is listening on the system.

   e. Click Test Connect.

      The connection is tested.

5. Click OK.

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

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

Create a DB2 Data Source on UNIX Systems

The SiteMinder ODBC data sources are configured using a system_odbc.ini file, which you can create by renaming db2wire.ini, located in policy_server_home/db, to system_odbc.ini. This system_odbc.ini file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the system_odbc.ini file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Each data source has a section in the system_odbc.ini file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding a DB2 Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the system_odbc.ini file if you create a new service name or want to use a different driver. You should have entries for the DB2 driver under [SiteMinder Data Source].

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

Note: policy_server_home specifies the Policy Server installation path.

Configure the DB2 Wire Protocol Driver

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

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

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

Point the Policy Server to the Database

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

Follow these steps:

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

   `ODBC`

3. Select the following value from the Database list:

   `Policy Store`

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

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

5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
6. Specify the maximum number of database connections that are allocated to CA SiteMinder®.

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

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

   `Key Store`

9. Select the following value from the Storage list:

   `ODBC`

10. Select the following option:

    `Use the Policy Store database`

11. Select the following value from the Database list:

    `Audit Logs`

12. Select the following value from the Storage list:

    `ODBC`

13. Select the following option:

    `Use the Policy Store database`

14. Click Apply to save the settings.

15. Click Test Connection to verify that the Policy Server can access the policy store.
16. Click OK.

    The Policy Server is configured to use the database as a policy store, key store, and logging database.

Set the CA SiteMinder® Super User Password

The default CA SiteMinder® administrator account is named:

```
siteminder
```

The account has maximum permissions.

We recommend that you do not use the default superuser for day–to–day operations. Use the default superuser to:

- Access the Administrative UI for the first–time.
- Manage CA SiteMinder® utilities for the first–time.
- Create another administrator with superuser permissions.

Follow these steps:

1. Copy the smreg utility to *siteminder_home*\bin.

   siteminder_home

   Specifies the Policy Server installation path.

   Note: The utility is at the top level of the Policy Server installation kit.

2. Run the following command:

   ```
   smreg -su password
   ```

   password

   Specifies the password for the default CA SiteMinder® administrator.

   Limits:

   – The password must contain at least six (6) characters and cannot exceed 24 characters.

   – The password cannot include an ampersand (&) or an asterisk (*).

   – If the password contains a space, enclose the passphrase with quotation marks.

   Note: If you are configuring an Oracle policy store, the password is case–sensitive. The password is not case–sensitive for all other policy stores.

3. Delete smreg from *siteminder_home*\bin. Deleting smreg prevents someone from changing the password without knowing the previous one.

   The password for the default CA SiteMinder® administrator account is set.

Import the Policy Store Data Definitions

Importing the policy store data definitions defines the types of objects that can be created and stored in the policy store.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\xps\dd.

   siteminder_home

   Specifies the Policy Server installation path.

2. Run the following command:

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   Imports the required data definitions.

Import the Default Policy Store Objects

Importing the default policy store objects configures the policy store for use with the Administrative UI and the Policy Server.

Consider the following items:

- Be sure that you have write access to *siteminer_home*\bin. The import utility requires this permission to import the policy store objects.

  siteminder_home

  Specifies the Policy Server installation path.

- Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges. For more information, see the release notes for your CA SiteMinder® component.

Follow these steps:

1. Open a command window and navigate to *siteminder_home*\db.
2. Import one of the following files:

   - To import smpolicy.xml, run the following command:

     ```
     XPSImport smpolicy.xml -npass
     ```

   - To import smpolicy–secure.xml, run the following command:

     ```
     XPSImport smpolicy–secure.xml -npass
     ```

     npass

     Specifies that no passphrase is required. The default policy store objects do not contain encrypted data.

Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The smpolicy–secure file provides more restrictive security settings. For more information, see Default Policy Store Objects Consideration (see page 90).

Note: Importing smpolicy.xml makes available legacy federation and Web Service Variables functionality that is separately licensed from CA SiteMinder®. If you intend on using the latter functionality, contact your CA account representative for licensing information.

Enable the Advanced Authentication Server

Enable the advanced authentication server as part of configuring your Policy Server.

Follow these steps:

1. Start the Policy Server configuration wizard.
2. Leave all the check boxes in the first screen of the wizard *cleared*.
3. Click Next.

   The master key screen appears.
4. Create the master encryption key for the advanced authentication server.

   Note: If you are installing another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
5. Complete the rest of the Policy Server configuration wizard.

   The advanced authentication server is enabled.

Prepare for the Administrative UI Registration

You use the default CA SiteMinder® super user account (siteminder) to log into the Administrative UI for the first–time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components.

You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Consider the following:

- The time from which you supply the credentials to when the initial Administrative UI login occurs is limited to 24 hours. If you do not plan on installing the Administrative UI within one day, complete the following before installing the Administrative UI.
- (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

To prepare for the Administrative UI registration

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   Specifies the password for the default CA SiteMinder® super user account (siteminder).

   Note: If you do not specify the passphrase, XPSRegClient prompts you to enter and confirm one.

   -adminui–setup

   Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

   -t *timeout*

   (Optional) Specifies the allotted time from when you to install the Administrative UI to the time you log in and create a trusted relationship with a Policy Server. The Policy Server denies the registration request when the timeout value is exceeded.

   Unit of measurement: minutes

   Default: 240 (4 hours)

   Minimum Limit: 15

   Maximum Limit: 1440 (24 hours)

   -r *retries*

   (Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect CA SiteMinder® administrator credentials when logging into the Administrative UI for the first–time

   Default: 1

   Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   XPSRegClient supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log into the Administrative UI for the first–time.

How to Store Session Information in IBM DB2

Complete the following procedures to configure an IBM DB2 database as a session store:

1. Be sure that you have gathered the required database information.
2. Create the session store schema.
3. Configure the IBM DB2 data source for CA SiteMinder®.
4. Point the Policy Server to the session store.

More information:

Gather Database Information (see page 322)
Configure an IBM DB2 Data Source for CA SiteMinder® (see page 325)

Create the Session Store Schema

You create the CA SiteMinder® schema so that an IBM DB2 database can store session information.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to *siteminder_home*\db\tier2\DB2.

   siteminder_home

   Specifies the Policy Server installation path.

3. Open the following file and copy the contents to a text editor:

   `sm_db2_ss.sql`

4. Paste the contents into a query and execute the query.

   Note: For more information executing a query, see the IBM documentation.

   The session store schema is added to the database.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can read and store session information.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select Session Server from the Database list.

   Data source settings become active.

3. Enter the name of the data source in the Data Source Information field.

   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.

4. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.

5. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.

6. Click Apply.

   The settings are saved.

7. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

8. Click OK.

   The Policy Server is configured to use the database as a session store.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Session Information in MySQL

Complete the following procedures to configure MySQL as a standalone session store:

1. Be sure that MySQL is installed using the default character set (Latin1). If MySQL was not installed using the default character set, reinstall MySQL before configuring the CA SiteMinder® data store.
2. Gather database information.
3. Create the session store schema.
4. Configure a MySQL data source for CA SiteMinder®.
5. Point the Policy Server to the database.
6. Restart the Policy Server.

More information:

Gather Database Information (see page 272)
Configure a MySQL Data Source for CA SiteMinder® (see page 274)

Create the Session Store Schema

You create the session store schema so the MySQL database can store the session information.

Follow these steps:

1. Log in to the Policy Server host system.

2. Navigate to the following location:

   `siteminder_home\db\tier2\MySQL.`

   siteminder_home

   Specifies the Policy Server installation path.

3. Open the following file in a text editor:

   `sm_mysql_ss.sql`

4. Locate the following lines:

   ```
   DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
   CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
   ```

5. Replace each instance of 'databaseName' with the name of the database functioning as the session store.

6. Copy the contents of the entire file.

7. Paste the file contents into a query and execute the query.

   The session store schema is created.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can read and store session information.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select Session Server from the Database list.

   Data source settings become active.

3. Enter the name of the data source in the Data Source Information field.

   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.

   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.

4. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.

5. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.

6. Click Apply.

   The settings are saved.

7. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

8. Click OK.

   The Policy Server is configured to use the database as a session store.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.

3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Session Information in Oracle

To configure an Oracle database as a session store, complete the following procedures:

1. Gather database information.
2. Create the session store schema.
3. Configure an Oracle data source for CA SiteMinder®.
4. Point the Policy Server to the database.
5. Restart the Policy Server.

More information:

Configure an Oracle Data Source for CA SiteMinder® (see page 305)
Gather Database Information (see page 301)

Create the Session Store Schema

Create the session store schema so the Oracle database can store the session information.

Follow these steps:

1. Log in to Oracle as the user who administers the database information. Log in with an Oracle utility, such as sqlplus.

   Note: We recommend that you do not create the schema with the SYS or SYSTEM users. If necessary, create an Oracle user, such as SMOWNER, and create the schema with that user.

2. To store Unicode characters, confirm that the character set for the Oracle database is set correctly. If you plan to use only English characters, skip this step.

   a. To find the character set, use the following query:

      SELECT value$ FROM sys.props$ WHERE name = 'NLS_CHARACTERSET' ;

   b. Verify that the character set is AL32UTF8 or UTF8 before importing the schema.

3. Import the following script:

   $NETE_PS_ROOT/db/sql/sm_oracle_ss.sql

   Note: Some Oracle SQL utilities have problems with environment variables. If you experience problems importing the script using the utility, specify an explicit path.

The session store schema is created in the database.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can read and store session information.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select Session Server from the Database list.

   Data source settings become active.

3. Enter the name of the data source in the Data Source Information field.
   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.
4. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
5. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.
6. Click Apply.

   The settings are saved.
7. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.
8. Click OK.

   The Policy Server is configured to use the database as a session store.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Session Information in SQL Server

To configure a SQL Server database as a standalone session store, complete the following procedures:

1. Gather database information.
2. Create the session store schema.
3. Configure a SQL Server data source for CA SiteMinder®.
4. Point the Policy Server to the database.
5. Restart the Policy Server.

More information:

Configure a SQL Server Data Source for CA SiteMinder® (see page 288)
Gather Database Information (see page 285)

Create the Session Store Schema

You create the session store schema so the SQL Server database can store and read session information.

To create the session store schema

1. Do one of the following:
   - If you are going to store Unicode characters in the session store, open sm_mssql_ss.sql.unicode in a text editor and copy the contents of the entire file.
   - If you are not going to store Unicode characters in the session store, open sm_mssql_ss.sql in a text editor and copy the contents of the entire file.
2. Start the Query Analyzer and log in as the who administers the Policy Server database.
3. Select the database instance from the database list.
4. Paste the schema into the query.
5. Execute the query.

   The session store schema is created in the database.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can read and store session information.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select Session Server from the Database list.

   Data source settings become active.

3. Enter the name of the data source in the Data Source Information field.

   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.

4. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.

5. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.

6. Click Apply.

   The settings are saved.

7. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

8. Click OK.

   The Policy Server is configured to use the database as a session store.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Audit Logs in IBM DB2

Complete the following procedures to configure an IBM DB2 database to store audit logs:

1. Be sure that you have gathered the required database information.
2. Be sure that the table space page size (page_size) and the buffer pool page size settings for the database instance are each set to at least 16k.

   The default DB2 value for each setting is not sufficient for the CA SiteMinder® audit log schema.
3. Create the audit store schema.
4. Configure the IBM DB2 data source for CA SiteMinder®.
5. Point the Policy Server to the audit store.
6. Restart the Policy Server

More information:

Gather Database Information (see page 322)
Configure an IBM DB2 Data Source for CA SiteMinder® (see page 325)

Create the Audit Store Schema

You create the CA SiteMinder® schema so that an IBM DB2 database can store audit logs.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to *siteminder_home*\db\tier2\DB2.

   siteminder_home

   Specifies the Policy Server installation path.

3. Open the following file and copy the contents to a text editor:

   ```
   sm_db2_logs.sql
   ```

4. Remove NULL from the following lines:

   ```
   sm_assertion_id         VARCHAR(255) NULL,
   sm_assertion_issuerid   VARCHAR(255) NULL,
   sm_assertion_destinationurl     VARCHAR(4096) NULL,
   sm_assertion_statuscode         VARCHAR(255) NULL,
   sm_assertion_NotOnBefore    TIMESTAMP,
   sm_assertion_notonorafter       TIMESTAMP,
   sm_assertion_sess_starttime     TIMESTAMP,
   sm_assertion_sess_notonorafter  TIMESTAMP,
   sm_assertion_authcontext        VARCHAR(255) NULL,
   sm_assertion_versionid          VARCHAR(255) NULL,
   sm_assertion_claims             VARCHAR(255) NULL,
   sm_application_name             VARCHAR(255) NULL,
   sm_tenant_name                  VARCHAR(255) NULL,
   sm_authentication_method        VARCHAR(255) NULL
   ```

5. Save the changes to the file.
6. Paste the contents into a query and execute the query.

   Note: For more information executing a query, see the IBM documentation.

   The audit store schema is added to the database.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can read and store audit logs.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select ODBC from the Storage list.

   ODBC settings appear.

3. Select Audit Logs from the Database list.
4. Select ODBC from the Storage list.

   Data source settings become active.

5. Enter the name of the data source in the Data Source Information field.

   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.

6. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
7. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.

8. Click Apply.

   The settings are saved.

9. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

10. Click OK.

    The Policy Server is configured to use the database as an audit logging database.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.

3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Audit Logs in MySQL

Complete the following procedures to configure MySQL as a standalone audit log store:

1. Be sure that MySQL is installed using the default character set (Latin1). If MySQL was not installed using the default character set, reinstall MySQL before configuring the CA SiteMinder® data store.
2. Gather database information.
3. Create the audit log schema.
4. Configure a MySQL data source for CA SiteMinder®.
5. Point the Policy Server to the database.
6. Restart the Policy Server.

More information:

Gather Database Information (see page 272)
Configure a MySQL Data Source for CA SiteMinder® (see page 274)

Create the Audit Log Schema

You create the audit log schema so the MySQL database can store audit logs.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to the following location:

   siteminder_home\db\tier2\MySQL.

   siteminder_home

   Specifies the Policy Server installation path.
3. Open the following file in a text editor:

   ```
   sm_mysql_logs.sql
   ```
4. Locate the following lines:

   ```
   DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
   CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
   ```
5. Replace each instance of 'databaseName' with the name of the database functioning as the audit store.
6. Copy the contents of the entire file.
7. Paste the file contents into a query and execute the query.

   The audit store schema is created.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can read and store audit logs.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.
2. Select ODBC from the Storage list.

   ODBC settings appear.
3. Select Audit Logs from the Database list.
4. Select ODBC from the Storage list.

   Data source settings become active.

5. Enter the name of the data source in the Data Source Information field.
   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.
6. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
7. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.
8. Click Apply.

   The settings are saved.
9. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.
10. Click OK.

    The Policy Server is configured to use the database as an audit logging database.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Audit Logs in Oracle

To configure an Oracle database to store audit logs, complete the following procedures:

1. Gather database information.
2. Create the audit store schema.
3. Configure an Oracle data source for CA SiteMinder®.
4. Point the Policy Server to the database.
5. Restart the Policy Server.

More information:

Configure an Oracle Data Source for CA SiteMinder® (see page 305)
Gather Database Information (see page 301)

Create the Audit Log Schema

You create the audit log schema so the Oracle database can store audit logs.

To create the CA SiteMinder® schema

1. Log into Oracle with sqlplus or some other Oracle utility as the user who administers the Policy Server database information.

   Note: We recommend that you do not create CA SiteMinder® schema with the SYS or SYSTEM users. If necessary, create an Oracle user, such as SMOWNER, and create the schema with that user.

2. Import the following script:

   $NETE_PS_ROOT/db/sql/sm_oracle_logs.sql

   Note: Environment variables may not function in Oracle's SQL utility. If you experience problems importing the script using the utility, specify an explicit path.

   The audit log schema is created in the database.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can read and store audit logs.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select ODBC from the Storage list.

   ODBC settings appear.

3. Select Audit Logs from the Database list.
4. Select ODBC from the Storage list.

   Data source settings become active.

5. Enter the name of the data source in the Data Source Information field.
   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.
6. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
7. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.

8. Click Apply.

   The settings are saved.

9. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

10. Click OK.

    The Policy Server is configured to use the database as an audit logging database.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Audit Logs in SQL Server

To configure a SQL Server database as a standalone audit log database, complete the following procedures:

1. Gather database information.
2. Create the audit store schema.
3. Configure a SQL Server data source for CA SiteMinder®.
4. Point the Policy Server to the database.
5. Restart the Policy Server.

More information:

Configure a SQL Server Data Source for CA SiteMinder® (see page 288)
Gather Database Information (see page 285)

Create the Audit Log Schema

You create the logging schema so the SQL Server database can store audit logs.

To create the audit log schema

1. Open sm_mssql_logs.sql in a text editor and copy the contents of the entire file.
2. Start the Query Analyzer and log in as the user who administers the Policy Server database.

3. Select the database instance from the database list.
4. Paste the schema from sm_mssql_logs.sql into the query.
5. Execute the query.

   The CA SiteMinder® audit log store schema is created in the database.

Point the Policy Server to the Database

You point the Policy Server to the database so the Policy Server can read and store audit logs.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select ODBC from the Storage list.

   ODBC settings appear.

3. Select Audit Logs from the Database list.
4. Select ODBC from the Storage list.

   Data source settings become active.

5. Enter the name of the data source in the Data Source Information field.
   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.
6. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
7. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.

8. Click Apply.

   The settings are saved.

9. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

10. Click OK.

    The Policy Server is configured to use the database as an audit logging database.

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Key Information in IBM DB2

To configure an IBM DB2 database as a standalone key store, complete the following procedures:

1. Gather database information.
2. Create the key store schema.
3. Configure the IBM DB2 data source for CA SiteMinder®.
4. Point the Policy Server to the key store.
5. Restart the Policy Server.

More information:

Gather Database Information (see page 322)
Configure an IBM DB2 Data Source for CA SiteMinder® (see page 325)

Create the Key Store Schema

You create the CA SiteMinder® schema so that an IBM DB2 database can store key information.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to *siteminder_home*\db\tier2\DB2.

   siteminder_home

   Specifies the Policy Server installation path.
3. Open the following file and copy the contents to a text editor:

   ```
   sm_db2_ps.sql
   ```
4. Paste the contents into a query and execute the query.

   Note: For more information executing a query, see the IBM documentation.

   The key store schema is added to the database.

Point the Policy Server to Database

You point the Policy Server to the database so the Policy Server can read and store key information.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.
2. Select ODBC from the Storage list.

   ODBC settings appear.
3. Select Key Store from the Database list and clear the Use Policy Store database check box.

   Data source settings become active.
4. Enter the name of the data source in the Data Source Information field.
   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.

5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.

6. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.

7. Click Apply.

   The settings are saved.

8. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

9. Click OK.

   The Policy Server is configured to use the database as a key store

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.

2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.

3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Key Information in MySQL

Complete the following procedures to configure MySQL as a standalone key store:

1. Be sure that MySQL is installed using the default character set (Latin1). If MySQL was not installed using the default character set, reinstall MySQL before configuring the CA SiteMinder® data store.

2. Gather database information.

3. Create the key store schema.

4. Configure a MySQL data source for CA SiteMinder®.

5. Point the Policy Server to the database.
6. Restart the Policy Server.

Create the Key Store Schema

You create the key store schema so the MySQL database can store key information.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to the following location:

   `siteminder_home\db\tier2\MySQL.`

   siteminder_home

   Specifies the Policy Server installation path.

3. Open the following file in a text editor:

   ```
   sm_mysql_ps.sql
   ```

4. Locate the following lines:

   ```
   DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
   CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
   ```

5. Replace each instance of 'databaseName' with the name of the database functioning as the key store.
6. Copy the contents of the entire file.
7. Paste the file contents into a query and execute the query.

   The key store schema is created.

Point the Policy Server to Database

You point the Policy Server to the database so the Policy Server can read and store key information.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select ODBC from the Storage list.

   ODBC settings appear.

3. Select Key Store from the Database list and clear the Use Policy Store database check box.

   Data source settings become active.

4. Enter the name of the data source in the Data Source Information field.

   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.

5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.

6. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.

7. Click Apply.

   The settings are saved.

8. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

9. Click OK.

   The Policy Server is configured to use the database as a key store

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.

2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.

3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Key Information in Oracle

To configure an Oracle database as a key store, complete the following procedures:

1. Gather database information.
2. Create the key store schema.
3. Configure an Oracle data source for CA SiteMinder®.
4. Point the Policy Server to the database.
5. Restart the Policy Server.

More information:

Configure an Oracle Data Source for CA SiteMinder® (see page 305)
Gather Database Information (see page 301)

Create the Key Store Schema

You create the key store schema so the Oracle database can store key information.

To create the CA SiteMinder® schema

1. Log into Oracle with sqlplus or some other Oracle utility as the user who administers the Policy Server database information.

   Note: We recommend that you do not create CA SiteMinder® schema with the SYS or SYSTEM users. If necessary, create an Oracle user, such as SMOWNER, and create the schema with that user.

2. Import the following script:

   $NETE_PS_ROOT/db/sql/sm_oracle_ps.sql

   Note: Environment variables may not function in Oracle's SQL utility. If you experience problems importing the script using the utility, specify an explicit path.

   The key store schema is created in the database.

Point the Policy Server to Database

You point the Policy Server to the database so the Policy Server can read and store key information.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select ODBC from the Storage list.

   ODBC settings appear.

3. Select Key Store from the Database list and clear the Use Policy Store database check box.

   Data source settings become active.

4. Enter the name of the data source in the Data Source Information field.

   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.
   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.

5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.

6. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.

7. Click Apply.

   The settings are saved.

8. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

9. Click OK.

   The Policy Server is configured to use the database as a key store

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

How to Store Key Information in SQL Server

To configure a SQL Server database as a standalone key store, complete the following procedures:

1. Gather database information.
2. Create the key store schema.
3. Configure a SQL Server data source for CA SiteMinder®.
4. Point the Policy Server to the database.
5. Restart the Policy Server.

More information:

Configure a SQL Server Data Source for CA SiteMinder® (see page 288)
Gather Database Information (see page 285)

Create the Key Store Schema

You create the key store schema so the SQL Server database can store key information.

To create the key store schema

1. Open sm_mssql_ps.sql in a text editor and copy the contents of the entire file.
2. Start the Query Analyzer and log in as the who administers the Policy Server database.

3. Select the database instance from the database list.

4. Paste the schema from sm_mssql_ps.sql into the query.

5. Execute the query.

   The CA SiteMinder® key store schema is created in the database.

Point the Policy Server to Database

You point the Policy Server to the database so the Policy Server can read and store key information.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.

   Database settings appear.

2. Select ODBC from the Storage list.

   ODBC settings appear.

3. Select Key Store from the Database list and clear the Use Policy Store database check box.

   Data source settings become active.

4. Enter the name of the data source in the Data Source Information field.

   - (Windows) this entry must match the name you entered in the Data Source Name field when you created the data source.

   - (UNIX) this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [CA SiteMinder® Data Sources]. If you modified the first entry, be sure that you enter the correct value.

5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.

6. Specify the maximum number of database connections allocated to CA SiteMinder®.

   Note: We recommend retaining the default for best performance.

7. Click Apply.

   The settings are saved.

8. Click Test Connection.

   SiteMinder returns a confirmation that the Policy Server can access the data store.

9. Click OK.

   The Policy Server is configured to use the database as a key store

Restart the Policy Server

You restart the Policy Server for certain settings to take effect.

Follow these steps:

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.

   The Policy Server stops as indicated by the red stoplight.
3. Click Start.

   The Policy Server starts as indicated by the green stoplight.

   Note: On UNIX or Linux operating environments, you can also execute the stop-all command followed by the start-all command to restart the Policy Server. These commands provide an alternative to the Policy Server Management Console.

Sample User Directories

CA SiteMinder® does not require the use of a proprietary user store. However, CA SiteMinder® does provide schema files that populate a relational database with sample users.

Configure an IBM DB2 Sample User Directory

You configure a sample user directory to populate a database with sample users.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to *siteminder_home*\db\tier2\DB2.

   siteminder_home

   Specifies the Policy Server installation path.
3. Open the following file and copy the contents to a text editor:

   smsampleusers_db2.sql

4. Paste the contents into a query and execute the query.

   Note: For more information about executing a query, see the IBM documentation.

   The user directory is populated with the sample users.

5. Configure the user directory connection to the Policy Server.

Note: For more information about configuring user directory connections, see the *Policy Server Configuration Guide*.

Configure a MySQL Sample User Directory

You configure a sample user directory to populate a database with sample users.

Follow these steps:

1. Log in to the Policy Server host system.
2. Navigate to the following location:

   `*siteminder_home*\db\tier2\MySQL.`

   siteminder_home

   Specifies the Policy Server installation path.

3. Open the following file in a text editor:

   ```
   smsampleusers_mysql.sql
   ```

4. Locate the following lines:

   ```
   DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
   CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
   ```

5. Replace each instance of 'databaseName' with the name of the database functioning as the sample user store.
6. Copy the contents of the entire file.
7. Paste the file contents into a query and execute the query.

   Note: For more information about executing a query, see the MySQL documentation.

   The user store is populated with the sample users.

8. Configure the user directory connection to the Policy Server.

Note: For more information about configuring user directory connections, see the *Policy Server Configuration Guide.*

Configure an Oracle Sample User Directory

You configure a sample user directory to populate a database with sample users.

To configure the sample user directory

1. Log into Oracle with sqlplus or some other Oracle utility as the user who administers the Policy Server database information.

   Note: We recommend that you do not create CA SiteMinder® schema with the SYS or SYSTEM users. If necessary, create an Oracle user, such as SMOWNER, and create the schema with that user.

2. Import the following script:

   $NETE_PS_ROOT/db/sql/smsampleusers_oracle.sql

   Note: Environment variables may not function in Oracle's SQL utility. If you experience problems importing the script using the utility, specify an explicit path.

   The user directory is populated with the sample users.

3. Configure the user directory connection to the Policy Server.

Note: More information on configuring user directory connections exists in the *Policy Server Configuration Guide*.

Configure a SQL Server Sample User Directory

You configure a sample user directory to populate a database with sample users.

To configure the sample user directory

1. Open smsampleusers_sqlserver.sql in a text editor and copy the contents of the entire file.

2. Start the Query Analyzer and log in as the user who administers the Policy Server database.

3. Select the database instance from the database list.

4. Paste the schema from smsampleusers_sqlserver.sql into the query.

5. Execute the query.

   The user directory is populated with the sample users.

6. Configure the user directory connection to the Policy Server.

Note: For more information about configuring user directory connections, see the *Policy Server Configuration Guide*.

Chapter 8: Installing the Administrative UI

Installation Road Map

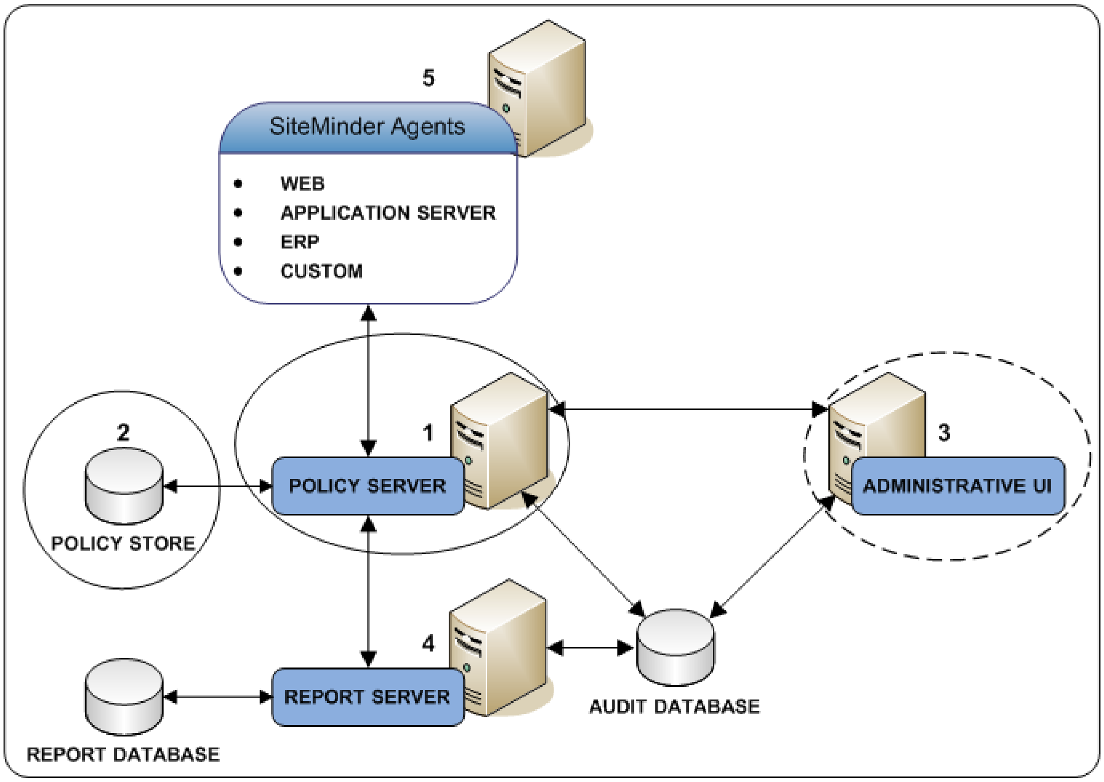
The following diagram illustrates a sample CA SiteMinder® installation and lists the order in which you install and configure each component.

- Solid lines surround the components that are required before installing and registering the Administrative UI. They include:
  - A Policy Server
  - A policy store

  If a Policy Server and a policy store are not part of your environment, install and configure both components before continuing.
- A dotted line surrounds the Administrative UI. Install this component now.

  Note: After you install and register the Administrative UI, you can prepare for a Web Agent installation, as illustrated by step five.

Figure 3: Admininstrative UI Installation Road Map



Administrative UI Installation Options

The Administrative UI requires an application server to run. As such, two installation options are available:

- **Stand–alone installation**—This option creates the required application server infrastructure through a prerequisite installer. The prerequisite installer installs an embedded application server (JBoss) and the required JDK. Verify that the Administrative UI host system meets the minimum system requirements before starting the installation.

  The prerequisite installer launches the Administrative UI installer after a successful installation. The Administrative UI installer uses the embedded application server infrastructure to complete the installation.

  Note: If you are installing to UNIX and running the prerequisite installation media in console–mode, you manually start the Administrative UI installer to complete the installation.

- **Existing application server installation**—This option lets you install the Administrative UI to an existing application server infrastructure. The Administrative UI installer prompts you for application server-specific information and the location of the required JDK. Verify that the Administrative UI host system meets all system and third–party component requirements before starting the installation.

The following sections detail the stand–alone installation. For more information about installing to an existing application server infrastructure, see Installing the Administrative UI to an Existing Application Server.

More information:

Installing the Administrative UI to an Existing Application Server (see page 451)

Trusted Relationship with a Policy Server

A trusted relationship between the Administrative UI and a Policy Server is required to begin managing your environment. You establish this relationship the first–time you log in using the default CA SiteMinder® super user account (siteminder) and password. These credentials are stored in the policy store.

When you configure the policy store, you use the XPSRegClient utility to submit the super user credentials to the Policy Server. The Policy Server uses these credentials to verify that the registration request is valid and that the relationship can be created.

Note: If you used the Policy Server installer to configure the policy store automatically, the installer used the XPSRegClient utility to submit the credentials.

The time from which the credentials are supplied to when the initial Administrative UI login can occur is limited to 24 hours. Therefore, the process for installing the Administrative UI is determined by when the policy store is configured and the Administrative UI is installed.

Complete the Administrative UI Installation Checklist

Complete the following steps before you install the Administrative UI:

□ Verify that you are using a supported operating system.

□ Verify that the Administrative UI host system meets the minimum system requirements.

□ (Linux) Be sure that the required Linux libraries are installed to the Administrative UI host system.

□ Determine when the policy store was configured.

If the policy store was configured more than 24 hours ago, use the XPSRegClient utility to submit the default CA SiteMinder® super user account credentials to the Policy Server before installing the Administrative UI. The Policy Server requires these credentials to create a trusted relationship with the Administrative UI.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

More information:

System Requirements (see page 23)
Required Linux Libraries (see page 457)

How to Install the Administrative UI

Complete the following steps to install the Administrative UI:

1. Be sure that you have reviewed the Administrative UI installation checklist.
2. (Linux) Review the required Linux libraries requirement.
3. Gather information for the installer.
4. (Optional) Reset the registration window.
5. Install the Administrative UI.
6. Register the Administrative UI.

Consider the following:

- After a successful Windows installation, the CA SiteMinder® Administrative UI login screen appears and the application server automatically starts, which lets you register the Administrative UI with a Policy Server.
- After a successful UNIX installation, you start the application server manually and log into the Administrative UI to complete the registration. For more information, see How to Register the Administrative UI.

Gather Information for the Installer

Gather the following information before installing and registering the Administrative UI:

- **Installation location**—Determine the Administrative UI installation path.
- **Administrative UI system name**—Identify the fully qualified name of the Administrative UI host system.
- **Server port**—Identify the port on which JBoss must listen for HTTP requests.
- **SiteMinder super user account password**—Identify the password for the default SiteMinder user account (siteminder).
- **Policy Server system name**—Identify the following:
  - The Policy Server to which the Administrative UI will be registered.
  - The fully qualified name of the Policy Server host system.
- **Policy Server authentication port**—If you changed the default settings after installing the Policy Server, identify the Policy Server authentication port. The Settings tab in the Policy Server Management Console lists the access control ports.

Reset the Administrative UI Registration Window

If either of the following actions occurred more than 24 hours ago, this step is required:

- You used the Policy Server installation wizard to configure a policy store automatically.
- You used the XPSRegClient utility to submit the CA SiteMinder® super user credentials to the Policy Server.

Note: (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder_administrator[:passphrase] -adminui-setup -t timeout -r
   retries -c comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   siteminder_administrator

   Specifies a CA SiteMinder® administrator. If you are installing the Administrative UI as part of:

   - A new 12.52 environment, specify the following default account:

   ```
   siteminder
   ```

   - An upgrade, specify any CA SiteMinder® administrator account with super user permissions in the policy store. If you do not have a super user account in the policy store, use the smreg utility to create the default account.

   passphrase

   Specifies the password for the CA SiteMinder® administrator account.

   -adminui-setup

   Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

   -t *timeout*

   (Optional) Specifies how long you have after you install the Administrative UI to log in for the time to complete the registration. The Policy Server denies the registration request when the timeout value is exceeded.

   Unit of measurement: minutes

   Default: 1440 (24 hours)

   Minimum limit: 1

   Maximum limit: 1440 (24 hours)

   -r *retries*

   (Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect CA SiteMinder® administrator credentials when logging in to the Administrative UI for the first–time.

   Default: 1

   Maximum limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

The utility supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log in to the Administrative UI for the first–time.

How to Install the Administrative UI

The following sections explain how to install the Administrative UI using the prerequisite installer as part of the stand-alone installation option.

Review Prerequisite Information

Consider the following items before you install the Administrative UI:

- You install the Administrative UI using the installation media on the Technical Support site.

  Note: For a list of installation media names, see the *Policy Server Release Notes*.

- If you are using the stand-alone option to install, the following procedures apply. If you are installing to an existing application server infrastructure, see Installing the Administrative UI to an Existing Application Server.
- (Windows) Run the installer from the Administrative UI host system. Do not run the installer from a mapped network share or UNC path.
- The installation zip contains the prerequisite installer and the Administrative UI installer.
  - If you are running the prerequisite installer on Windows, be sure that both executables are in the same location. The prerequisite installer automatically starts the Administrative UI installer to complete the installation.
  - If you are running the prerequisite installer on UNIX, be sure that both executables are in the same location. However, you manually start the Administrative UI installer to complete the installation. The prerequisite installer does not automatically start the Administrative UI installer.
- The installation zip contains a layout.properties file at the same level as the installation media. If you moved the installation media after extracting the installation zip, move the properties file to the same location or the installation fails.
- (Red Hat Linux) The Red Hat 6 operating system relies on entropy for performance. Increase entropy before installing the component. Without sufficient entropy, the installation can take an exceedingly long time to complete. We recommend that you use the following command to set a symbolic link:

  ```
  mv /dev/random /dev/random.org
  ln –s /dev/urandom /dev/random
  ```

- (UNIX) Depending on your permissions, run the following command to add executable permissions to the directory that contains the installation media:

  ```
  chmod -R+x directory
  ```

  directory

  Specifies the directory that contains the installation media.

- (UNIX) If you execute the Administrative UI installer across different subnets, it can crash. Install the Administrative UI directly on the host system.

More information:

Install the Administrative UI (see page 460)

Install and Register the Administrative UI

Install the Administrative UI and prerequisite components to provide a management console for all tasks that are related to access control, reporting, and policy analysis.

Follow these steps::

1. Exit all applications that are running.
2. Navigate to the installation media.
3. Double-click *prerequisite_installation_media*.

   prerequisite_installation_media

   > Specifies the Administrative UI prerequisite installer executable.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.
4. Use your completed installation worksheet to enter the required values.
5. Click Install.

   The required components are installed.
6. Click Done.

   The Administrative UI installer starts.
7. Follow the prompts and click Install.

   The Administrative UI is installed. The CA SiteMinder® Administrative UI login screen appears.
8. Type siteminder in the User Name field.
9. Type the siteminder account password in the Password field.
10. Type the fully qualified Policy Server host name in the Server field.

    Consider the following:

    - You can enter a valid IPv4 address or IPv6 address.
    - If you do not specify a port, the registration defaults to 44442, which is the default Policy Server authentication port.

    The Administrative UI opens and is registered with the Policy Server.

Install the Administrative UI Using a GUI

Install the Administrative UI and prerequisite components to provide a management console for all tasks that are related to access control, reporting, and policy analysis. This procedure describes how to install the Administrative UI using a GUI.

Follow these steps::

1. Exit all applications that are running.
2. Open a shell and navigate to the installation media.
3. Enter the following command:

   ```
   ./prerequisite_installation_media
   ```

   prerequisite_installation_media

   Specifies the Administrative UI prerequisite installer executable.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.
4. Use your completed installation worksheet to enter the required values.
5. Click Install.

   The required components are installed. The prerequisite installer prompts you to run the Administrative UI installer.
6. Enter the following command:

   ```
   ./installation_media
   ```

   installation_media

   Specifies the Administrative UI installer executable.

   The Administrative UI installer starts.
7. Follow the prompts and click Install.

   The Administrative UI is installed.

   Note: You cannot use the Administrative UI to manage your environment until you have registered it with a Policy Server.

More information:

How to Register the Administrative UI (see page 375)

Install the Administrative UI Using a UNIX Console

Install the Administrative UI and prerequisite components to provide a management console for all tasks that are related to access control, reporting, and policy analysis. This procedure describes how to install the Administrative UI using a UNIX console.

Follow these steps::

1. Exit all applications that are running.
2. Open a shell and navigate to the installation media.
3. Enter the following command:

   ```
   ./prerequisite_installation_media -i console
   ```

   prerequisite_installation_media

   Specifies the Administrative UI prerequisite installer executable.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.

4. Use your completed installation worksheet to enter the required values.
5. Press Enter.

   The required components are installed. The prerequisite installer prompts you to run the Administrative UI installer.

6. Enter the following command:

   ```
   ./installation_media -i console
   ```

   installation_media

   Specifies the Administrative UI installer executable.

   The Administrative UI installer starts.

7. Follow the prompts and press Enter.

   The Administrative UI is installed.

   Note: You cannot use the Administrative UI to manage your environment until you have registered it with a Policy Server.

More information:

How to Register the Administrative UI (see page 375)

Troubleshoot the Administrative UI Installation

Use the following files to troubleshoot the Administrative UI installation:

- Administrative_UI_Prerequisite_Installer_InstallLog.log

  If you used the stand–alone installation option, this log lists the number of successes, warnings, non–fatal errors, and errors that occurred during the prerequisite installation. Individual installation actions are listed with the respective status.

  Location: *administrative_ui_home*\CA\SiteMinder\adminui\install_config_info

  administrative_ui_home

  Specifies the Administrative UI installation path.

- CA_SiteMinder_Administrative_UI_InstallLog.log

  This log lists the number of successes, warnings, non–fatal errors, and errors that occurred during the Administrative UI installation. Individual installation actions are listed with the respective status.

  Location: *administrative_ui_home*\CA\SiteMinder\adminui\install_config_info

  administrative_ui_home

  Specifies the Administrative UI installation path.

How to Register the Administrative UI

You are required to register the Administrative UI before it can be used to manage CA SiteMinder® objects. Registering the Administrative UI creates a trusted connection between the Administrative UI and a Policy Server. Consider the following items:

- (UNIX) You are required to start the application server manually and log in to the Administrative UI to complete the registration.
- (Windows) The CA SiteMinder® Administrative UI login screen appears and the application server starts automatically after installing the Administrative UI to Windows. These actions let you register the Administrative UI immediately. If you did not register the Administrative UI immediately after installing it, complete the following process.

This process explains how to register an Administrative UI that you installed using the prerequisite installer. If you installed the Administrative UI to an existing application server environment, see the respective process in Installing the Administrative UI to an Existing Application Server.

To register the Administrative UI, complete the following procedures:

1. Create the FIPs environment variable (see page 376).

2. Start the application server (see page 377).
3. Register the Administrative UI.

More information:

How to Register the Administrative UI (see page 463)

Create the FIPS Environment Variable

If your environment meets both of the following criteria, creating the FIPs environment variable is required to register the Administrative UI for the first–time:

- The Policy Server to which you are registering is operating in FIPs–only mode.
- The Administrative UI is not installed on the Policy Server host system.

Follow these steps:

1. Complete one of the following steps:
   - (Windows) Log into the Administrative UI host system as an administrative user.
   - (UNIX) Log into the Administrative UI host system as the user that installed the Administrative UI.
2. Set the following environment variable:

   CA_SM_PS_FIPS140=ONLY

   Note: For more information about setting environment variables, see your OS–specific documentation.
3. Verify that Windows or the UNIX shells that runs the Administrative UI correctly recognizes the CA_SM_PS_FIPS140 variable.

Start the Application Server

If you used the stand-alone option to install the Administrative UI, the following procedure applies. If you installed the Administrative UI to an existing application server infrastructure, see Installing the Administrative UI to an Existing Application Server.

To start the application server

1. From the Administrative UI host system, do one of the following:
   - **Windows**—Open the Microsoft Services console.

     The application server automatically starts after installing the Administrative UI on Windows. You do not have to start the application server after installation.
   - **UNIX**—Navigate to *install_home*/CA/siteminder/adminui/bin

     install_home.

     Specifies the Administrative UI installation path.
2. Do one of the following:
   - **Windows**—Start the CA SiteMinder® Administrative UI service.
   - **UNIX**—Type run.sh and press Enter.

   The application server is started.

More information:

Installing the Administrative UI to an Existing Application Server (see page 451)
Start the Application Server (see page 467)

Register the Administrative UI

Register the Administrative UI with a Policy Server to begin managing your environment.

Follow these steps:

1. Complete one of the following steps:

   ■ Windows:

   – (Recommended) Use the Administrative UI shortcut to open the Administrative UI. Using the shortcut registers the Administrative UI over SSL. If you do not have access to the shortcut, open a web browser and go to the following location:

     https://*host*:8443/iam/siteminder/adminui

     Note: A self–signed certificate that is valid for ten years is created and used for the connection. The certificate is created with an RSA 2048 key strength.

   – Open a web browser and go to the following location:

     http://host:8080/iam/siteminder/adminui

   ■ UNIX:

   – (Recommended) Open a web browser and go to the following location to register the Administrative UI over SSL:

     https://host:8443/iam/siteminder/adminui

   – Open a browser and go to the following location:

     http://*host*:8080/iam/siteminder/adminui

     Note: If the host system does not have a web browser, you can remotely access the login screen.

   host

   Specifies the fully qualified Administrative UI host system name.

   The CA SiteMinder® Administrative UI login screen appears.

2. Enter the following value in the User Name field:

   `siteminder`

3. Type the CA SiteMinder® superuser account password in the Password field.

   Note: If your superuser account password contains dollar-sign ($) characters, replace each instance of the dollar-sign character with $DOLLAR$. For example, if the CA SiteMinder® superuser account password is $password, enter $DOLLAR$password in the Password field.

4. Type the fully qualified Policy Server host name in the Server field.

   Consider the following items:

   - You can enter a valid IPv4 address or IPv6 address.
   - If you do not specify a port, the registration defaults to 44442, which is the default Policy Server authentication port.

   The Administrative UI opens and is registered with the Policy Server.

More information:

Registration Not on File Error Appears (see page 487)
Enable Secure Cookies (see page 379)

Enable Secure Cookies

If you have registered the Administrative UI using HTTPS, then modify the context.xml file of the application server to enable secure cookies.

Follow these steps:

1. Shut down the application server.
2. Navigate to the following location:

   ```
   user_console.war\WEB-INF
   ```

3. Open the context.xml file.
4. Add the following parameter to the SessionCookie tag:

   ```
   secure="true"
   ```

5. Save and close the file.
6. Restart the application server.

   The context.xml file is updated and secure cookies are enabled.

More information:

Start the Application Server (see page 377)
Stop the Application Server (see page 380)

Stop the Application Server

If you used the stand-alone option to install the Administrative UI, the following procedure applies. If you installed the Administrative UI to an existing application server infrastructure, see Installing the Administrative UI to an Existing Application Server.

To stop the application server

1. From the Administrative UI host, do one of the following:
   - **Windows**—Open the Microsoft Services console.
   - **UNIX**—Navigate to *install_home*/CA/siteminder/adminui/bin

     administrative_ui_install.

       Specifies the Administrative UI installation path.
2. Do one of the following:
   - **Windows**—Stop the CA SiteMinder® Administrative UI service.
   - **UNIX**—Type shutdown.sh and press Enter.

   The application server is stopped.

More information:

Installing the Administrative UI to an Existing Application Server (see page 451)
Stop the Application Server (see page 470)

Administrator Credentials

By default, the Administrative UI uses the policy store as its source for CA SiteMinder® administrator credentials. You can configure the Administrative UI to use an external store, for example, a corporate directory.

Note: For more information about configuring an external administrator user store, see the *Policy Server Configuration Guide*.

(Optional) Install and Configure Additional Administrative UIs for High Availability

Install more than one Administrative UI to be sure that unexpected outages do not prevent you from managing CA SiteMinder® objects. Consider the following before installing another Administrative UI:

- Register the Administrative UI with a Policy Server that is not already sharing a trusted connection with an Administrative UI. Registering with another Policy Server prevents a single Policy Server outage from disabling both GUIs.
- An Administrative UI cannot failover to multiple Policy Servers. However, you can configure the Administrative UI to manage multiple Policy Servers.
- If the existing Administrative UI is configured for external CA SiteMinder® administrator authentication:
  - Configure the new Administrative UI with the same external store. Configuring the new Administrative UI with the same external store helps ensure that all CA SiteMinder® administrators are available to all GUIs.
  - Be sure to configure subsequent Administrative UI connections to the same external store using the same network identifier. Mixing network identifiers for multiple Administrative UI connections to the same external store is not supported.

Example: If you configured the first connection with 172.16.0.0, create subsequent connections with 172.16.0.0. If you configured the first connection with comp001@example.com, create subsequent connections with comp001@example.com.

More information:

How to Install the Administrative UI (see page 367)

How to Configure Additional Policy Server Connections

By default, the Administrative UI is configured with a single Policy Server as part of the installation process. You can, however, configure additional connections to administer more than one Policy Server. For example, you can create connections to manage Policy Servers in development and staging environments.

To configure additional Policy Server connections, complete the following steps:

1. Configure a connection to an external administrator user store.

   Note: If the Administrative UI is using the policy store as its source of administrator identities, you cannot configure additional Policy Server connections. For more information about configuring an external administrator user store connection, see the *Policy Server Configuration Guide*.

2. Run the registration tool.
3. Configure the connection to the Policy Server.

Run the Registration Tool

You run the Administrative UI registration tool to create a client name and passphrase. A client name and passphrase pairing are values that the Policy Server uses to identify the Administrative UI you are registering. You submit the client and passphrase values from the Administrative UI to complete the registration process.

To run the registration tool

1. Open a command prompt from the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient client_name[:passphrase] -adminui -t timeout -r retries -c comment
   -cp -l log_path -e error_path
   -vT -vI -vW -vE -vF
   ```

   Note: Inserting a space between *client_name* and [:*passphrase*] results in an error.

   client_name

   Identifies the Administrative UI being registered.

   Limit: This value must be unique. For example, if you have previously used smui1 to register an Administrative UI, enter smui2.

   Note: Record this value. This value is to complete the registration process from the Administrative UI.

   passphrase

   Specifies the password required to complete the registration of the Administrative UI.

   Limits:

   - The passphrase must contain at least six (6) characters.
   - The passphrase cannot include an ampersand (&) or an asterisk (*).

- If the passphrase contains a space, it must be enclosed in quotation marks.
- If you are registering the Administrative UI as part of an upgrade, you can reuse a previous passphrase.

Note: If you do not specify the passphrase in this step, XPSRegClient prompts you to enter and confirm one.

Important! Record the passphrase, so that you can refer to it later.

-adminui

Specifies that an Administrative UI is being registered.

-t *timeout*

(Optional) Specifies how long you have to complete the registration process from the Administrative UI. The Policy Server denies the registration request when the timeout value is reached.

Unit of measurement: minutes

Default: 240 (four hours)

Minimum Limit: 1

Maximum Limit: 1440 (one day)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you complete the registration process from the Administrative UI. A failed attempt can result from an incorrect client name or passphrase submitted to the Policy Server during the registration process.

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The registration tool prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log_path*

(Optional) Specifies where to export the registration log file.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

The registration tool lists the name of the registration log file and prompts for a passphrase.

3. Press Enter.

   The registration tool creates the client name and passphrase pairing.

You can now register the Administrative UI with a Policy Server. You complete the registration process from the Administrative UI.

Gather Registration Information

The Administrative UI requires specific information about the Policy Server and the client name and passphrase you created to complete the registration process. Gather the following information before logging into the Administrative UI:

- **Client name**—The client name you specified using the XPSRegClient tool.
- **Passphrase**—The passphrase you specified using the XPSRegClient tool.

- **Policy Server host**—The IP address or name of the Policy Server host system.
- **Policy Server authentication port**—The port on which the Policy Server is listening for authentication requests.

  Default: 44442

Note: A worksheet is provided to help you gather and record information before registering the Administrative UI.

Configure the Connection to the Policy Server

You configure the connection so the Administrative UI can be used to manage CA SiteMinder® objects.

To configure a Policy Server connection

1. Log into the Administrative UI with an account that has super user permissions.
2. Click Administration, Admin UI.
3. Click Policy Server Connections, Register Policy Server Connection.

   The Register Policy Server Connection screen appears.

   Note: Click Help for descriptions of settings and controls, including their respective requirements and limits.
4. Type a connection name in the Name field.
5. Type the Policy Server host name or IP address in the Policy Server Host field.
6. Type the Policy Server authentication port in the Policy Server Port field.

   Note: This value must match the value in the Authentication port (TCP) field on the Settings tab in the Policy Server Management Console. The default authentication port is 44442. To determine the port number, open the Settings tab in the Policy Server Management Console.
7. Type the client name and passphrase you created using the registration tool in the respective fields.
8. Select a FIPS mode:
   - If you installed the Policy Server in FIPS-compatibility mode, select Compatibility mode.
   - If you installed the Policy Server in FIPS-only mode, select FIPS only mode.
9. Click Submit.

   The connection between the Administrative UI and the Policy Server is configured.

   The Administrative UI login screen contains a list of Policy Servers to which the Administrative UI is registered. By default, the Policy Server that was registered first is the default connection.

Modify the Default Policy Server Connection

The Administrative UI login screen contains a list of Policy Servers to which the Administrative UI is registered. By default, the Policy Server that was registered first appears as the default connection. You can modify the list to have another Policy Server connection appear as the default.

To modify the default Policy Server connection

1. Click Administration, Admin UI.
2. Click Policy Server Connections, Modify Policy Server Connection.

   The Modify Policy Server Connection pane appears.
3. Specify search criteria and click Search.

   Administrative UI connections matching the criteria appear.
4. Select the connection you want and click Select.

   Settings specific to the Administrative UI connection appear.
5. Click the arrow icon in the Advanced group box.

   Advanced settings appear.
6. Select the Default Connection check box and click Submit.

   The Policy Server connection is configured as the default connection.

Delete a Policy Server Connection

The Administrative UI login screen contains a list of Policy Servers to which the Administrative UI is registered. You delete a Policy Server connection to remove it from the list when the connection is no longer required.

To delete a Policy Server connection:

1. Click Administration, Admin UI.
2. Click Policy Server Connections, Delete Policy Server Connection.

   The Delete Policy Server Connection pane appears.
3. Specify search criteria and click Search.

   Administrative UI connections matching the criteria appear.
4. Select the connection you want and click Select.

   You are prompted to confirm that the connection can be deleted.
5. Click Yes.

   The connection to the Policy Server is deleted.

(Optional) Uninstall the Administrative UI

You uninstall the Administrative UI when it is no longer required on the system.

Note: If you used the stand-alone option to install the Administrative UI, the following procedure applies. If you installed the Administrative UI to an existing application server infrastructure, see Installing the Administrative UI to an Existing Application Server.

Follow these steps:

1. Stop the application server.
2. Open the Windows Control Panel and go to the list of programs.
3. Right–click CA CA SiteMinder® Administrative UI.
4. Click Uninstall/Change.
5. Follow the instructions of the wizard.

   Note: If you are prompted to remove a shared file, click No to All.
6. If requested, reboot the system.
7. Open the Windows Control Panel and go to the list of programs.
8. Right–click Administrative UI Prerequisite Installer.
9. Follow the instructions of the wizard.

   Note: If you are prompted to remove a shared file, click No to All.
10. If requested, reboot the system.

    The Administrative UI and the required third–party components are uninstalled.

More information:

Installing the Administrative UI to an Existing Application Server (see page 451)
Uninstall the Administrative UI on Windows (see page 472)

Uninstall the Administrative UI on UNIX

You uninstall the Administrative UI when it is no longer required on the system.

Consider the following items:

- Do not manually remove the installation directories to uninstall this component. Execute the uninstall shell script. If you only remove the installation directories, related registries can be left behind. If you try to re–install this component on this host system, the entries can prevent a successful installation.
- If you used the stand-alone option to install the Administrative UI, the following procedure applies. If you installed the Administrative UI to an existing application server infrastructure, see Installing the Administrative UI to an Existing Application Server.

Follow these steps:

1. Stop the application server.
2. Open a shell and navigate to:

   ```
   administrative_ui_home/CA/SiteMinder/adminui/install_config_info
   ```

   administrative_ui_home

   Specifies the Administrative UI installation path.
3. Run the following command:

   ```
   ./sm-wamui-uninstall.sh
   ```

   The process to remove the Administrative UI starts.
4. Follow the prompts to uninstall the Administrative UI.

   The installer prompts you when the Administrative UI is uninstalled.
5. Open a command window and navigate to:

   ```
   administrative_ui_home/CA/SiteMinder/webadmin/install_config_info
   ```

   administrative_ui_home

   Specifies the Administrative UI installation path.
6. Run the following command:

   ```
   ./prerequisite-uninstall.sh
   ```
7. Follow the prompts to uninstall the Administrative UI prerequisite components.

   The installer prompts you when the third–party components are uninstalled.

   The Administrative UI and the required third-party components are uninstalled.

More information:

Installing the Administrative UI to an Existing Application Server (see page 451)

Prepare for Web Agent Installation

Before you install a Web Agent, you must have:

- Installed the Policy Server.
- Configured a policy/key store to communicate with the Policy Server.
- Installed and registered the Administrative UI.
- Confirmed that the Policy Server can communicate with the system on which you will install the Web Agent.

Before you can register a trusted host at the Web Agent site, the following objects must be configured in the Administrative UI.

Note: For more information about configuring each of the following objects, see the *Policy Server Configuration Guide*.

To centrally manage Agents, configure the following using the Administrative UI:

- **A CA SiteMinder® Administrator that has the right to register trusted hosts**—A trusted host is a client computer where one or more CA SiteMinder® Web Agents are installed. The term trusted host refers to the physical system. There must be an administrator with the permission to register trusted hosts. The default CA SiteMinder® administrator has this permission.
- **Agent identity—**An Agent identity establishes a mapping between the name and the IP address of the web server instance hosting a Web Agent. You define an Agent identity from the Agents object in the Administrative UI. You assign the Agent identity a name and specify the Agent type as a Web Agent.

  Note: The name you assign for the Agent is the same name you specify in the DefaultAgentName parameter for the Agent Configuration Object.
- **Host Configuration Object—**A host configuration object defines the communication between the trusted host and the Policy Server after the initial connection between the two is made.

  Do not confuse the host configuration object with the trusted host configuration file, SmHost.conf, which is installed at the trusted host after a successful host registration. The settings in the SmHost.conf file let the host connect to a Policy Server for the first connection only. Subsequent connections are governed by the host configuration object.

- **Agent Configuration Object—**An Agent configuration object includes the parameters that define the Web Agent configuration. There are a few required parameters you are required to set for the basic operation described below.

  Note: For more information about Agent parameters, see the *Web Agent Configuration Guide*.

  - **For all Agents—**The Agent Configuration Object must include a value for the DefaultAgentName. The DefaultAgentName must match the Agent identity name you specified in the Agents object. The DefaultAgentName identifies the Agent identity that the Web Agent uses when it detects an IP address on its web server that does not have an Agent identity assigned to it.

  - **For Domino Web Agents—**The Agent Configuration Object must include values for the following parameters:

    - **DominoDefaultUser—**If the user is not in the Domino Directory, and they have been authenticated by CA SiteMinder® against another user directory, this is the name by which the Domino web agent identifies that user to the Domino server. The DominoDefaultUser value can be encrypted.

    - **DominoSuperUser—**Ensures that all users successfully logged into CA SiteMinder® are logged into Domino as the DominoSuperUser. The DominoSuperUser value can be encrypted.

  - **For IIS Web Agents—**The Agent Configuration Object must include values for the DefaultUserName and DefaultPassword parameters. The DefaultUserName and DefaultPassword identify an existing Windows account that has sufficient privileges to access resources on an IIS web server protected by CA SiteMinder®. When users need to access resources on an IIS web server protected by CA SiteMinder®, they may not have the necessary server access privileges. The Web Agent must use the Windows account, which is previously assigned by an administrator, to act as a proxy user account for users granted access by CA SiteMinder®.

  Note: If you plan to use the NTLM authentication scheme, or enable the Windows User Security Context feature, do not specify values for these IIS Web Agent parameters.

Chapter 9: Installing Reports

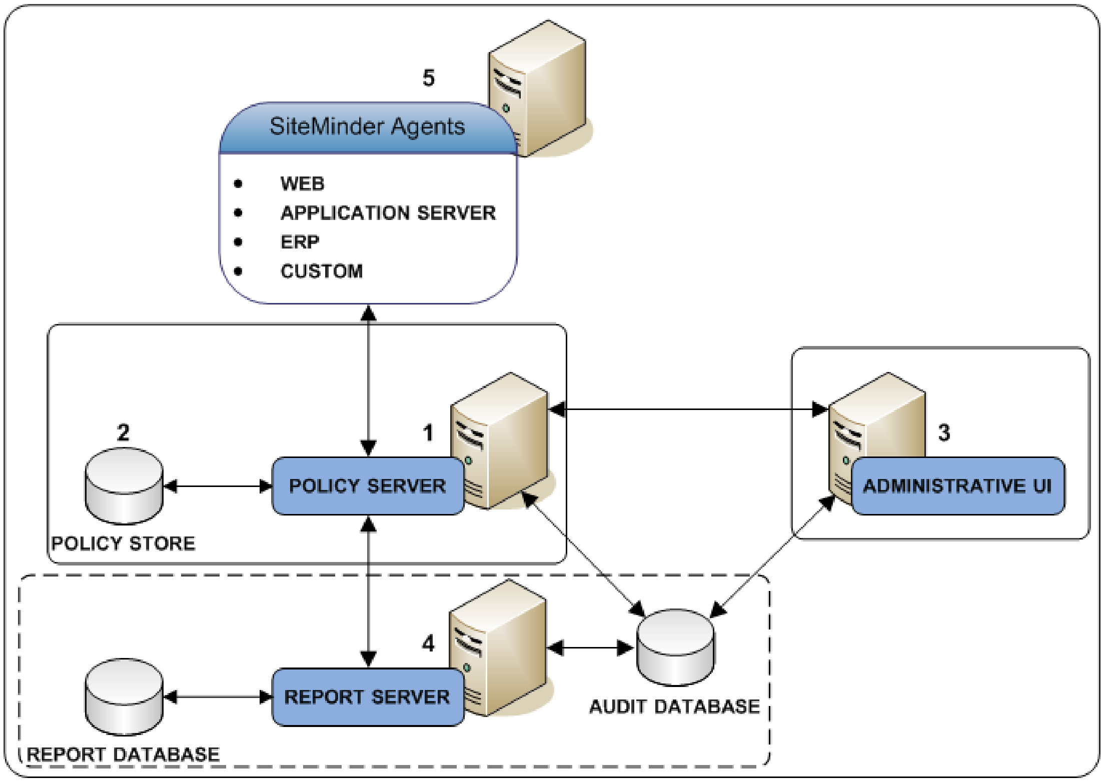
Installation Road Map

The following diagram illustrates a sample CA SiteMinder® installation and lists the order in which you install and configure each component.

- Solid lines surround the components that are required before installing and configuring reports. They include the following components:
  - A Policy Server
  - A policy store
  - An Administrative UI registered with a Policy Server.
- Dotted lines surround the components that you install and configure now. They include the following components:
  - The Report Server
  - A report database

– A CA SiteMinder® audit database.

Figure 4: Report Server Installation Road Map



Reporting Installation Checklists

Review the Report Server and report database checklists to help ensure the following:

- Your environment meets the minimum operating system and database requirements
- You complete the required prerequisite configuration

Report Server

□ Be sure that the Report Server host system meets the minimum operating system requirements:

- Windows (see page 27)
- UNIX

□ (Solaris) Install the required operating system patches to the Report Server host system.

Note: For more information, see the *Policy Server Release Notes*.

□ Be sure that the Report Server host meets the connectivity requirements (see page 29).

□ Be sure that the Report Server host name does not include any of the following characters:

- An underscore (_)
- A period (.)
- A slash (/) (\)

□ If you are reinstalling the Report Server, uninstall the current instance. The installation fails if you attempt to install over an existing instance.

□ Windows installations:

- Be sure that you have access to a user account that is a member of the local Administrators group. The user account that runs the installer must be a member of the local Administrators group.

  Important! Installing to a system where the default Windows security settings have been modified for the local Administrator group is not supported.

- Be sure that the system to which you are installing is not a domain controller. Installing to a domain controller is not supported.

□ UNIX installations:

- Be sure that the Report Server host IP is configured properly in the /etc/hosts file to avoid an IP resolution problem.
- Be sure that you have access to a root user account and a non–root user account. You require a root-user account to start the installation and a non–root user account to complete the installation. Be sure that the non–root user account:
  - Is the owner of a valid home directory.
  - Has write permissions to the home directory.

- Be sure that the following commands and utilities are installed on the operating system and available on the PATH environment variable for the root user account:
  - /bin/sh
  - uname
  - awk
  - tar
  - stty
  - pwd
  - expr
  - chown
  - id
  - ulimt
  - read
  - hostname
  - grep
  - dirname
  - which
  - touch
  - sed
  - tail
  - gzip
- Be sure that the PATH environment variable of the root–user account does not inlcude GNU or third–party replacements for core system command–line tools or an individually downloaded and compiled version of the tool.
- Set at least one of the following variables to a valid utf8/UTF-8 locale:
  - LC_ALL

    Example: export LC_ALL=en_US.UTF-8
  - LANG

    Example: export LANG=en_US.UTF-8
  - LC_CTYPE

    Example: export LC_CTYPE=en_US.UTF-8

Report Database and Audit Database

- □ If you are not using the embedded version of MySQL:
  - – Be sure that the database server host system has a fixed host name.
  - – Be sure that you are using a supported database to function as the report database (see page 29).
  - – Be sure that a new, empty database is available.
  - – Be sure that the database client and server are configured to use UTF8 character encoding. For more information about the required settings for a Unicode configuration, see your vendor-specific documentation.
- □ (SQL Server) If you are using SQL Server as a report database, an audit database, or both, complete the following items on the Report Server host system:
  - – Be sure that a CA SiteMinder® supported SQL Server driver is installed on the Report Server host system.
  - – Create a data source name (DSN) that identifies each database. The Report Server uses the DSN to communicate with each database.
- □ (Oracle) If you are using Oracle as a report database, an audit database, or both:
  - ■ Do the following items on the Report Server host system:
    - – Be sure that a supported Oracle Net client is installed.
    - – Use an Oracle Net Service Name to identify each database in the tnsnames.ora file. The Report Sever uses the service name to communicate with each database.
    - – Set the NLS_LANG variable to one of the following UTF–8 settings:

      – AMERICAN_AMERICA.WE8MSWIN1252

      – AMERICAN_AMERICA.AL32UTF8
    - – Set the ORACLE_HOME variable to *Oracle_Net_client.*

      Oracle_Net_client

      Specifies the Oracle Net client installation path.

      Windows Example: C:\oracle\product\10.2.0\client

      UNIX Example: export ORACLE_HOME=/opt/oracle/product/10.2.0/client1
    - – (Windows) Add the ORACLE_HOME variable to the system environment variables.

      Example: %Oracle_Home%\bin

   - (UNIX) Set the LD_LIBRARY_PATH variable to $ORACLE_HOME/lib32:$ORACLE_HOME/lib.

     Example:
     LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$LD_LIBRARY_PATH

   - (UNIX) Set the PATH variable to $ORACLE_HOME/bin:$PATH.

     Example: export PATH=$ORACLE_HOME/bin:$PATH

- ■ Do the following items on the database server host system: Set the NLS_LANG variable to one of the following UTF–8 settings:
   - AMERICAN_AMERICA.WE8MSWIN1252
   - AMERICAN_AMERICA.AL32UTF8

Report Database and Audit Database

□ If you are not using the embedded version of MySQL:

- Verify that the database server host system has a fixed host name.
- Verify that you are using a supported database to function as the report database (see page 29).
- Verify that a new, empty database is available.
- Verify that the database client and server are configured to use UTF-8 character encoding. For more information about the required settings for a Unicode configuration, see your vendor-specific documentation.

□ (SQL Server) If you are using SQL Server as a report database, an audit database, or both, complete the following items on the Report Server host system:

- Verify that a CA SiteMinder® supported SQL Server driver is installed on the Report Server host system.
- Create a data source name (DSN) that identifies each database. The Report Server uses the DSN to communicate with each database.
- Verify that the database is enabled for UTF-8 character encoding. For more information about the required settings for a Unicode configuration, see your SQL Server documentation.

□ (Oracle) If you are using Oracle as a report database, an audit database, or both:

- Do the following items on the Report Server host system:
  - Verify that a supported Oracle Net client is installed.
  - Verify that the database client and server are configured to use UTF-8 character encoding. For more information about the required settings for a Unicode configuration, see your vendor-specific documentation.
  - Use an Oracle Net Service Name to identify each database in the tnsnames.ora file. The Report Server uses the service name to communicate with each database.
  - Set the NLS_LANG variable to one of the following UTF–8 settings:

    – AMERICAN_AMERICA.WE8MSWIN1252

    – AMERICAN_AMERICA.AL32UTF8
  - Set the ORACLE_HOME variable to *Oracle_Net_client.*

    Oracle_Net_client

    Specifies the Oracle Net client installation path.

    Windows Example: C:\oracle\product\10.2.0\client

    UNIX Example: export ORACLE_HOME=/opt/oracle/product/10.2.0/client1
  - (Windows) Add the ORACLE_HOME variable to the system environment variables.

    Example: %Oracle_Home%\bin
  - (UNIX) Set the LD_LIBRARY_PATH variable to $ORACLE_HOME/lib32:$ORACLE_HOME/lib.

    Example: LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$LD_LIBRARY_PATH
  - (UNIX) Set the PATH variable to $ORACLE_HOME/bin:$PATH.

    Example: export PATH=$ORACLE_HOME/bin:$PATH
- Do the following items on the database server host system: Set the NLS_LANG variable to one of the following UTF–8 settings:
  - AMERICAN_AMERICA.WE8MSWIN1252
  - AMERICAN_AMERICA.AL32UTF8

Reporting Considerations

Consider the following items before installing the Report Server:

- Installing the Report Server on a host system with any other CA SiteMinder® component is not supported. Be sure to install the Report Server on a separate host system.
- A UNIX installation can take several hours. Before you install, increase the page size to 4 GB or equal to RAM size. If the installation takes longer than four hours, stop the installation and increase the page size.
- If JBoss is installed on the Report Server host system, port conflicts can occur. If you experience port conflicts after installing the Report Server, you can locate JBoss port information in the following files:
  - jboss-service.xml

    Default location: *jboss_home*\server\server_configuration\conf
  - server.xml

    Default location: *jboss_home*\server\server_configuration\deploy\jbossweb-tomcat55.sar

    jboss_home

      Specifies the JBoss installation path.

    server_configuration

      Specifies the name of your server configuration.

      Default value: default

    Note: If you change either of these files, restart JBoss. For more information, see the Red Hat documentation.
  - service-bindings.xml

    This file is only present if the Administrative UI was installed to the Report Server host system using the stand-alone option.

    Default location: *administrative_ui_install*\webadmin\conf

    administrative_ui_installation

      Specifies the Administrative UI installation path.

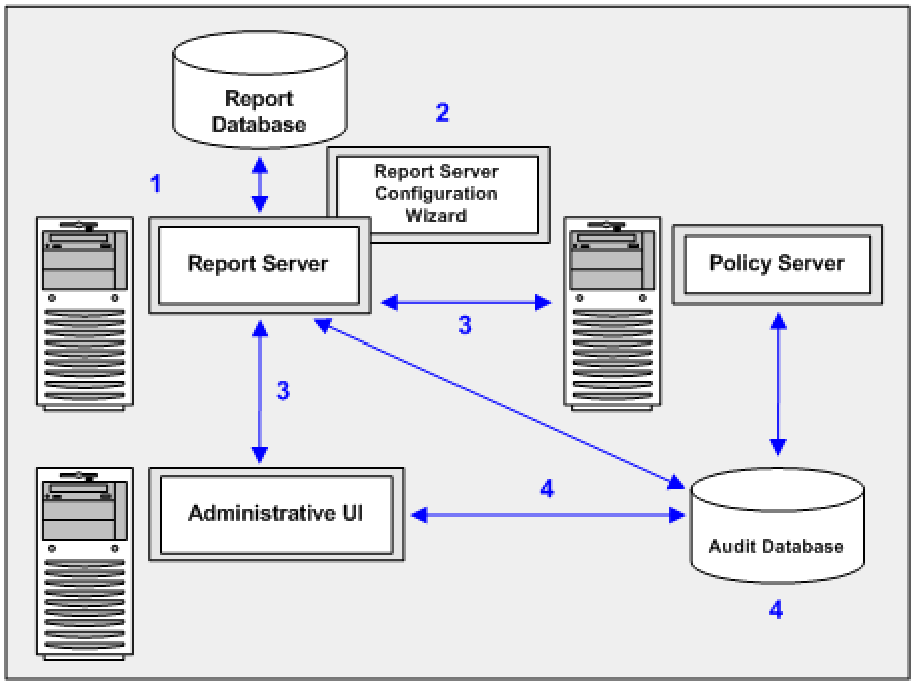
    Note: If you change this file, restart the Administrative UI application server.

More information:

Administrative UI Installation Options (see page 366)
Start the Application Server (see page 377)
Stop the Application Server (see page 380)

How the Reports Installation Works

The CA SiteMinder® reporting feature requires that you install and configure a Report Server, a report database, and a CA SiteMinder® audit database to manage CA SiteMinder® policy analysis and audit-based reports. The following diagram details a sample CA SiteMinder® environment and lists the order in which each component is installed or configured:



The following list explains each of the illustrated steps:

1. **Install the Report Server**—Installing the Report Sever is the first step in the process. You configure a report database during the installation.

2. **Install the CA SiteMinder® report templates**—Installing the CA SiteMinder® report templates is the second step in the process. The CA SiteMinder® Report Server Configuration Wizard configures the Report Server to use a set of CA SiteMinder® policy analysis and auditing report templates.

3. **Register the Report Server**—Registering the Report Server is the third step in the process. Registration requires that you configure a connection between:

   - The Report Server and a Policy Server
   - The Report Server and the Administrative UI

4. **Configure a CA SiteMinder® audit database**—Configuring a CA SiteMinder® audit database is the fourth step in the process. A separate CA SiteMinder® audit database, which is registered with the Administrative UI, is required to run audit-based reports.

How to Install the Report Server

Complete the following procedures to install the Report Server:

1. Review the installation checklists.
2. Gather information for the installer.
3. Install the Report Server.

Gather Information for the Installer

Review the following sections to identify the information required by the Report Server installer.

Installation Credentials

Depending on the operating system to which you are installing, the installer requires one or more sets of credentials:

- **(Windows and UNIX) BusinessObjects Administrator password**

  The installer creates a default SAP BusinessObjects Enterprise administrator account (administrator). You use this account to import CA SiteMinder® report templates and to access the BusinessObjects Content Management Console. Determine the password for this account.

  The password must meet the following composition criteria:

  - The password must include at least six characters.
  - The password cannot contain the word "administrator" in any form.
  - The password must include at least two of the following character types:
    - Uppercase characters
    - Lowercase characters
    - Numerals
    - Punctuation

- **(UNIX) Non–root user account**—You require a root–user account to start the installation and a non–root user account to complete the installation. Identify the non–root user account:

  - User name
  - Group name

MySQL Report Database

If you are using the embedded version of MySQL to function as the report database, the installer requires specific information. Use the report database installation worksheet to gather the following information before starting the installation:

- **MySQL root password**

  The password for the MySQL root user account.

  Note: You cannot change the name of the root user account. The installer defaults the name to root.

- **User**

  The name of the report database administrator account.

  Installer default: sa

- **Password**

  The password of the report database administrator account.

SQLAnywhere Report Database

From CA SiteMinder® 12.51, CA SiteMinder® supports CA Business Intelligence 3.3 that lets you use SQLAnywhere as a report database on only the RHEL 6 platform.

If you want to use the embedded version of SQLAnywhere to function as the report database, the installer requires specific information. Use the report database installation worksheet to gather the following information before starting the installation:

- **SQLAnywhere root password**

  The password for the SQLAnywhere root user account.

  Note: You cannot change the name of the root user account. The installer defaults the name to root.

- **User**

  The name of the report database administrator account.

  Installer default: sa

- **Password**

  The password of the report database administrator account.

Microsoft SQL Server Report Database

If you are using Microsoft SQL Server to function as the report database, the installer requires specific information. Use the report database installation worksheet to gather the following information before starting the installation:

- **Data Source Name (DSN)**

  The DSN that Report Server is to use to communicate with the report database.

  Note: The Report Server is compiled as 32–bit native binary and is designed to use 32–bit data source middleware connectivity. If you are installing to a Windows 64–bit operating system, be sure to create the DSN using odbcad32.exe. This executable is located in the following location:

  ```
  install_home\Windows\SysWOW64.
  ```

  install_home

  Specifies the installation path of the Windows operating system.

- **Login ID**

  The name of the report database administrator account. This account must have the default (DBO) account permissions.

- **Password**

  The password of the report database administrator account.

Oracle Report Database

If you are using Oracle to function as the report database, the installer requires specific information. Use the report database installation worksheet to gather the following information before starting the installation:

- **Oracle Net Client Service name**

  The service name that the Report Server is to use to communicate with the report database.

  - (Windows) The installer refers to the Oracle Net Client Service name as Server.
  - (UNIX) The installer refers to the Oracle Net Client Service name as TNSNAME.

- **User name**

  The name of the report database administrator account. This account must have the following privileges:

  - create session
  - create table
  - create procedure

  Note: You can also use an administrator account with the CONNECT and RESOURCE roles enabled. Be sure to disable the Admin Option setting for both roles.

- **Password**

  The password of the report database administrator account.

Apache Tomcat Installation

CA SiteMinder® only supports the version of Apache Tomcat that is embedded with the Report Server installation. Use the web application installation worksheet to gather the following information before starting the installation:

- **Connection port**

  The port to which Apache Tomcat is to connect and wait for requests.

  Installer default: 8080

- **Redirect port**

  Identify the port to which Apache Tomcat must redirect requests.

  Installer default: 8443

- **Shutdown port**

  The port to which the Apache Tomcat SHUTDOWN command must be issued.

  Installer default: 8005

Install the Report Server

The following sections detail how to install the Report Server on Windows and UNIX.

Before You Install

Consider the following items before you install the Report Server:

- Installing the Report Server on a host system with any other CA SiteMinder® component is not supported. Be sure to install the Report Server on a separate host system.

- You install the Report Server using the installation media on the Technical Support site.

  Note: For a list of installation media names, see the *Policy Server Release Notes*.

- The Report Server is compiled as 32–bit native binary and is designed to use 32–bit data source middleware connectivity. If you are installing to a Windows 64–bit operating system, be sure to create the DSN using odbcad32.exe. This executable is located in the following location:

  install_home\Windows\SysWOW64.

  install_home

  Specifies the installation path of the Windows operating system.

- A UNIX console installation is not supported.
- The Report Server installation includes the following components that run as processes:
  - The Content Management Server
  - The Server Intelligence Agent

  These components require TCP/IP ports to communicate. The installer lets you modify the default settings to prevent port conflicts on the Report Server host system.
- **Important!** The installation zip contains multiple folders. The installer executable requires this folder structure. If you moved the Report Server installer after extracting the zip, copy the entire folder structure to the same location. Execute the installation media from this folder structure.
- **Important!** (UNIX) The user account installing the Report Server must have executable permissions on the directory that contains the installation media. If the user account does not have these permissions, run the following command:

  ```
  chmod -R+x directory
  ```

  directory

  Specifies the directory that contains the installation media.
- (UNIX) If you execute the Report Server installer across different subnets, it can crash. Install the Report Server directly on the host system.
- (UNIX) Before you install the Report Server on an RHEL 6 machine, ensure that you complete the following tasks on the RHEL 6 machine:
  - Install the following RPMs:
    - ncurses-libs.i686
    - Compat-libstdc++-33.3.3-69.el6.i686
    - libXext-1.1-3.el6.i686
    - libXext-devel-1.1-3.el6.i686
    - ncurses-base
    - ncurses-libs 5.9-7.20121017
    - xorg-x11-libX11-7.6-23.1.2.i586
    - xorg-x11-libXau-7.6_1.0.6-9.1.1.i586
    - xorg-x11-libxcb-7.6_1.7-8.1.i586
  - Set the LD_LIBRARY_PATH environment variable to the location of the 32-bit libncurses.so.5 library.

Windows

Follow these steps:

1. Be sure that you have reviewed the installation checklists (see page 392).
2. Be sure that you have gathered the required information for the installer.
3. Exit all applications that are running.
4. Double–click *installation_media*.

   installation_media

   Specifies the Report Server installation executable.

   The CA Business Intelligence installation wizard appears and prompts you for a locale.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.
5. Select English and click OK.

   The installer introduction appears.
6. Click Next.

   The CA license agreement appears.
7. Accept the license agreement and click Next.

   The installer prompts you to install CA sample templates.
8. Select No and click Next.

   Note: CA sample templates are not related to the CA SiteMinder® reporting templates. The CA SiteMinder® Report Server Configuration wizard installs the required reporting templates. You run the wizard after installing the Report Server.

   The installer prompts you to save a response file for a silent installation.
9. Select Yes and click Next.

   An installation summary appears.
10. Review the summary and click Install.

    The installer installs the components. The CA Business Intelligence Setup wizard appears.
11. Click Next.

    The installer introduction appears.
12. Click Next.

    The SAP BusinessObjects Enterprise license agreement appears.
13. Accept the license agreement and click Next.

    The installer prompts you to select language packs. English is selected by default.

14. Leave the default English setting and click next.

    The installer prompts you for an installation type.

15. Select New and do one of the following steps to configure the report (CMS) database:

    - (Recommended) To install the embedded version of MySQL, select Install MySQL Database Server and click Next.
    - To configure an existing Microsoft SQL Server or Oracle database, select Use an existing database server and click Next.

      The installer prompts you for the Content Management Server port and the password for the SAP BusinessObjects Enterprise administrator account.

16. Complete the following steps:

    a. Specify the port on which the Content Management Server must listen.

    b. Specify a password for the default SAP BusinessObjects Enterprise administrator.

       Important! Do not select Configure the SAP BusinessObjects Enterprise Administrator password at a later time.

    c. Click Next.

       The installer prompts you for the Server Intelligence Agent node name and port.

17. Specify a node name and port. Click Next.

    The installer prompts you to configure the report (CMS) database.

    Important! The Report Server is a CA common component that CA products can share. As such, the installer lets you configure the report database to database types and versions that other products support, but CA SiteMinder® does not. For a list of supported database types and versions, see the CA SiteMinder® 12.52 Platform Support Matrix.

18. Do one of the following steps:

    - (Recommended) If you are configuring MySQL, enter the password for the root user account and the report database administrator credentials.
    - If you are configuring Microsoft SQL Server:

      a. Select SQL Server (ODBC) and click Browse to open the SQL Server Logon screen.

      b. Select a DSN and enter administrator credentials.

         Note: If you are installing on a 64-bit version of Windows, select Consume DSN created under WOW64. The option lets you use a 32–bit DSN.

      c. Click OK.

- If you are configuring Oracle, enter the required values for the service name and the administrator credentials.

  Note: Do not configure an Auditing Database. This component is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®. A CA SiteMinder® audit database is required to run audit–based reports.

19. Click Next.

    The installer prompts you to select a web application server.

20. Complete the following steps:

    a. Select Install Tomcat application server and deploy to it.

       Note: CA SiteMinder® only supports the embedded version of Apache Tomcat.

    b. Clear the IIS Web Application Server option.

    c. Click Next.

       The installer prompts you for Apache Tomcat information.

21. Enter the Apache Tomcat ports and click Next.

    The installer prompts you to start the installation.

22. Click Next to start the installation.

    The installer prompts you when the installation is complete.

23. Clear the Launch SAP BusinessObjects Administration Console option and click Finish.

    The Report Server is installed.

UNIX

Follow these steps:

1. Be sure that you have reviewed the installation checklists (see page 392).
2. Be sure that you have gathered the required information for the installer.
3. Be sure to start the installation using a root user account.
4. Exit all applications that are running.
5. Open a Bourne shell and navigate to the installation media.
6. Enter the following command:

   ```
   ./installation_media -i console
   ```

   installation_media

   Specifies the Report Server installation executable.

Note: For a list of installation media names, see the *Policy Server Release Notes*.

The CA Business Intelligence installer starts and prompts you for a locale.

7. Type the value for English and press Enter.

   The installer introduction appears.

8. Press Enter.

   The CA license agreement appears.

9. Complete the following steps:

   a. Press Enter to advance the license agreement.

   b. Type y to accept the license agreement.

   c. Press Enter.

   The installer prompts you for non–root user credentials.

10. Type the user name and group name and press Enter.

    The installer prompts you to specify the path to the CA Shared Components directory.

11. Leave the default value and press Enter.

    The installer prompts you to install CA sample templates.

12. Type N and press Enter.

    Note: CA sample templates are not related to the CA SiteMinder® reporting templates. The CA SiteMinder® Report Server Configuration wizard installs the required reporting templates. You run the wizard after installing the Report Server.

    The installer prompts you to save a response file for a silent installation.

13. Type Y and press Enter.

    An installation summary appears.

14. Review the summary and press Enter.

    The installer installs the components. The SAP BusinessObjects Enterprise installer prompts you to select an installation language.

15. Select English and press Enter.

    The SAP BusinessObjects Enterprise license agreement appears.

16. Press y to accept the license agreement.

    The installer prompts you enter the Report Server installation directory.

17. Press Tab to auto–complete the default setting and press Enter.

    The installer prompts you to select language packs. English is selected by default.

18. Leave the default and press Enter.

    The installer prompts you for an installation type.

19. Select User – Regular SAP BusinessObjects Enterprise installation and press Enter.

    The installer prompts you for an installation type.

20. Select New and press Enter.

    Note: Do not clear the Enable servers after installation option.

    The installer prompts you for the Content Management Server port and the password for the SAP BusinessObjects Enterprise administrator account.

21. Complete the following steps:

    a. Specify the port to which the Content Management Server must connect and listen for requests.

    b. Specify a password for the default SAP BusinessObjects Enterprise administrator.

    c. Press Enter.

    The installer prompts you to select the type of database that is to function as the report (CMS) database.

22. Complete one of the following steps:

    - (Recommended) To install the embedded version of MySQL, select Install MySQL and press Enter.
    - To configure an existing Oracle database, select Use an existing database server and press Enter.
    - (RHEL 6) To install SQLAnywhere, select Install SQLAnywhere and press Enter.

    Important! The Report Server is a CA common component that CA products can share. As such, the installer lets you configure the report database to database types and versions that other products support, but CA SiteMinder® does not. For a list of supported database types and versions, see the CA SiteMinder® 12.52 Platform Support Matrix.

    The installer prompts for additional report database information.

23. Complete one of the following steps:

    - (MySQL/SQLAnywhere) Enter the required values for the root user account and the report database administrator credentials.
    - (Oracle) Complete the steps:

      a. Select Oracle and press Enter.

         The installer prompts for database information.

      b. Type the service name and administrator credentials.

24. Press Enter.

    - If you are installing the embedded version of MySQL, the installer prompts you for Auditing Database information.
    - If you are configuring Oracle, the installer prompts you to install the Auditing Database.

      The Auditing Database is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®. A CA SiteMinder® audit database is required to run audit–based reports.

25. Complete one of the steps:

    - (MySQL/SQLAnywhere) Accept the defaults and press Enter.
    - (Oracle) Complete the following steps:

      a. Select the Do not install Auditing Database option.

      b. Press Enter.

         The installer prompts you to reinitialize the database.

      c. Select Yes and press Enter.

    The installer prompts you for a Service Intelligence Agent node name and port.

26. Type a node name and port and press Enter.

    The installer prompts you to select a web application server.

27. Select the Install Tomcat deploy web applications option.

    Note: CA SiteMinder® only supports the embedded version of Apache Tomcat.

    The installer prompts you for Apache Tomcat ports.

28. Type the required Apache Tomcat port information and press Enter.

    The installer displays the path of the installation directory.

29. Press Enter to start the installation.

    The installer displays the installation progress and confirms when the installation is complete.

30. Press Enter to exit the installer.

Troubleshoot the Report Server Installation

Use the following files to troubleshoot the Report Server installation:

- CA_Business_Intelligence_InstallLog.log

  We recommend opening this log first to view reported errors.

- ca-install.log

  We recommend scrolling to the bottom of this file to view reported errors. Search for “BIEK_GetExitCode” to verify the returned value of the “BIEK_GetExitCode” function. If the returned value is not 0, then there is an installation error. Search for the following keywords to determine the cause of the error:

  - Error
  - Warning
  - CMS
  - InfoStore

The log files are located in a temporary location during the installation. The TEMP environment property on the system determines the temporary location. If the installation fails, you can locate the log file in this temporary location. After a successful installation, the log files are located at the top level of the Report Server installation directory.

How to Install the Report Templates

Complete the following procedures to install the report templates:

1. Gather information for the installer.
2. Install the report templates.
3. Restart the Report Server.
4. Increase the Job Server service timeout value.

Gather Information for the Installer

The Report Server Configuration Wizard requires the following information:

- **BusinessObjects administrator password**—Identify the password for the default BusinessObjects administrator account. The Report Server installer creates a default administrative account during installation. A password for this account was required to complete the installation. The Report Server Configuration Wizard requires the password to use the default administrative account to install the report templates.

- **CA SiteMinder® audit database type**—Identify the type of database that is to function as a CA SiteMinder® audit database. A separate CA SiteMinder® audit database is required to run audit-based reports. The Report Server Configuration Wizard requires the database type to configure the Report Server to use a set of report templates based on the audit database type.

  Note: You do not have to configure a CA SiteMinder® audit database before running the Report Server Configuration Wizard.

A worksheet is provided to help you gather and record required information before installing the report templates.

Install the Report Templates

You install the CA SiteMinder® report templates with the Report Server Configuration Wizard. The following sections detail how to run the Report Server Configuration Wizard on Windows and UNIX.

Before You Install

Consider the following items before you install the report templates:

- You run the Report Server Configuration Wizard using the installation media on the Technical Support site.

  Note: For a list of installation media names, see the *Policy Server Release Notes*.

  Important! (UNIX) The installation media requires executable permissions. Run the following command to add the permission:

  ```
  chmod +x installation_media
  ```

  installation_media

  Specifies the name of the Report Server Configuration Wizard installation executable.

- (UNIX) If you execute the Report Server Configuration Wizard across different subnets, it can crash. Install the report templates directly on the Report Server host system.

Windows

To install the report templates on Windows

1. Be sure that you have gathered the required information for the installer (see page 411).
2. Exit all applications that are running.

3. Double–click *installation_media*.

   installation_media

   Specifies the name of the Report Server Configuration Wizard installation executable.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.

4. For each prompt, use your completed Report Server configuration worksheet to enter the required values.

5. Review the installation settings and click Install.

   The report templates are installed.

6. Restart the Report Server.

   The Report Server is configured to use the CA SiteMinder® report templates.

UNIX GUI

To install the report templates using a UNIX GUI

1. Be sure that you have gathered the required information for the installer (see page 411).

2. Exit all applications that are running.

3. Open a shell and navigate the installation media.

4. Enter the following command:

   ```
   ./installation_media
   ```

   installation_media

   Specifies the name of the Report Server Configuration Wizard installation executable.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.

5. For each prompt, use your completed Report Server configuration worksheet to enter the required values.

   Note: Oracle is the only supported audit database for a Solaris Report Server. If you installed the Report Server to Solaris, you are not prompted for an audit database type. The Report Server Configuration Wizard automatically installs Oracle-specific report templates.

6. Review the installation settings and click Install.

   The report templates are installed.

7. Restart the Report Server.

   The Report Server is configured to use the CA SiteMinder® report templates.

UNIX Console

To install the report templates using a UNIX console

1. Be sure that you have gathered the required information for the installer (see page 411).

2. Exit all applications that are running.

3. Open a shell and navigate to the installation media.

4. Enter the following command:

   ```
   ./installation_media -i console
   ```

   installation_media

   Specifies the name of the Report Server Configuration Wizard installation executable.

   -i console

   Specifies that installation start in a UNIX console.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.

5. For each prompt, use your completed Report Server configuration worksheet to enter the required values.

   Note: Oracle is the only supported audit database for a Solaris Report Server. If you installed the Report Server to Solaris, you are not prompted for an audit database type. The Report Server Configuration Wizard automatically installs Oracle-specific report templates.

6. Review the installation settings and press Enter.

   The report templates are installed.

7. Restart the Report Server.

   The Report Server is configured to use the CA SiteMinder® report templates.

Increase the Job Server Service Timeout Value

Some of the Report Server services have a default timeout of 10 minutes. The Report Server can take longer than 10 minutes to generate large analysis reports.

Increase the timeout value of the Crystal Reports Job Server service to be sure that large analysis reports are successfully generated.

Increase the Timeout Value on Windows

Follow these steps:

1. Click Start, Programs, BusinessObjects XI Release 3.1, BusinessObjects Enterprise, Central Configuration Manager.

   The Central Configuration Manager console appears.

2. Right-click Crystal Reports Job Server and select Stop.

   The Crystal Reports Job Server service stops.

3. Right-click Crystal Reports Job Server and select Properties.

   The Crystal Reports Job Server Properties dialog appears.

4. From the Properties tab, append the following entry to the end of the string in the Command field:

   ```
   -requesttimeout 6000000
   ```

   Note: The timeout value is measured in milliseconds. Specifying 6000000 increases the timeout value to one (1) hour.

5. Click OK.

   The Central Configuration Manager appears.

6. Right-click Crystal Reports Job Server and select Start.

   The Crystal Reports Job Server service starts.

7. Exit the Central Configuration Manager.

   The timeout value for the Crystal Reports Job Server service is set to one (1) hour.

Increase the Timeout Value on UNIX

Follow these steps:

1. Navigate to *report_server_home*/CommonReporting3/bobje.

   report_server_home

   Specifies the Report Server installation path.

2. Open the ccm.config file, and append the following entry to the end of the value for reportjobserverLAUNCH key:

   ```
   -requesttimeout 6000000
   ```

   Note: The timeout value is measured in milliseconds. Specifying 6000000 increases the timeout value to one (1) hour.

3. Save and close the ccm.config file.

   The timeout value for the Crystal Reports Job Server service is set to one (1) hour.

How to Register the Report Server

Registering the Report Server requires access to the Policy Server host system, the Report Server host system, and the Administrative UI host system. The registration process:

- Establishes a trusted relationship between the Report Server and the Policy Server.
- Establishes a trusted relationship between the Report Server and the Administrative UI.

Complete the following steps to register the Report Server:

1. Create the client name and passphrase.
2. Gather the registration information.
3. Register the Report Server with a Policy Server.
4. Restart the Report Server.
5. Configure the connection to the Administrative UI.

Create a Client Name and Passphrase

You run the XPSRegClient utility to create a client name and passphrase. A client name and passphrase are:

- Values that the Policy Server uses to identify the Report Server you are registering
- Values that you use with the XPSRegClient tool to register the Report Server with the Policy Server

To run the registration tool

1. Open a command–line window from the Policy Server host system.
2. Navigate to *siteminder_home*/bin.

   siteminder_home

   Specifies the Policy Server installation path.

3. Run the following command:

   ```
   XPSRegClient client_name[:passphrase] -report -t timeout -r retries
   -c comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   client_name

   Identifies the name of Report Server you are registering.

   Limit: The value must be unique. For example, if you have previously used reportserver1, enter reportserver2.

   Note: Record this value. This value is required to complete registration process from the Report Server host system.

   passphrase

   Specifies the password required to complete the Report Server registration.

   Limits: The passphrase

   - Must contain at least six (6) characters.
   - The passphrase cannot include an ampersand (&) or an asterisk (*).
   - If the passphrase contains a space, it must be enclosed in quotation marks.

   If you do not specify the passphrase in this step, XPSRegClient prompts you to enter and confirm it.

   Note: Record this value. This value is required to complete registration process from the Report Server host system.

   -report

   Specifies that a Report Server is being registered.

   -t *timeout*

   (Optional) Specifies how long you have to complete the registration process from the Report Server host system. The Policy Server denies the registration request when the timeout value is reached.

   Unit of measurement: minutes

   Default: 240 (4 hours)

   Minimum Limit: 1

   Maximum Limit: 1440 (one day)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you complete the registration process from the Report Server host system. A failed attempt can result from submitting an incorrect passphrase to the Policy Server during the registration.

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The registration tool prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comment with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: siteminder_home\log, where siteminder_home is where the Policy Server is installed.

-e *error path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

The utility lists the name of the registration log file. If you did not provide a passphrase, the utility prompts for one.

4. Press Enter.

   The registration tool creates the client name and passphrase.

You can now register the Report Server with the Policy Server. You complete the registration process from the Report Server host system.

Gather Registration Information

Completing the registration process between the Report Server and the Policy Server requires specific information. Gather the following information before running the XPSRegClient utility from the Report Server host system.

- **Client name**—The client name you specified using the XPSRegClient tool.
- **Passphrase**—The passphrase you specified using the XPSRegClient tool.
- **Policy Server host**—The IP address or name of the Policy Server host system.

Register the Report Server with the Policy Server

You register the Report Server with the Policy Server to create a trusted relationship between both components. You configure the connection from the Report Server host system using the Report Server registration tool.

Follow these steps:

1. From the Report Server host system, open a command–line window and navigate to *report_server_home*\external\scripts.

   report_server_home

   Specifies the Report Server installation location.

   Default: (Windows) C:\Program Files\CA\SC\CommonReporting3

   Default: (UNIX) /opt/CA/SharedComponents/CommonReporting3

2. Run one of the following commands:

   - (Windows)

     ```
     regreportserver.bat -pshost host_name -client client_name -passphrase
     passphrase -psport portnum -fipsmode 0|1
     ```

     Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   - (UNIX)

     ```
     regreportserver.sh -pshost host_name -client client_name -passphrase
     passphrase -psport portnum -fipsmode 0|1
     ```

-pshost *host name*

Specifies the IP address or name of the Policy Server host system to which you are registering the Report Server.

-client *client name*

Specifies the client name. The client name identifies the Report Server instance that you are registering.

Note: This value must match the client name that you specified using the XPSRegClient utility when you registered the Report Server on the Policy Server host system.

Example: If you specified "reportserver1" when using the XPSRegClient utility, enter "reportserver1".

-passphrase *passphrase*

Specifies the passphrase that is paired with the client name. The client name identifies the Report Server instance that you are registering.

Note: This value must match the passphrase that you specified using the XPSRegClient utility when you registered the Report Server on the Policy Server host system.

Example: If you specified CA SiteMinder® when using the XPSRegClient utility, enter CA SiteMinder®.

-psport *portnum*

(optional) Specifies the port on which the Policy Server is listening for the registration request.

fipsmode

(optional) Specifies how the communication between the Report Server and the Policy Server is encrypted.

Default: 0

- Zero (0) specifies FIPS–compatibility mode.
- One (1) specifies FIPS–only mode.

3. Press Enter.

   You receive a message stating that the registration is successful.

Restart the Report Server

(Windows) Follow these steps:

1. Click Start, Programs, BusinessObjects XI 3.1, BusinessObjects Enterprise, Central Configuration Manager.

   The Central Configuration Manager console appears.

2. Stop the Apache Tomcat and Server Intelligence Agent Services.

   The Report Server stops.

3. Start the Apache Tomcat and Server Intelligence Agent Services.

   The Report Server is restarted.

(UNIX) Follow these steps:

1. Log in to the system as the non–root user that installed the Report Server.
2. Be sure that at least one of the following environment variables is set to a valid utf8/UTF-8 locale:
   - LC_ALL
   - LANG
   - LC_CTYPE
3. Navigate to r*eport_server_hom*e/CommonReporting3/external/scripts and run the following command:

```
../setupenv.sh
```

report_server_home

Specifies the Report Server installation path.

4. Be sure that:

   - The IAM_RPTSRV_HOME variable is set to *report_server_home*/CommonReporting3.

     report_server_home

     Specifies the Report Server installation path.

   - (Oracle report database only) The LD_LIBRARY_PATH variable is set as follows:

     ```
     $ORACLE_HOME/lib32:$ORACLE_HOME/lib:$LD_LIBRARY_PATH
     ```

     Example:

     ```
     export
     LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$LD_LIB
     RARY_PATH
     ```

5. Navigate to report_*server_home*/CommonReporting3/bobje and run the following command:

   ```
   ./stopservers
   ```

   report_server_home

   Specifies the Report Server installation path.

6. Run the following command:

   ```
   ./tomcatshutdown.sh
   ```

   The Report Server stops.

7. Run the following command:

   ```
   ./startservers
   ```

8. Run the following command:

   ```
   ./tomcatstartup.sh
   ```

   The Report Server is restarted.

Configure the Connection to the Administrative UI

You configure the Report Server and Administrative UI connection to configure a trusted relationship between both components. You configure the connection from the Administrative UI.

Note: The Administrative UI can have a trusted relationship with one or more Policy Servers. However, each trusted relationship only allows one Report Server connection. If you must connect to a new Report Server, either delete the current Report Server connection or connect to another Policy Server to configure the connection.

To configure the connection to the Administrative UI

1. Log into the Administrative UI.
2. Click Administration, Admin UI.
3. Click Report Connections, Create Report Server Connection.

   The Create Report Server Connection pane appears.

   Note: Click Help for descriptions of settings and controls, including their respective requirements and limits.
4. Type a connection name in the Connection Name field.
5. Type the Report Server host system name or IP address in the Report Server Host field.
6. Enter the Apache Tomcat connection port in the Tomcat Port field.

   Note: This value is the web server port you entered when installing the Report Server.
7. Enter the administrator password in the respective fields.

   Note: This value is the password you entered for the default BusinessObjects administrator account when installing the Report Server.
8. Click Submit.

   The connection between the Report Server and the Administrative UI is configured.

You have completed installing and registering the Report Server. You can now run policy analysis reports.

Note: Creating and managing audit reports requires a separate audit database.

How to Configure an Audit Database

A CA SiteMinder® audit database is required to run CA SiteMinder® audit–based reports.

Note: Although you can write audit information to a text file, you must store your audit information in a supported ODBC database to create and manage audit-based reports. For a list of the supported versions, see the CA SiteMinder® 12.52 Platform Support Matrix.

Complete the following steps to configure an audit database:

1. (Optional) If you have not already done so, configure a CA SiteMinder® audit database.

   Important! If you are configuring the audit database in Oracle, be sure that the user account you supply does not have the DB role. If the user account has the DB role, audit–based reports do not return correct results.

2. Register the audit database with the Administrative UI.
3. Configure connectivity between the audit database and the Report Server.

Register the Audit Database with the Administrative UI

You register the audit database with the Administrative UI to create a trusted connection between the components. Registering the audit database with the Administrative UI lets CA SiteMinder® administrators create and manage audit-based reports.

Note: The Administrative UI can have a trusted relationship with one or more Policy Servers. However, each trusted relationship only allows one audit database connection. If you must connect to a new audit database, either delete the current connection or connect to another Policy Server to configure the connection.

To register the audit database with the Administrative UI

1. Log in to the Administrative UI.
2. Click Administration, Admin UI.
3. Click Report Connections, Create Audit Report Connection.

   The Create Audit Report Connection pane appears.

   Note: Click Help for descriptions of settings and controls, including their respective requirements and limits.

4. Select the database vendor from the Database Vendor drop-down list.

   The vendor-specific fields appear.

5. Type the name of the connection in the Connection Name field.
6. Enter the audit database host system name or IP address in the Database Server Host field.

7. Enter the audit database data source information in the DSN field:

   - **Oracle**—Enter the Oracle Net Service name you specified when creating the audit database DSN.

     Note: The service name must be associated with the DSN you entered in the Data Tab of the Policy Server Management Console when configuring the audit database connection to the Policy Server. The service name must match the DSN you create on the Report Server.

   - **SQL Server**—Enter the DSN.

     Note: The DSN name must match the DSN you specified in the Data Tab of the Policy Server Management Console when configuring the audit database connection to the Policy Server. The DSN name must also match the DSN you create on the Report Server.

8. Enter the port on which the audit database server is listening in the Database Server Port field.

9. Complete *one* of the following steps:

   - **Oracle**—Re–enter the Oracle Net Service Name in the Service Name field.
   - **SQL Server**—Enter the audit database name in the Database Name field.

10. Enter administrator credentials for the audit database in the respective fields.

    Note: The administrator credentials must match the credentials that you specified in the Data tab of the Policy Server Management Console when configuring the audit database connection to the Policy Server.

11. Click Submit.

    The audit database is registered with the Administrative UI.

Audit Database and Report Server Connectivity

A Report Server connects to a CA SiteMinder® audit database to create audit-based reports. When an audit-based report is scheduled in the Administrative UI, the Administrative UI passes the following connection information to the Report Server:

- (Oracle) The Oracle Net Service Name that identifies the audit database
- (Microsoft SQL Server) The name of the:
  - Audit database
  - Data source used to connect to audit database
- The user account credentials required to access the audit database

To configure connectivity between the audit database and the Report Server, do one of the following:

- (Oracle) Be sure that the:
  - Oracle Net client is installed to the Report Server host system.
  - Oracle Net Service Name that identifies the audit database is present in the tnsnames.ora file on the Report Server host system.
- (Microsoft SQL Server) Be sure that the data source used to connect to the audit database is present on the Report Server host system.

Note: For more information about supported database drivers, see the 12.52 CA SiteMinder® Platform Support Matrix.

Start the Report Server

(Windows) Follow these steps:

1. Click Start, Programs, BusinessObjects XI 3.1, BusinessObjects Enterprise, Central Configuration Manager.

   The Central Configuration Manager console appears.

2. Start the Apache Tomcat and Server Intelligence Agent Services.

   The Report Server is started.

(UNIX) Follow these steps:

1. Log in to the system as the non–root user that installed the Report Server.
2. Be sure that at least one of the following environment variables is set to a valid utf8/UTF-8 locale:
   - LC_ALL
   - LANG
   - LC_CTYPE
3. Navigate to *report_server_hom*e/CommonReporting3/external/scripts and run the following script:

   ```
   ../setupenv.sh
   ```

   report_server_home

   Specifies the Report Server installation path.

4. Be sure that:

   - The IAM_RPTSRV_HOME variable is set to *report_server_home*/CommonReporting3.

     report_server_home

     Specifies the Report Server installation path.

   - (Oracle report database only) The LD_LIBRARY_PATH variable is set to $ORACLE_HOME/lib32:$ORACLE_HOME/lib:$ETPKIHOME/lib:$LD_LIBRARY_PATH

     Example: export LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$ETPKIHOME/lib:$LD_LIBRARY_PATH

   - The ETPKIHOME variable is set to r*eport_server_hom*e/CommonReporting3.

     *report_server_hom*e

     Specifies the Report Server installation path.

5. Navigate to r*eport_server_hom*e/CommonReporting3/bobje

   ***report_server_hom*e**

   Specifies the Report Server installation path.

6. Run the following command:

   ```
   ./startservers
   ```

7. Run the following command:

   ```
   ./tomcatstartup.sh
   ```

   The Report Server is started.

Stop the Report Server

(Windows) Follow these steps:

1. Click Start, Programs, BusinessObjects XI 3.1, BusinessObjects Enterprise, Central Configuration Manager.

   The Central Configuration Manager console appears.

2. Stop the Apache Tomcat and Server Intelligence Agent Services.

   The Report Server is stopped.

(UNIX) Follow these steps:

1. Log in to the system as the non–root user that installed the Report Server.
2. Be sure that at least one of the following environment variables is set to a valid utf8/UTF-8 locale:
   - LC_ALL
   - LANG
   - LC_CTYPE
3. Navigate to r*eport_server_hom*e/CommonReporting3/external/scripts and run the following command:

   ```
   ../setupenv.sh
   ```

   report_server_home

   Specifies the Report Server installation path.

4. Be sure that:
   - The IAM_RPTSRV_HOME variable is set to *report_server_home*/CommonReporting3.

     report_server_home

     Specifies the Report Server installation path.

   - (Oracle report database only) The LD_LIBRARY_PATH variable is set to $ORACLE_HOME/lib32:$ORACLE_HOME/lib:$ETPKIHOME/lib:$LD_LIBRARY_PATH

     Example: export LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$ETPKIHOME/lib:$LD_LIBRARY_PATH

   - The ETPKIHOME variable is set to r*eport_server_hom*e/CommonReporting3.

     *report_server_hom*e

     Specifies the Report Server installation path.

5. Navigate to *report_server_home*/CommonReporting3/bobje.

   report_server_home

   Specifies the Report Server installation path.

6. Run the following command:

   ```
   ./stopservers
   ```

7. Run the following command:

   ```
   ./tomcatshutdown.sh
   ```

   The Report Server is stopped.

How to Uninstall Reporting

Complete the following procedures to uninstall CA SiteMinder® reports:

1. Uninstall the CA SiteMinder® Report Server Configuration Wizard.
2. Uninstall the Report Server.
3. Remove leftover items.
4. Remove the report database tables.

Uninstall the Report Server Configuration Wizard from Windows

Follow these steps:

1. Exit all applications that are running.
2. Navigate to *report_server_home*\CommonReporting3\Uninstall_CASiteMinder_ConfigurationWizard.

   report_server_home

   Specifies the Report Server installation path.

   Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your CA SiteMinder® component.

3. Double-click uninstall.exe.

   The wizard starts.

4. Follow the prompts.

   Note: If a message prompts you to remove shared files, click No to All.

5. If requested, restart the system.

   The Report Server Configuration Wizard is uninstalled.

Uninstall the Report Server Configuration Wizard from UNIX

Follow these steps:

1. Exit all applications that are running.
2. Navigate to *report_server_home/*CommonReporting3/Uninstall_CASiteMinder_ConfigurationWizard.

   report_server_home

   Specifies the Report Server installation path.

3. Run the following command:

   ```
   ./uninstall
   ```

   The process starts.

4. Follow the prompts.

   The Report Server Configuration Wizard is uninstalled.

Uninstall the Report Server from Windows

Follow these steps:

1. Exit all applications that are running.
2. Navigate to r*eport_server_home*\CommonReporting3\Uninstall CA Business Intelligence 3.2.

   report_server_home

   Specifies the Report Server installation path.

3. Double-click Uninstall CA Business Intelligence 3.2.exe

   Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your CA SiteMinder® component.

   The uninstaller starts.

   Note: If you installed the Report Server silently, the uninstaller starts silently. If you want to uninstall using a wizard:

a. Open a command prompt.

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

b. Navigate to r*eport_server_home*\CommonReporting3\Uninstall CA Business Intelligence 3.2.

c. Enter the following command:

```
Uninstall CA Business Intelligence 3.2.exe -i swing
```

4. Follow the prompts.

   Consider the following items:

   - If a message prompts you to remove shared files, click No to All.
   - If a message prompts you to close the Java Platform SE binary and BOE120MySQL, select the Do not close applications and click OK.

5. If requested, reboot the system.

   The Report Server is uninstalled.

Note: Uninstalling the Report Server does not remove the tables in the report database. Manually remove these tables.

Uninstall the Report Server from UNIX

Do not manually remove the installation directories to uninstall this component. Execute the uninstall shell script. If you only remove the installation directories, related registries can be left behind. If you try to re–install this component on this host system, the entries can prevent a successful installation.

Follow these steps:

1. Open a Bourne shell and navigate to *report_server_home*/CommonReporting3/Uninstall.

   report_server_home

   Specifies the Report Server installation path.

2. Run the following command:

```
./UninstallCABusinessIntelligence 3.2
```

   The process starts.

3. Follow the prompts.

   The Report Server is uninstalled.

Note: Uninstalling the Report Server does not remove the tables in the report database. Manually remove these tables.

Remove Windows Items

You manually remove leftover items to keep the system as clean as possible. If you reinstall the Report Server to the same system, removing leftover items prevents the Report Server installation from failing.

Follow these steps:

1. Navigate to *report_server_home*.

   report_server_home

   Specifies the Report Server installation path.

2. Delete the following directory:

   CommonReporting3

   You have removed the leftover items.

Remove UNIX Items

You manually remove leftover items to keep the system as clean as possible. If you reinstall the Report Server to the same system, removing leftover items prevents the Report Server installation from failing.

Important! Other CA products can share the SharedComponents directory. The profile.CA file sets the environment variables for this location. Be sure that no other CA products are sharing the SharedComponets directory before you remove this file.

Follow these steps:

1. Navigate to *report_server_home*

   report_server_home

   Specifies the Report Server installation path.

2. Delete the following folder:

   CommonReporting

3. Navigate to /etc.
4. Remove the following file:

   profile.CA

   You have removed the leftover items.

Remove the Report Database Tables

Uninstalling the Report Server does not remove the tables in the report database. Access the database functioning as the report database and manually remove all tables.

Delete a Report Server Connection to the Administrative UI

You delete a Report Server connection when the connection is no longer required.

To delete a Report Server connection

1. Click Administration, Admin UI.
2. Click Report Connections, Delete Report Server Connection.

   The Delete Report Server Connection pane appears.
3. Specify search criteria and click Search.

   The Report Server connection matching the criteria appears.
4. Select the connection and click Select.

   You are prompted to confirm that the connection can be deleted.
5. Click Yes.

   The Report Server connection is deleted.

Reinstall the Report Server

If you are reinstalling the Report Server, uninstall the existing instance before reinstalling. If you reinstall over an existing instance, the installation fails.

More information:

How to Uninstall Reporting (see page 429)

Chapter 10: Configuring the OneView Monitor

This section contains the following topics:

OneView Monitor Overview

The OneView Monitoring infrastructure consists of a number of modules that enable the monitoring of CA SiteMinder® components. Included is the Monitor process that runs in the context of a Java Runtime Environment (JRE). The Monitor GUI's HTML pages are generated by Java Server Pages (JSPs) and servlets hosted on a ServletExec servlet engine running on the same machine as the Policy Server.

The OneView Monitor utility monitors the following CA SiteMinder® components:

- Policy Server
- Web Agents

Note: More information about using the OneView Monitor exists in the *Policy Server Administration Guide*.

System Requirements for OneView Monitor

The system to which you are configuring the OneView Monitor GUI must meet at least the following system requirements:

- **JDK**—The required version of the Java SDK is installed on the system.
- **Servlet Engine**—The required version of ServletExec is installed on the system.

  Note: The Policy Server installation kit includes the installation executable for ServletExec/AS at the following location:

  ```
  thirdparty-tools\servlet-engine-6.0
  ```
- **Web server**—A supported Web server is installed on the system.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

Configure the OneView Monitor

If you did not configure the OneView Monitor GUI when installing the Policy Server, you can configure it using the Policy Server Configuration Wizard.

You can find the following Policy Server Configuration Wizard executables in *siteminder_home*\siteminder\install_config_info for Windows and *siteminder_home*/siteminder/install_config_info for UNIX:

- ca-ps-config.exe

  Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your CA SiteMinder® component.
- ca-ps-config.bin

siteminder_home

Specifies the path to where the Policy Server is installed.

Limitation of OneView Monitor GUI/IIS Web Agent on Same Machine

CA does not support the configuration of the IIS-based OneView Monitor GUI and the IIS Web Agent on the same machine if the Agent has Registration Services enabled. With this configuration, there is a conflict with the same instance of ServletExec.

How to Configure the OneView Monitor GUI on Windows/IIS

To configure the OneView Monitor GUI on Windows/IIS complete the following procedures:

1. Read the prerequisites to installing ServletExec on Windows.
2. Install ServletExec/ISAPI on Windows/IIS.

   Note: The Monitor GUI's HTML pages are generated by Java Server Pages (JSPs) and servlets hosted on a ServletExec servlet engine running on the same machine as the Policy Server.

3. Assign modify permissions to the Internet guest account for the *policy_server_home*\monitor\settings folder.
4. Set permissions for the IIS Users.
5. If you did not have the Policy Server installation program auto-configure the OneView Monitor GUI, configure it by running the Policy Server Configuration Wizard.
6. Start the OneView Monitor service.
7. Access the OneView Monitor GUI.

Prerequisites to Installing ServletExec on Windows

Consider the following prerequisites before installing ServletExec:

- ServletExec is a third–party product. We recommend that you read the ServletExec documentation before installing the component.

  Note: For more information, see the New Atlanta web site.

- The Policy Server requires a 32–bit JDK when installed to a supported 64–bit Windows operating system. If you are installing ServletExec/AS 6.0 to a 64–bit Windows operating system, ServletExec requires a 64–bit JVM. If necessary, install a 64–bit JVM before installing ServletExec.

Install ServletExec on Windows IIS

Follow these steps:

1. If you have a previous version of ServletExec, back it up.
2. Run the ServletExec installation executable.

   Note: The Policy Server installation kit includes the installation executable for ServletExec/AS 6.0 at the following location:

   ```
   thirdparty-tools\servlet-engine-6.0
   ```

   Note: For more information about upgrading and installing ServletExec, see the New Atlanta documentation.

3. If you installed a 64–bit JVM as a ServletExec/AS prerequisite, complete the following steps:

   a. Use the Services control panel to stop the ServletExec service.

   b. (Optional) Uninstall the 64–bit JVM.

   c. Edit the StartServletExec.bat and StopServletExec.bat files to point to the 32–bit JVM.

   d. Use the Services control panel to start the ServletExec service.

4. Stop and restart the IIS Admin Web service and IIS Web server.

Set Permissions for IIS Users After Installing ServletExec

Since ServletExec/AS runs as part of the IIS process, it runs as different users at different times. As a result, you must set the following permissions for the ServletExec installation directory and subdirectories.

To set permissions for IIS users after installing ServletExec, Make sure the user that runs IIS (for example, Network Services) has read and write access to the entire directory tree under C:\Program Files\New Atlanta.

How to Configure the OneView Monitor GUI on UNIX/Sun Java System

To configure the OneView Monitor GUI on a UNIX/Sun Java System complete the following procedures:

1. Read the prerequisites to installing ServletExec.
2. Disable servlets in Sun Java System (Sun One/iPlanet) 6.0.
3. Install ServletExec/AS on UNIX/Sun Java System.

4. If you did not have the Policy Server installation program auto-configure the OneView Monitor GUI, configure it by running the Policy Server Configuration Wizard.
5. Start the OneView Monitor Service.
6. Access the OneView Monitor GUI.

Prerequisites to Installing ServletExec

CA recommends that you read the ServletExec documentation before installing ServletExec. If ServletExec is not running properly, then the OneView Monitor GUI does not work since it relies on ServletExec's servlet engine.

You can access the ServletExec documentation on the New Atlanta Web site.

Disable Servlets in Sun Java System 6.0

Ensure you follow the steps in this section before installing ServletExec.

To disable servlets in Sun Java System 6.0

1. Open the Sun Java System Enterprise Administration Server home page by entering the following URL in a browser: http://<yourserver.com>:<portnumber>

   yourserver.com

   Specifies the domain name of the Enterprise Administration Server

   port

   Specifies the port number

2. In the Select a Server drop-down menu, select the target server, and then click Manage.
3. Select the Java tab.
4. Deselect Enable Java for class defaultclass and Enable Java Globally and click OK.
5. Stop and restart the Web server so the settings can take effect.

Install ServletExec/AS on UNIX/Sun Java System

The Monitor GUI's HTML pages are generated by Java Server Pages (JSPs) and servlets hosted on a ServletExec servlet engine running on the same machine as the Policy Server.

To install ServletExec

1. Log in to the UNIX account where you want to install the Policy Server.

   Note: You must log in as the same user who installed the Sun Java System Web server.

2. Run the ServletExec AS installer.

   Note: For more information on running the ServletExec AS installer, refer to New Atlanta Communications' ServletExec documentation. Consider the following before installing ServletExec:

   - Make sure you have permission to create a new file in /tmp. New Atlanta recommends installing ServletExec in /usr/local/NewAtlanta. Installing ServletExec in /usr/local/NewAtlanta may change the permissions for the obj.conf file and the Sun Java System start script. After the installation, be sure the owner of obj.conf and the start script is the same user who owns the Web server.

   - When prompted, install a Web server adaptor and an instance of ServletExec.

   - When prompted, ensure that the installer does not modify the Web server's configuration files. If you let the installer modify the Web server’s obj.conf and magnus.conf configuration files, the Web server instance fails to run after you configure the OneView Monitor GUI on this instance.

3. After the installation program completes, restart the Web server.

More Information:

Start the OneView Monitor Service (see page 441)

Start the OneView Monitor Service

To start the OneView Monitor service

1. Make sure the IPC port numbers are available.

   The OneView Monitor uses the following port numbers to communicate with the Policy Server processes:

   - Monitoring Agent: 44449
   - Monitor: 44450

   To see which port numbers are unavailable, open a Command Window and enter:

   ```
   netstat -an
   ```

   Note: For more information on changing the port numbers, see the P*oli*cy Server Administration Guide.

2. Using the Status tab of the Policy Server Management Console, start the Monitor service.

Access the OneView Monitor GUI

To access the OneView Monitor GUI

Enter the following URL in a browser:

http://*server:<portnumber>*/sitemindermonitor

server

Specifies the Web Server's IP Address

portnumber

Specifies the port number.

Monitor a Policy Server Cluster

The OneView Monitor can be configured to monitor a Policy Server cluster when one Policy Server is set up as a centralized monitor for other Policy Servers in a cluster.

Note: More information about using the OneView Monitor exists in the *Policy Server Administration Guide*.

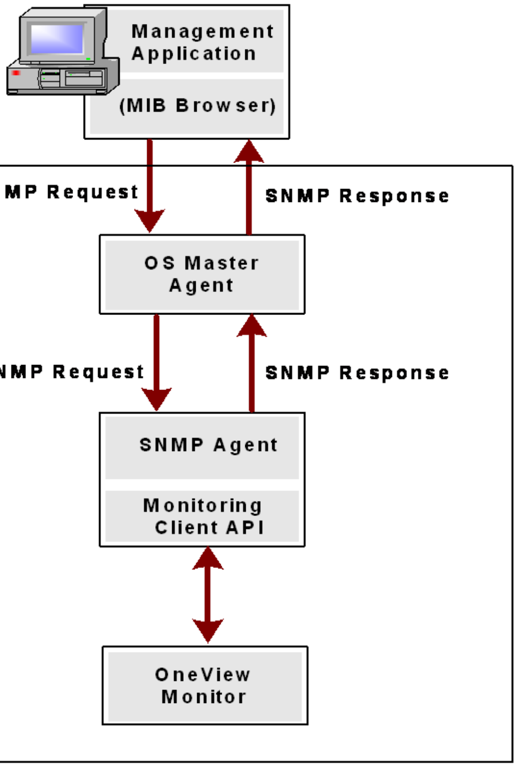
Chapter 11: SNMP Support

This section contains the following topics:

SNMP Support Overview

SNMP support includes a Management Information Base (MIB), an SNMP Agent, and the Event SNMP Trap library. You can configure the SNMP Agent and Event SNMP Trap library independently and enable one or disable the other or vice versa. The SNMP Agent enables monitoring applications to retrieve operational data from the OneView Monitor. The SNMP Agent sends data to the SNMP manager and supports SNMP request handling.

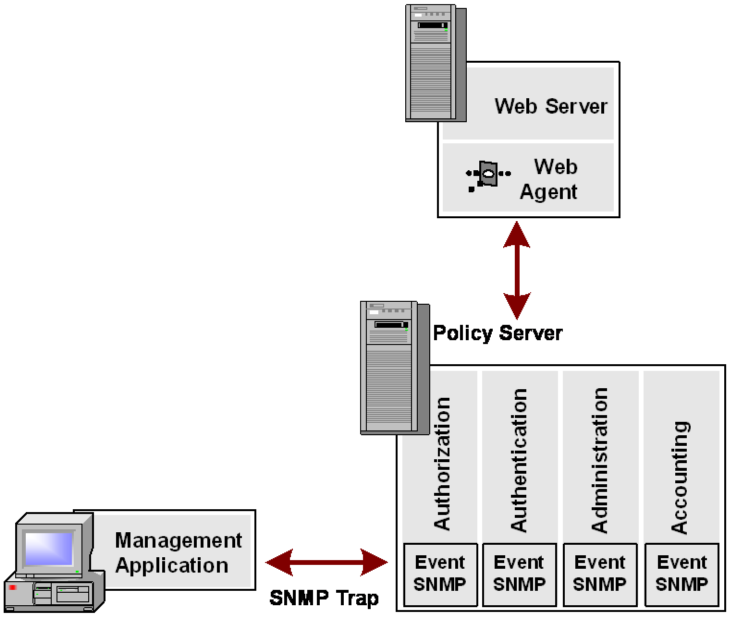
The following figure shows the architecture between the management application, OS Master Agent, SNMP Agent, and the OneView Monitor.



The OS Master Agent, such as the native Solaris SunSolstice Master Agent, invokes the SNMP Agent once you restart the Master Agent. Upon receiving an SNMP request from the management application the OS Master Agent forwards the SNMP request to the SNMP Agent. The SNMP Agent contacts the OneView Monitor, retrieves the required information using Monitor Client API, and then sends the response to the Master Agent. The Master Agent, in turn, forwards the response to the management application.

If you do not configure the SNMP Agent during the Policy Server installation, all the SNMP files are still installed in case you want to use the Agent later. However, to get the Agent running, you need to manually get the Agent started by configuring the SNMP Agent on a Windows or UNIX system.

The Event SNMP Trap library converts some CA SiteMinder® events into SNMP traps before sending them to the management application as noted in the following figure. The trap library captures events sent by the Policy Server, decides if SNMP traps are to be generated on a given event, and generates a trap.



Note: For more information on the SNMP Agent and the OneView Monitor, see the *Policy Server Administration Guide*.

Prerequisites for Windows and UNIX Systems

You need to have a Master Agent installed with your operating system before installing or using the SNMP Agent.

Windows Prerequisites

SiteMinder SNMP support on Windows requires the SNMP service. For more information about installing the SNMP service, see the Windows online help system.

UNIX Systems Prerequisites

The following section details UNIX prerequisites for SNMP support:

Solaris

You need the native Solaris SunSolstice Master Agent, which comes with the operating system.

Linux

For the supported Master Agent on Red Hat Advanced Server 3.0, upgrade the net–snmp package to net-snmp-5.1-2.1 or greater.

To upgrade the net–snmp package to net-snmp-5.1-2.1 or greater, use the following setting in the snmpd.conf file for the net–snmpd command:

```
proxy -c public -v 1 localhost:8001 .1.3.6.1.4.1.2552
```

Note: After you upgrade the net–snmp package, add proxy support to the snmpd.conf file.

You can find the snmpd.conf file specific to CA SiteMinder® in the following location (The host usually has many snmpd.conf files):

```
/opt/siteminder/etc/snmp/conf/snmpd.conf
```

Configure the SNMP Agent on Windows

To configure the SNMP agent on Windows

1. Be sure that the NETE_PS_ROOT environment variable is set to the CA SiteMinder® installation directory. The Policy Server installation program should have already done this.
2. Open *siteminder_home*\config\snmp.conf file and edit the last row to contain the full path to *siteminder_home*\log\snmp.log.

   Note: You only need to do this if you did not specify the Policy Server installation program to automatically configure SNMP.

   Correct example: LOG_FILE=C:\Program Files\Netegrity\siteminder\ log\snmp.LOG

   Incorrect example: LOG_FILE=$NETE_PS_ROOT\log\snmp.log
3. Edit the w*indows_dir*/java_service.ini file.

   Note: You only need to do this if you did not specify the Policy Server installation to automatically configure SNMP.

a. Set SERVICE_BINARY_NAME to the full path name of JavaService.exe.

   Example: SERVICE_BINARY_NAME=c:\winnt\JavaService.exe

b. Set WORKING_DIR to the full path to directory *siteminder_home*\bin:

   Example: WORKING_DIR=C:\Program files\Netegrity\siteminder\bin

c. Set JRE_PATH to the full path of javaw.exe.

4. Run *siteminder_home*\bin\thirdparty\proxyreg.exe to change the registry keys for the apadll.dll and snmp.conf:

   ```
   proxyreg.exe full_path_for_apadll.dll full_path_for_snmp.conf
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Example: proxyreg.exe "c:\program files\netegrity\siteminder\ bin\ thirdparty\apadll.dll" "c:\programfiles\netegrity\ siteminder\ config\ snmp.conf"

5. Run *WINNT dir*/JavaService.exe with the -install option, to register the Netegrity SNMP agent as a WINNT service.

6. Start the Netegrity SNMP agent by using the Windows Services dialog box.

7. Restart the SNMP service.

How to Configure SNMP Event Trapping on Windows

Configuring SNMP event trapping on Windows requires you to:

1. Enable SNMP event trapping.
2. Configure snmptrap.config (see page 448).

Enable SNMP Event Trapping

To enable SNMP event trapping, use the XPSConfig utility to set the event handler library (eventsnmp.dll) to the XPSAudit list. The default location of eventsnmp.dll is *policy_server_home*\bin.

policy_server_home

Specifies the Policy Server installation location.

Note: More information on using the XPSConfig utility to set event handler libraries exists in the *Policy Server Administration Guide*.

After enabling SNMP event trapping, configure the snmptrap.conf file.

Configure snmptrap.conf

To configure the SNMP configuration file

1. Edit snmptrap.conf.

   Note: snmptrap.conf is located in *policy_server_home*\config.

   policy_server_home

   Specifies the Policy Server installation location.

2. For the specified trap(s) that you want to receive, uncomment out the appropriate line(s).
3. Specify the IP Address, port number, and community for where you want the trap to be sent.
4. Save the snmptrap.config file with the new changes.
5. Restart the Policy Server.

More Information:

Stop and Restart the Policy Server (see page 450)

Configure the SNMP Agent on UNIX Systems

To configure the SNMP Agent on UNIX systems

1. Ensure the NETE_PS_ROOT environment variable is set to the CA SiteMinder® installation directory. The Policy Server installation program should have already done this.

   Example: /home/smuser/siteminder

2. Edit the file /etc/snmp/conf/RunSubagent.sh:

   a. Set the correct JRE path: JAVA_HOME=$INSTALL_HOME/bin/jdk/<required_version>/jre

   b. Set the correct CA SiteMinder® path:

      Example: INSTALL_HOME=/home/smuser/siteminder

      Note: The INSTALL_HOME variable should contain the full path for the CA SiteMinder® installation directory.

3. Restart the SNMP daemon on Solaris
   a. Become root.
   b. Goto /etc/rc3.d.
   c. Execute the S76snmpdx script twice, as follows:

      sh S76snmpdx stop to stop the running Solaris master agent.

      sh S76snmpdx start to start the Solaris master agent and Netegrity subagent.

How to Configure SNMP Event Trapping on UNIX Systems

Configuring SNMP event trapping on UNIX systems requires you to:

1. Enable SNMP event trapping.
2. Configure snmptrap.config (see page 449).

Enable SNMP event trapping

To enable SNMP event trapping, use the XPSConfig utility to set the event handler library (libeventsnmp.so) to the XPSAudit list. The default location of libeventsnmp.so is *policy_server_home*/lib.

policy_server_home

Specifies the Policy Server installation location.

Note: More information on using the XPSConfig utility to set event handler libraries exists in the *Policy Server Administration Guide*.

After enabling SNMP event trapping, configure the snmptrap.config file.

Configure snmptrap.config

To configure snmptrap.config

1. Edit snmptrap.config, which is located in /home/smuser/siteminder/config.
2. For the specified trap(s) that you want to receive, uncomment out the appropriate line(s).
3. Specify the IP Address, port number, and community for where you want the trap to be sent.
4. Save the snmptrap.config file with the new changes.
5. Restart the Policy Server.

More Information:

Stop and Restart the Policy Server (see page 450)

Stop and Restart the Policy Server

In order for the SNMP configurations changes to take effect, you need to stop and restart the Policy Server using the Status tab of the Policy Server Management Console.

Test SNMP Gets for Red Hat Enterprise Linux Advanced Server

You should test SNMP Gets after configuring SNMP.

To test SNMP Gets

1. Start the native SNMP master agent. On Red Hat AS, the master agent is not started automatically on start up as is the case on Solaris and HP-UX. To start the master agent, go to the /etc/rc1.d directory and run the following command (run as root):

   ```
   K50snmpd start
   ```

2. Start the Netegrity subagent using the following command (run as root):

   ```
   sh /etc/init.d/NetegrityAgent
   ```

3. To stop the Netegrity subagent on Red Hat AS, run the following command as root:

   ```
   sh $NETE_PS_ROOT/etc/snmp/conf/StopSubagent.sh
   ```

Chapter 12: Installing the Administrative UI to an Existing Application Server

Administrative UI Installation Options

The Administrative UI requires an application server to run. As such, two installation options are available:

- **Stand–alone installation**—This option creates the required application server infrastructure through a prerequisite installer. The prerequisite installer installs an embedded application server (JBoss) and the required JDK. Verify that the Administrative UI host system meets the minimum system requirements before starting the installation.

  The prerequisite installer launches the Administrative UI installer after a successful installation. The Administrative UI installer uses the embedded application server infrastructure to complete the installation.

  Note: If you are installing to UNIX and running the prerequisite installation media in console–mode, you manually start the Administrative UI installer to complete the installation.

- **Existing application server installation**—This option lets you install the Administrative UI to an existing application server infrastructure. The Administrative UI installer prompts you for application server-specific information and the location of the required JDK. Verify that the Administrative UI host system meets all system and third–party component requirements before starting the installation.

The following sections detail how to install the Administrative UI to an existing application server. For more information about the stand-alone installation, see Installing the Administrative UI.

More information:

Installing the Administrative UI (see page 365)

Administrative UI Installation Requirements

The following sections detail the minimum system and application server requirements for installing the Administrative UI to an existing application server infrastructure.

Administrative UI System Requirements

The Administrative UI host must meet the following minimum system requirements.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

Verify Windows System Requirements

If you are installing the Administrative UI to an existing application server, verify that the Windows system meets the following minimum system requirements:

- **CPU**—x86 or x64, 1.2 GHz or better.
- **Memory**—1 GB of system RAM. We recommend 2 GB.

  Note: If you are running WebSphere, 2 GB of system RAM is required.
- **Available disk space**—540 MB.

  Note: If you are running WebSphere, 2 GB of available disk space is required.
- **Temp directory space**—3 GB.
- **JDK**—The required JDK version is installed on the system to which you are installing the Administrative UI.
- **Screen resolution**—1024 x 768 or higher resolution with 256 colors or better to view the Administrative UI properly.

Verify UNIX System Requirements

If you are installing the Administrative UI to an existing application server, the UNIX system must meet the following minimum system requirements:

- **CPU**
  - Solaris—UltraSparc, 440 MHz or better.
  - Red Hat Linux—x86 or x64, 700 MHz or better.

    Note: The Red Hat 6 operating system relies on entropy for performance. Increase entropy before installing the component. Without sufficient entropy, the installation can take an exceedingly long time to complete. We recommend that you use the following command to set a symbolic link:

    ```
    mv /dev/random /dev/random.org
    ln –s /dev/urandom /dev/random
    ```
- **Memory**—1 GB of system RAM. We recommend 2 GB.

  Note: If you are running WebSphere, 2 GB of system RAM is required.
- **Available disk space**—540 MB.

  Note: If you are running WebSphere, 2 GB of available disk space is required.

- **Temp directory space**—3 GB.
- **JDK**—The required JDK version is installed on the system to which you are installing the Administrative UI.

  Note: If your application server runs on a Red Hat Linux operating system, install unlimited cryptography jar files for an IBM JDK when installing the Administrative UI.
- **Screen resolution**—1024 x 768 or higher resolution with 256 colors or better to view the Administrative UI properly.

Application Server Requirements

The Administrative UI is a J2EE application and requires a supported application server. Be sure of the following:

- A supported version of JBoss, WebLogic, or WebSphere is installed on the system that is to host the Administrative UI.
- The Administrative UI is the only application deployed on the application server.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

JBoss

To prepare JBoss for Administrative UI installation, disable the HDScanner service.

Follow these steps:

1. Navigate to *jboss_home*/server/*server_profile*/deploy.

   jboss_home

   Specifies the JBoss installation path.

   server_profile

   Specifies the name of the server profile deployed in the application server.

   Example: default
2. Remove the following file to disable the service:

   hdscanner-jboss-beans.xml

WebLogic as an Application Server

The following sections provide basic instructions for using WebLogic as a CA SiteMinder® application server.

Install WebLogic

Install a version of a WebLogic server that is supported by CA SiteMinder®.

Note: More information on installing a WebLogic server exists in BEA's WebLogic server documentation.

Create a WebLogic Application Server Instance

Before installing the Administrative UI, create a WebLogic domain using the Configuration Wizard that is part of the WebLogic installation and do the following:

- Note the name of the domain. You will need the domain name when installing the Administrative UI.
- Select the Basic WebLogic Server Domain template.
- Verify that the JAVA_HOME variable is set to the path for the required Java environment in the setDomainEnv.cmd/ .sh file. This file is located in *web_logic_home*\user_projects\domains\weblogic_domain\bin.

  web_logic_home

  Specifies the WebLogic server installation path.

  weblogic_domain

  Specifies the name of the WebLogic domain you created.

Verify the WebLogic Domain

Confirm the following:

- The WebLogic server is running.
- You can access the WebLogic console at http://*server.domain.port*/console

  Example: http://myserver.mycompany.com:7001/console
- In the WebLogic console, under Domain Configurations, select the domains link and verify that the WebLogic domain you created appears in the list of existing domains.

Note: Once you have completed the verification, shut down the application server to prepare for the Administrative UI installation.

WebSphere as an Application Server

The following sections provide basic instructions for using WebSphere as a CA SiteMinder® application server.

Install WebSphere

Use the IBM documentation to install WebSphere.

Consider the following items when installing WebSphere:

- Select the Server and Client option.
- Disable the Administrative Security option.
- (Solaris) Before you install the Embedded Messaging service:
    - Configure the following groups:
        - mqm
        - mqbrkrs
    - Configure the following users:
        - mqm
        - root

      Note: For more information, see the IBM documentation.

Verify WebSphere is Working

Use the snoop utility provided by IBM to verify that WebSphere is installed correctly before installing the Administrative UI.

To verify WebSphere is working

1. Enter http://<*fqdn:port*>/snoop to verify that WebSphere is installed correctly.

   Example: http:MyServer.MyCompany.com:9080/snoop.

   If WebSphere is installed correctly, Snoop Servlet—Request Client Information page is displayed in the browser.

2. Enter http://<*fqdn*>/snoop to verify that the WebSphere application server plug-in is installed correctly.

   Example: http://MyServer.MyCompany.com/snoop

   If WebSphere is installed correctly, the same Snoop Servlet—Request Client Information page is displayed in the browser.

   You have verified that WebSphere is working properly.

Note: Contact IBM Technical Support for additional assistance with WebSphere.

Trusted Relationship with a Policy Server

A trusted relationship between the Administrative UI and a Policy Server is required to begin managing your environment. You establish this relationship the first–time you log in using the default CA SiteMinder® super user account (siteminder) and password. These credentials are stored in the policy store.

When you configure the policy store, you use the XPSRegClient utility to submit the super user credentials to the Policy Server. The Policy Server uses these credentials to verify that the registration request is valid and that the relationship can be created.

Note: If you used the Policy Server installer to configure the policy store automatically, the installer used the XPSRegClient utility to submit the credentials.

The time from which the credentials are supplied to when the initial Administrative UI login can occur is limited to 24 hours. Therefore, the process for installing the Administrative UI is determined by when the policy store is configured and the Administrative UI is installed.

Administrative UI Installation Checklist

Complete the following before you install the Administrative UI:

- □ Be sure that you are using a supported operating system.
- □ Be sure that the Administrative UI host system meets the minimum system requirements.
- □ (Linux) Be sure that the required Linux libraries are installed to the Administrative UI host system.
- □ Be sure that a supported application server is installed on the Administrative UI host system.
- □ Be sure that the required JDK is installed to the Administrative UI host system.
- □ Determine when the policy store was configured.

  If the policy store was configured more than 24 hours ago, use the XPSRegClient utility to submit the default CA SiteMinder® super user account credentials to the Policy Server before installing the Administrative UI. The Policy Server requires these credentials to create a trusted relationship with the Administrative UI.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

More information:

Application Server Requirements (see page 453)
Administrative UI System Requirements (see page 452)

How to Install the Administrative UI

Complete the following procedures to install the Administrative UI:

1. Be sure that you have reviewed the installation checklist.
2. (Linux) Review the required Linux libraries requirement.
3. Gather application server information for the Administrative UI installer.
4. Install the Administrative UI.
5. Start the application server.

Required Linux Libraries

Certain library files are required for components operating on Linux operating environments. Failure to install the correct libraries can cause the following error:

```
java.lang.UnsatisfiedLinkError
```

If you are installing, configuring, or upgrading a Linux version of this component, the following libraries are required on the host system:

Red Hat 5.x

compat–gcc-34-c++-3.4.6-*patch_version*.I386

Red Hat 6.x (32-bit)

libstdc++-4.4.6-3.el6.i686.rpm

To have the appropriate 32-bit C run–time library for your operating environment, install the previous rpm.

Red Hat 6.x (64-bit)

libXau-1.0.5-1.el6.i686.rpm

libxcb-1.5-1.el6.i686.rpm

libstdc++-4.4.6-4.el6.i686.rpm

compat-db42-4.2.52-15.el6.i686.rpm

compat-db43-4.3.29-15.el6.i686.rpm

libX11-1.3-2.el6.i686.rpm

libXrender-0.9.5-1.el6.i686.rpm

libexpat.so.1 (provided by expat-2.0.1-11.el6_2.i686.rpm)

libfreetype.so.6 (provided by freetype-2.3.11-6.el6_2.9.i686.rpm)

libfontconfig.so.1 (provided by fontconfig-2.8.0-3.el6.i686.rpm)

libICE-1.0.6-1.el6.i686.rpm

libuuid-2.17.2-12.7.el6.i686.rpm

libSM-1.1.0-7.1.el6.i686.rpm

libXext-1.1-3.el6.i686.rpm

compat-libstdc++-33-3.2.3-69.el6.i686.rpm

compat-db-4.6.21-15.el6.i686.rpm

libXi-1.3-3.el6.i686.rpm

libXtst-1.0.99.2-3.el6.i686.rpm

libXft-2.1.13-4.1.el6.i686.rpm

libXt-1.0.7-1.el6.i686.rpm

libXp-1.0.0-15.1.el6.i686.rpm

Gather Application Server Information

The Administrative UI installer requires specific information about the application server that is installed on the Administrative UI host system.

The following sections detail the required information depending on the type of application server.

Note: Worksheets are provided to help you gather and record required information before installing the Administrative UI.

JBoss Information

Gather the following information about JBoss before installing and registering the Administrative UI:

JBoss installation folder

> The path to the folder where JBoss is installed.

JBoss URL

> The fully qualified URL of the JBoss host system.

JDK

> The installation location of the required JDK.

WebLogic Information

Gather the following information before installing and registering the Administrative UI:

WebLogic binary folder

> The path to the WebLogic installation directory.

WebLogic domain folder

> The path to the WebLogic domain you created for the Administrative UI.

WebLogic server name

> The name of the WebLogic server on which the WebLogic domain is configured.

Application server URL and port

> The fully qualified URL of the WebLogic host system.

JDK

> The installation location of the required JDK.

WebSphere Information

Gather the following information about WebSphere before installing and registering the Administrative UI:

WebSphere installation folder

> The full path to the folder in which WebSphere is installed.

WebSphere URL

> The fully qualified URL of the WebSphere host system.

Server name

> The name of the application server.

Profile name

The name of the profile being used for the Administrative UI.

Cell name

The name of the cell where the server is located.

Node name

The name of the node where the server is located.

JDK

The installation location of the required JDK.

Install the Administrative UI

The following sections detail how to install the Administrative UI to an existing application server infrastructure.

Before You Install

Consider the following items before you install the Administrative UI:

- You install the Administrative UI using the installation media on the Technical Support site.

  Note: For a list of installation media names, see the *Policy Server Release Notes*.

- If you are installing to an existing application server infrastructure, the following procedures apply. If you are using the stand-alone option to install, see Installing the Administrative UI.
- (Windows) Run the installer from the Administrative UI host system. Do not run the installer from a mapped network share or UNC path.
- The installation zip contains a layout.properties file at the same level as the installation media. If you moved the installation media after extracting the installation zip, move the properties file to the same location or the installation fails.
- (Red Hat Linux) The Red Hat 6 operating system relies on entropy for performance. Increase entropy before installing the component. Without sufficient entropy, the installation can take an exceedingly long time to complete. We recommend that you use the following command to set a symbolic link:

  ```
  mv /dev/random /dev/random.org
  ln –s /dev/urandom /dev/random
  ```

- (UNIX) Depending on your permissions, run the following command to add executable permissions to the directory that contains the installation media:

  ```
  chmod -R+x directory
  ```

  directory

  Specifies the directory that contains the installation media.

- (UNIX) The user installing the Administrative UI must have read/write permissions for the directory to which the application server is installed.
- (UNIX) If you execute the Administrative UI installer across different subnets, it can crash. Install the Administrative UI directly on the host system.

More information:

Installing the Administrative UI (see page 365)
How to Install the Administrative UI (see page 371)

Install the Administrative UI

Install the Administrative UI to your existing application server to provide a management console for all tasks that are related to access control, reporting, and policy analysis.

Follow these steps:

1. Exit all applications that are running.
2. Navigate to the installation media.
3. Double-click *installation_media*.

   installation_media

   Specifies the Administrative UI installation executable.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.
4. Use your completed installation worksheet to enter the required values.
5. Review the installation settings and click Install.

   The Administrative UI is installed.

   Note: You cannot use the Administrative UI to manage your environment until you have registered it with a Policy Server.

More information:

How to Register the Administrative UI (see page 463)

Install the Administrative UI Using a GUI

Install the Administrative UI to your existing application server to provide a management console for all tasks that are related to access control, reporting, and policy analysis.

Follow these steps:

1. Exit all applications that are running in the foreground.
2. Open a shell and navigate to the installation media.
3. Enter the following command:

   ```
   ./installation_media gui
   ```

   installation_media

   Specifies the Administrative UI installation executable.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.
4. Use your completed installation worksheet to enter the required values.
5. Review the installation settings and click Install.

   The Administrative UI is installed.
6. Click Done and reboot the system.

   The Administrative UI is installed.

   Note: You cannot use the Administrative UI to manage your environment until you have registered it with a Policy Server.

Install the Administrative UI Using a UNIX Console

Install the Administrative UI to your existing application server to provide a management console for all tasks that are related to access control, reporting, and policy analysis.

Follow these steps:

1. Exit all applications that are running in the foreground.

2. Open a shell and navigate to the installation media.
3. Enter the following command:

   ```
   ./installation_media -i console
   ```

   installation_media

   Specifies the Administrative UI installation executable.

   The installer starts.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.
4. Use your completed installation worksheet to enter the required values.
5. Review the installation settings and press Enter.

   The Administrative UI is installed.
6. Press Enter.

   The installer closes.
7. Reboot the system.

   The Administrative UI is installed.

   Note: You cannot use the Administrative UI to manage your environment until you have registered it with a Policy Server.

More information:

How to Register the Administrative UI (see page 463)

How to Register the Administrative UI

Register the Administrative UI before you use it to manage your environment. Registering the Administrative UI creates a trusted connection between the Administrative UI and a Policy Server.

This process explains how to register an Administrative UI that you installed to an existing application server infrastructure. To register an Administrative UI you installed using the stand-alone option, see Installing the Administrative UI.

To register the Administrative UI, complete the following procedures:

1. Reset the registration window (see page 368).
2. If necessary, create the FIPs environment variable (see page 376).
3. Start the application server (see page 467).
4. Register the Administrative UI (see page 468).

More information:

Installing the Administrative UI (see page 365)
How to Register the Administrative UI (see page 375)

Reset the Administrative UI Registration Window

If either of the following actions occurred more than 24 hours ago, this step is required:

- You used the Policy Server installation wizard to configure a policy store automatically.
- You used the XPSRegClient utility to submit the CA SiteMinder® super user credentials to the Policy Server.

Note: (UNIX) Be sure that the CA SiteMinder® environment variables are set before you use XPSRegClient. If the environment variables are not set, set them manually (see page 476).

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command:

```
XPSRegClient siteminder_administrator[:passphrase] -adminui-setup -t timeout -r retries -c comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

siteminder_administrator

Specifies a CA SiteMinder® administrator. If you are installing the Administrative UI as part of:

- A new 12.52 environment, specify the following default account:

```
siteminder
```

- An upgrade, specify any CA SiteMinder® administrator account with super user permissions in the policy store. If you do not have a super user account in the policy store, use the smreg utility to create the default account.

passphrase

Specifies the password for the CA SiteMinder® administrator account.

-adminui-setup

Specifies that the Administrative UI is being registered with a Policy Server for the first–time.

-t *timeout*

(Optional) Specifies how long you have after you install the Administrative UI to log in for the time to complete the registration. The Policy Server denies the registration request when the timeout value is exceeded.

Unit of measurement: minutes

Default: 1440 (24 hours)

Minimum limit: 1

Maximum limit: 1440 (24 hours)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect CA SiteMinder® administrator credentials when logging in to the Administrative UI for the first–time.

Default: 1

Maximum limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The utility prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log path*

(Optional) Specifies where the registration log file must be exported.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

3. Press Enter.

   The utility supplies the Policy Server with the administrator credentials. The Policy Server uses these credentials to verify the registration request when you log in to the Administrative UI for the first–time.

Create the FIPS Environment Variable

If your environment meets both of the following criteria, creating the FIPs environment variable is required to register the Administrative UI for the first–time:

- The Policy Server to which you are registering is operating in FIPs–only mode.
- The Administrative UI is not installed on the Policy Server host system.

Follow these steps:

1. Complete one of the following steps:
   - (Windows) Log into the Administrative UI host system as an administrative user.
   - (UNIX) Log into the Administrative UI host system as the user that installed the Administrative UI.
2. Set the following environment variable:

   CA_SM_PS_FIPS140=ONLY

   Note: For more information about setting environment variables, see your OS–specific documentation.
3. Verify that Windows or the UNIX shells that runs the Administrative UI correctly recognizes the CA_SM_PS_FIPS140 variable.

Start the Application Server

If you installed the Administrative UI to an existing application server infrastructure, the following procedure applies. If you installed the Administrative UI using the stand-alone option, see Installing the Administrative UI.

Follow these steps:

1. Complete one of the following steps:

   ■ **JBoss**—From a command prompt, navigate to *jboss_home*\bin.

     jboss_home

       Specifies the JBoss installation path.

   ■ **WebLogic**—From a command prompt, navigate to *domains*\bin.

     domains

       Specifies the path of the WebLogic domain you created for the Administrative UI.

       Example: C:\bea\user_projects\domains\mydomain

   ■ **WebSphere**—From a command prompt, navigate to *profile*\bin.

     profile

       Specifies the path of the WebSphere profile name you created for the Administrative UI.

       Example: C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSvr01\bin

2. Complete one of the following steps:

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   ■ **JBoss**

     – Windows: Type the following command and press Enter:

       run.bat

     – UNIX: Type the following command and press Enter:

       run.sh

- **WebLogic**
  - Windows: Type the following command and press Enter:

    startWebLogic.cmd
  - UNIX: Type the following command and press Enter:

    startWebLogic.sh
- **WebSphere**
  - Windows: Type the following command and press Enter:

    startServer.bat *identifier*
  - UNIX: Type the following command and press Enter:

    startServer.sh *identifier*

  identifier

  Specifies the identifier for the WebSphere installation.

  Example: startServer.bat Server1

The application server is started.

More information:

Installing the Administrative UI (see page 365)
Start the Application Server (see page 377)

Register the Administrative UI

You register the Administrative UI with a Policy Server to begin managing your environment.

Follow these steps:

1. Complete one of the following steps:
   - (Windows) Use the Administrative UI shortcut to open the Administrative UI.
   - (UNIX) Open a web browser and go to the following location:

     `host:port/iam/siteminder/adminui`

     Note: If the host system does not have a web browser, you can remotely access the login screen.

     host

     Specifies the fully qualified Administrative UI host system name.

port

Specifies the port on which JBoss listens for HTTP requests.

The CA SiteMinder® Administrative UI login screen appears.

2. Enter the following value in the User Name field:

   ```
   siteminder
   ```

3. Type the CA SiteMinder® superuser account password in the Password field.

   Note: If your superuser account password contains dollar-sign ($) characters, replace each instance of the dollar-sign character with $DOLLAR$. For example, if the CA SiteMinder® superuser account password is $password, enter $DOLLAR$password in the Password field.

4. Type the fully qualified Policy Server host name in the Server field.

   Consider the following items:

   - You can enter a valid IPv4 address or IPv6 address.
   - If you do not specify a port, the registration defaults to 44442, which is the default Policy Server authentication port.

   The Administrative UI opens and is registered with the Policy Server.

More information:

Registration Not on File Error Appears (see page 487)

Stop the Application Server

If you installed the Administrative UI to an existing application server infrastructure, the following procedure applies. If you installed the Administrative UI using the stand-alone option, see Installing the Administrative UI.

To stop the application server

1. Do one of the following:

   - **JBoss**—From the Administrative UI host system, open the Start Task Engine Command prompt.
   - **WebLogic**—From the Administrative UI host system, open the Start Task Engine Command prompt.
   - **WebSphere**—From a command prompt, navigate to *profile*\bin

     profile

     Specifies the path of the WebSphere profile name you created for the Administrative UI

     Example: C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSvr01\bin

2. Do one of the following:

   - **JBoss**—Enter the following keyboard combination:

     `Ctrl+c.`

   - **WebLogic**—Enter the following keyboard combination:

     `Ctrl+c.`

   - **WebSphere**

     – Windows: Type stopServer.bat *identifier* and press Enter.

     Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

     – UNIX: Type stopServer.sh *identifier* and press Enter.

     identifier

     Specifies the identifier for the WebSphere installation.

     Example: stopServer.bat Server1

   The application server is stopped.

More information:

Installing the Administrative UI (see page 365)
Stop the Application Server (see page 380)

Administrator Credentials

By default, the Administrative UI uses the policy store as its source for CA SiteMinder® administrator credentials. You can configure the Administrative UI to use an external store, for example, a corporate directory.

Note: For more information about configuring an external administrator user store, see the *Policy Server Configuration Guide*.

Administrative UI High Availability

Install more than one Administrative UI to be sure that unexpected outages do not prevent you from managing CA SiteMinder® objects. Consider the following before installing another Administrative UI:

- Register the Administrative UI with a Policy Server that is not already sharing a trusted connection with an Administrative UI. Registering with another Policy Server prevents a single Policy Server outage from disabling both GUIs.
- An Administrative UI cannot failover to multiple Policy Servers. However, you can configure the Administrative UI to manage multiple Policy Servers.
- If the existing Administrative UI is configured for external CA SiteMinder® administrator authentication:
    - Configure the new Administrative UI with the same external store. Configuring the new Administrative UI with the same external store helps ensure that all CA SiteMinder® administrators are available to all GUIs.
    - Be sure to configure subsequent Administrative UI connections to the same external store using the same network identifier. Mixing network identifiers for multiple Administrative UI connections to the same external store is not supported.

Example: If you configured the first connection with 172.16.0.0, create subsequent connections with 172.16.0.0. If you configured the first connection with comp001@example.com, create subsequent connections with comp001@example.com.

More information:

How to Install the Administrative UI (see page 457)

Uninstall the Administrative UI on Windows

You uninstall the Administrative UI from an existing application server when it is no longer required on the system.

Follow these steps:

1. Stop the application server.
2. Open the Windows Control Panel and go to the list of programs.
3. Right–click CA CA SiteMinder® Administrative UI.
4. Click Uninstall/Change.
5. Follow the instructions of the wizard.

   Note: If you are prompted to remove a shared file, click No to All.
6. If requested, reboot the system.

   The Administrative UI is uninstalled.

More information:

(Optional) Uninstall the Administrative UI (see page 387)

Uninstall the Administrative UI on UNIX

You uninstall the Administrative UI from an existing application server when it is no longer required on the system.

Note: Do not manually remove the installation directories to uninstall this component. Execute the uninstall shell script. If you only remove the installation directories, related registries can be left behind. If you try to re–install this component on this host system, the entries can prevent a successful installation.

Follow these steps:

1. Stop the application server.
2. Open a shell and navigate to the following directory:

   ```
   administrative_ui_home/CA/adminui/install_config_info
   ```

   administrative_ui_home

   Specifies the Administrative UI installation path.

3. Run the following command:

   ```
   ./smwam-ui-uninstall.sh
   ```

   The process to uninstall the Administrative UI starts.

4. Follow the prompts to uninstall the Administrative UI.

   The installer prompts you when the Administrative UI is removed.

   The Administrative UI is uninstalled.

More information:

Installing the Administrative UI (see page 365)
Uninstall the Administrative UI on UNIX (see page 388)

Chapter 13: Troubleshooting

This section contains the following topics:

Policy Server Troubleshooting

The following sections detail common problems you may experience with the Policy Server during installation and the proposed solutions.

NETE_PS_ALT_CONF_FILE Environment Variable on Solaris

After installing the Policy Server on Solaris, the nete_ps_env.ksh script may have the following entry:

```
export NETE_PS_ALT_CONF_FILE=/export/siteminder/config/.siteminder.conf
```

The NETE_PS_ALT_CONF_FILE environment variable is used by the stop-all and start-all scripts, which stop and start the Policy Server's service. The .siteminder.conf file is a temporary, run-time file created by these scripts and has no affect your CA SiteMinder® configuration.

Do not modify the NETE_PS_ALT_CONF_FILE environment variable.

Policy Server Fails to Start After Installation

Valid on Windows and UNIX Systems

Symptom:

I have installed the Policy Server, but it is not starting.

Solution:

You may have the wrong JRE version installed. Make sure you have the correct JRE version.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

CA SiteMinder® Environment Variables are not set in the Profile File

Valid on UNIX

Symptom:

The Policy Server was installed without adding the CA SiteMinder® environment variables (smprofile.ksh) to the .profile file. I need to set the CA SiteMinder® environment variables manually.

Solution:

To add the CA SiteMinder® environment variables

1. Log in to the Policy Server host system.
2. Open a shell and navigate to *siteminder_home*.

   siteminder_home

   Specifies the Policy Server installation path.

3. Run the following command:

   ```
   smprofile.ksh
   ```

   The CA SiteMinder® environment variables are set.

Winsock error 10054 message

Valid on Windows

Symptom:

When I try to log into the Policy Server, I receive the "Unable to proceed, winsock error 10054" message.

Solution:

One of the following could be the cause of the problem:

- The policy store does not contain the proper CA SiteMinder® schema. Make sure you imported the correct CA SiteMinder® schema.
- The Policy Server is not running. To start this server, use the Status tab on the Policy Server Management Console.

  Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut with Administrator permissions. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.
- The Policy Server is not connected to the policy store properly. Using the Data tab on the Policy Server Management Console, click Test Connection to make sure the policy store connects successfully. If it does not, reenter the data source information values on the Data tab by pointing the Policy Server at the policy store.

Working with a CA SiteMinder® License

Symptom:

- I am currently using the Policy Server evaluation license and want to acquire and add a permanent license.
- I have a CA SiteMinder® license, but cannot find it.
- I have a CA SiteMinder® license, but do not know how to update it with a new product key.

Solution:

To request a CA SiteMinder® license

1. Go to the Technical Support site.
2. Click CA Licensing Inquires. This link is located under Address Licensing Needs.

   The CA Customer Care site opens in a new window.

3. Click Licensing Issue Request. This link is located under Contact Us.

   An online request form opens in a new window.

4. Complete the required information and click Submit.

To add a permanent CA SiteMinder® license to a Policy Server

1. Request a CA SiteMinder® license.
2. Access the Policy Server host system.
3. Do one of the following:
   - (Windows) Navigate to *siteminder_home*\license
   - (UNIX) Navigate to *siteminder_home*/license

     siteminder_home

     Specifies the Policy Server installation path.
4. Copy the license.dat file to the license directory.
5. Restart the Policy Server.

To find an existing CA SiteMinder® license

1. Log into the Technical Support site.
2. Click Licensing. Licensing is located on the left side under Support.

   The CA Licensing screen appears.
3. Click View Licenses. View Licenses is located under SiteMinder and Identity Manager Licenses.

   All license details, including the respective key, appear.

To apply a CA SiteMinder® license key to the license file

1. Access the Policy Server host system.
2. Do one of the following:
   - (Windows) Navigate to *siteminder_home*\license
   - (UNIX) Navigate to *siteminder_home*/license

     siteminder_home

     Specifies the Policy Server installation path.
3. Open the license.dat file.
4. Copy and paste the license key acquired from the Support site into the license file.
5. Save the license file
6. Restart the Policy Server.

Non-english Input Characters Contain Junk Characters

Symptom:

When I install or configure SiteMinder components in the console mode on UNIX machines, few non-English input characters are not displayed correctly in the console window.

Solution:

Verify terminal settings of your console window and confirm that the console does not clear high (8th) bit of input characters by executing the following command:

```
stty –istrip
```

Java Error Messages When Uninstalling

Symptom:

When I attempt to uninstall the Policy Server, Web Agent, SDK, or the documentation, the uninstallation program stops and issues one of the following error messages:

- “Could not find a valid Java virtual machine to load. You need to reinstall a supported Java virtual machine.”
- "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program."

Solution:

Make sure the JRE is in the PATH variable.

Set the JRE in the PATH Variable on Windows

To set the JRE in the PATH variable

1. Go to the Control Panel.
2. Double-click System.
3. In the Environment Variables dialog, add the location of the JRE to the Path system variable.

Set the JRE in the PATH Variable on Solaris

To set the JRE in the PATH variable

Run the following commands:

1. PATH=$PATH:<JRE>/bin

   JRE

   Specifies the location of your JRE.

2. export PATH

Adobe Acrobat Reader Won't Install

Valid on Windows

Symptom:

When I try to install Adobe Acrobat, the installation program hangs.

Solution:

If the Acrobat Reader installation program hangs while the Policy Server service is running, stop it using the Policy Server Management Console's Status tab. After stopping the service, the installation program should start.

Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut with Administrator permissions. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

Problem With Using Active Directory as a User Store

Symptom:

When I use Active Directory as a user store, the Policy Server issues error messages that it cannot connect to this store.

Solution:

When creating an Active Directory-based user store, make sure you specify a fully qualified host name (for example, host.domain.com) in the Administrative UI and do not use the machine's IP Address. Moreover, make sure you can ping host.domain.com and domain.com from the machine where the Policy Server is installed since Active Directory sends referrals to the Policy Server that are identified by the fully qualified host name. If the fully qualified host names are invalid and unreachable, the Policy Server issues error messages.

AE failed to load library 'smjavaapi’. System error

Valid on Windows and UNIX Systems

Symptom:

During Authorization, I receive the "AE failed to load library 'smjavaapi'. System error: The specified module could not be found." error message.

Solution:

Set the PATH variable to <*SiteMinder_installation*>\config\JVMOptions.txt for Windows or the LD_LIBRARY_PATH to <*SiteMinder_installation*>/config/JVMOptions.txt for UNIX systems.

Policy Store Troubleshooting

The following sections detail common problems you may experience with the policy store during installation and the proposed solutions.

Policy Stores with Large Numbers of Objects

Valid on Windows and UNIX Systems

Symptom:

My Policy store has returned the exception java.lang.IndexOutOfBounds to the Administrative UI.

Solution:

Policy Stores with large numbers of objects may return the exception java.lang.IndexOutOfBounds to the Administrative UI.

Define the registry key \HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\ObjectStore\MaxObjects to a value lower than 100 (such as 50).

SSL initialization failed: error -8174 (security library: bad database.)

Valid on Windows and UNIX Systems

Symptom:

My environment is configured with an Oracle Directory Server policy store. The policy store is configured to communicate over SSL.

I have received the following error message:

```
SSL initialization failed: error -8174 (security library: bad
database.)
```

The message appears after I run the following command:

```
smldapsetup ldmod -fpstore -ssl1 -c/app/siteminder/ssl/cert8.db
```

Solution:

1. Verify that the key3.db file exists in the same directory as the cert8.db file.
2. Rerun the smldapsetup command. User the -c option to specify the path of the directory where the SSL client certificate database file exists.

   Example:

   ```
   -c/app/siteminder/ssl/cert8.db
   ```

ODBC Policy Store Import Fails with UserDirectory Error

Symptom:

I receive an error message stating that the policy store failed operation "save" for object type "UserDirectory" when importing policy store data into an ODBC policy store.

Solution:

It is possible that the server name in the ODBC store's userDirectory object is longer than 512 characters, which by default, exceeds the limit allowed by the MS SQL Server and Oracle policy store schema scripts that are shipped with CA SiteMinder®.

Do one of the following:

If you are trying to import policy data into a supported version of a MS SQL Server policy store:

1. Open sm_mssql_ps.sql.

   Note: This schema script is located in *policy_server_home*\db\SQL.

2. Search for the following text:

   CREATE TABLE smuserdirectory5

3. Modify "server smstringreq512N," to one of the following depending on your needs:

   - server smstringreq1024,N
   - server smstringreq4000,N

4. Re-import the policy store schema into the policy store.
5. Import the policy store data.

If you are trying to import policy data into a supported version of an Oracle policy store:

1. Open sm_oracle_ps.sql.

   Note: This schema script is located in *policy_server_home*\db\SQL.

2. Search for the following text:

   CREATE TABLE smuserdirectory5

3. Modify "server VARCHAR2(512) NOT NULL," to one of the following depending on your needs:

   - server VARCHAR2(1024) NOT NULL,
   - server VARCHAR2(4000) NOT NULL,

4. Re-import the policy store schema into the policy store.
5. Import the policy store data.

OneView Monitor Troubleshooting

The following sections detail common problems you may experience with the OneView Monitor during installation and the proposed solutions.

Fix Modified UNIX/Sun Java System Web Server Configuration Files

If the ServletExec installation modified the Oracle iPlanet web server configuration files, the web server instance fails after you configure the OneView Monitor UI. The ServletExec installer added entries in these files that conflict with entries from the Policy Server.

Follow these steps:

1. Open the following configuration file: /*sunjavasystem_home*/servers/https-*web_server_instance_name*.domain.com/config/magnus.conf.

2. Remove the first line:

   ```
   Init fn="ServletExecInit"
   ServExec_instance_name.instances="IP_address:port_number"
   ```

   ServExec_instance_name

   Specifies the name of your SerlvetExec instance.

   IP_address

   Specifies the IP address of the system to which ServletExec is installed.

   port_number

   Specifies the port number for the SerlvetExec instance.

   Note: The Policy Server Configuration Wizard added the correct entry at the end of the file.

3. Open the following configuration file: /*sunjavasystem_home*/servers/https-*web_server_instance_name*.domain.com/config/obj.conf.

4. Complete the following steps:

   a. Remove fourth and fifth lines from the top of the file:

   ```
   NameTrans fn="assign-name" from="/servlet/*"
   name="<ServExec_instance_name>"
   NameTrans fn="assign-name" from="*.jsp*"
   name="<ServExec_instance_name>"
   ```

   Important! Do not remove the following entry from the second and third lines. The Policy Server Configuration Wizard added this entry.

   ```
   name=se-ServExec_instance_name
   ```

   b. Remove the second to the last section from the end of the file:

   ```
   <Object name="ServExec_instance_name"
   Service fn="ServletExecService" group="ServExec_instance_name"
   </Object>
   ```

Important! Do not remove the following entry. The Policy Server Configuration Wizard added this entry.

```
<Object name="se-ServExec_instance_name">
```

5. Save the configuration files and start the web server instance.

Windows/IIS Virtual Path to /sitemindermonitor Does Not Exist

Valid on Windows

Symptom:

The virtual path to the /sitemindermonitor does not exist under Default Web Site in the IIS Microsoft Management Console.

Solution:

Create the virtual path.

To create the virtual path

1. From the Start menu, go to: Programs, Administrative Tools, Internet Service Manager.
2. Select Default Web Site.
3. From the Action menu, select New, Virtual Directory.

   The Virtual Directory Wizard opens.
4. Specify the name (alias) of the virtual directory. For example: sitemindermonitor

   Note: You can specify any name for the alias as sitemindermonitor is an example
5. Click Next.
6. Specify the path to <*siteminder_installation*>\monitor\.
7. Click Next.
8. Select the following permission:

   ```
   Allow Execute Access
   ```
9. Click Finish.

Administrative UI Troubleshooting

The following sections detail common problems you may experience with registering the Administrative UI and the proposed solutions.

Administrative UI Hangs

Symptom:

I have restarted the Policy Server to which the Administrative UI is registered. When I try to start a task in the Administrative UI, it hangs.

Solution:

Restart the Administrative UI.

WebSphere Crashes with an Unhandled Exception

Symptom:

I have installed the Administrative UI to an existing WebSphere infrastructure. WebSphere has crashed and the native_stderr log reports an unhandled exception in the IBM Java Garbage Collector.

Solution:

Patch the embedded Java SDK in WebSphere.

Note: For more information, see the IBM Solution.

Cannot Register a Policy Server Connection

Symptom:

The Administrative UI is registered to a Policy Server that is unavailable and I am trying to register another Policy Server connection. When I log into the Administrative UI with an administrator that has super user permissions, the Register Policy Server Connection task does not appear.

Solution:

A single user was delegated super user permissions when the connection to the external administrator store was configured. Log into the Administrative UI with this super user account. When a Policy Server connection becomes unavailable, this super user is the only user that can register a Policy Server connection.

API Error Appears

Symptom:

The Administrative UI registration fails with an Agent API failure message.

Solution:

The Policy Server is not started. Start the Policy Server using the Policy Server Management Console.

Registration Not on File Error Appears

Symptom:

Registering the Administrative UI with a Policy Server fails with a registration record not on file error message.

You can receive this message when:

- You have installed the Administrative UI and are trying to register the Administrative UI with a Policy Server for the first–time.
- You have registered the Administrative UI and are trying to register an additional Policy Server connection.

Solution:

Do one of the following:

If you are registering the Administrative UI for the first–time

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient siteminder_administrator[:passphrase] -adminui–setup
   ```

   siteminder_administrator

   Specifies a CA SiteMinder® administrator. If you are installing the Administrative UI as part of:

   - A new 12.52 environment, specify the default CA SiteMinder® administrator account (siteminder).
   - An upgrade, specify any CA SiteMinder® administrator account with super user permissions in the policy store.

   Note: If you are upgrading from r12.0 SP1 and do not have a super user account, use the smreg utility to create the default CA SiteMinder® administrator (siteminder). For more information about using the smreg utility, see the *Policy Server Administration Guide*.

passphrase

Specifies the password for the CA SiteMinder® administrator account.

Limits:

- The passphrase must contain at least six (6) characters.
- The passphrase cannot include an ampersand (&) or an asterisk (*).
- If the passphrase contains a space, enclose the passphrase with quotation marks.

3. Log into the Administrative UI using the default CA SiteMinder® administrator account to complete the registration.

If you are trying to register an additional Policy Server connection

1. Log into the Policy Server host system.
2. Run the following command:

```
XPSRegClient client_name[:passphrase] -adminui
```

client_name

Identifies the Administrative UI being registered.

Limit: This value must be unique. For example, if you have previously used smui1 to register an Administrative UI, enter smui2.

passphrase

Specifies the password required to complete the registration of the Administrative UI.

Limits:

- The passphrase must contain at least six (6) characters.
- The passphrase cannot include an ampersand (&) or an asterisk (*).
- If the passphrase contains a space, enclose the passphrase with quotation marks.

3. Log into the Administrative UI to register the Policy Server connection.

Invalid Registration File Error Appears

Symptom:

I am trying to register an additional Policy Server connection. The registration fails with an invalid registration file error message.

Solution:

Verify that the passphrase you entered is identical to the passphrase you created using XPSRegClient. The value you created must match the value that you enter using the Administrative UI.

If you do not have a passphrase:

1. Log into the Policy Server host system.
2. Run the following command:

   ```
   XPSRegClient client_name[:passphrase] -adminui
   ```

   client_name

   Identifies the Administrative UI being registered.

   Limit: This value must be unique. For example, if you have previously used smui1 to register an Administrative UI, enter smui2.

   passphrase

   Specifies the password required to complete the registration of the Administrative UI.

   Limits:

   - The passphrase must contain at least six (6) characters.
   - The passphrase cannot include an ampersand (&) or an asterisk (*).
   - If the passphrase contains a space, enclose the passphrase with quotation marks.

3. Log into the Administrative UI to register the Policy Server connection.

Registration Fails without Timeout

Symptom:

The Administrative UI registration fails without timing out.

Solution:

Do the following:

- Ping the machine hosting the Policy Server to be sure it is available.
- Locate the following registration file in *policy_server_home*\bin:

  ```
  name.XPSReg
  ```

  policy_server_home

  Specifies the Policy Server installation path

  name

  Identifies the client name you specified when using the Administrative UI registration tool (XPSRegClient) to create a client name and passphrase.

  If the registration file does not exist, run XPSRegClient to create a client name and passphrase.
- Open the Policy Server log file (smps.log) and review it for errors that may have occurred around the time of the registration.

Cannot Find the Administrative UI Registration Log

Symptom:

I am trying to troubleshoot the Administrative UI registration and cannot find the log file.

Solution:

XPSRegClient creates and saves the log file in *policy_server_home*\log. The file name is XPSRegClient.*date*

policy server home

Specifies the Policy Server installation path.

date

Specifies the date on which XPSRegClient created the file.

Example: XPSRegClient.2007-12-1.154002

Note: The last six digits are a unique identifier you can use if more than one file is created on the same day.

Search Fails with Timeout Error

Symptom:

I cannot complete a search for policy objects. The Administrative UI displays a connection timeout error instead of returning the search results.

Solution:

When you search on many policy objects using the Administrative UI, either or both of the following results can occur:

- The connection between the Administrative UI and the Policy Server can time out.
- The Policy Server tunnel buffer can become corrupt.

The latter results in a connection timeout error. Adjusting the Administrative UI Policy Server connection timeout and creating a registry key for the Policy Server tunnel buffer size solves the problem.

To adjust the Policy Server connection timeout:

1. Log in to the Administrative UI.
2. Click Administration, Admin UI, Policy Server Connections, Modify Policy Server Connection, Search to open the Policy Server connection object.
3. Select the appropriate Policy Server and click Submit.
4. Set the Timeout field in the Advanced section to a large value, such as 2,000 seconds.

   The Policy Server connection timeout is now increased.

To create a registry key for the tunnel buffer size:

1. Create the following Policy Server registry key:

   HKLM\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\PolicyServer\

   Max AdmComm Buffer Size
2. Set this registry key to a large value, such as 2,097,000 Kilobytes (0x1FFF68).
3. Save the changes and exit the registry.

Note: If the problem persists after the connection timeout and buffer size changes, restart the Administrative UI

Cannot Find the Default Logging File

Symptom:

I am trying to troubleshoot a deployed Administrative UI instance and cannot find the default application server log file.

Solution:

If you used the stand–alone installation option, the name of the default log file is server.log. This log file is located at *administrative_ui_home*\CA\SiteMinder\adminui\server\default\log.

administrative_ui_home

Specifies the Administrative UI installation path.

Note: If you installed the Administrative UI to an existing instance of JBoss, WebSphere, or WebLogic, see your vendor–specific documentation for more information about default logging.

Default Log File does not Provide Enough Information

Symptom:

I am trying to troubleshoot a deployed Administrative UI instance and the default application server log file does not provide enough information.

Solution:

Use the SiteMinderLog4j properties file to configure CA SiteMinder®-specific logging settings. The file contains comments about configuring the logging settings. The location of the file depends on the installation option that was used to install the Administrative UI.

- Stand–alone installation

  If you used the stand–alone installation option, the properties file is located at *administrative_ui_home*\CA\SiteMinder\adminui\server\default\deploy\iam_siteminder.ear\user_console.war\META-INF.

  administrative_ui_home

  Specifies the Administrative UI installation path.

- Existing application server infrastructure

  If you installed the Administrative UI to an existing application server infrastructure, the properties file is located at:
  deploy\iam_siteminder.ear\user_console.war/META-INF

  deploy

  Specifies where your application server deploys applications.

Note: If you upgraded the Administrative UI to 12.52, the properties file is located at *deploy*/IdentityMinder.ear/user_console.war/META-INF.

Report Server Troubleshooting

The following sections detail common problems you may experience with using the Report Server and the proposed solutions.

Report Server Installation Fails with Error Regarding Characters

Symptom:

The installation fails with an error regarding the characters I used in the installation path.

Solution:

The Report Server installation only supports the following character types in the installation path:

- Alphanumeric
- Spaces
- Dashes
- Underlines

Modify the installation path to include character types only.

Report Server Installer Displays Missing File Error

Valid on Windows

Symptom:

During the installation, a message states that the vcredist.msi file is missing. The message prompts me to map to the directory where the file is located.

Solution:

Try one the following solutions:

- Uninstall the Microsoft Visual C++ 2005 Redistributable.
- Click Cancel to continue with the installation.

The installation completes successfully. If you encounter a problem with the Xcelsius application, download and install vcredist.msi from the Microsoft website.

Uninstall Prompts to Close Applications

Valid on Windows 2008 R2

Symptom:

I am uninstalling the Report Server. The installer has prompted me to close the following applications before continuing:

- Java Platform SE binary
- BOE120MySQL

Solution:

Select the Do not close the applications option and click OK.

Letting the installer automatically close the applications causes the process to fail.

Audit-based Reports Return No Results

Valid for Oracle-based audit stores.

Symptom:

My audit-based reports are not returning results.

Solution:

Determine if the user account that was used when configuring the audit database has the DB role. If the user account has the DB role, remove it. The DB role prevents audit-based reports from querying the correct audit table.

Policy Analysis Reports Fail to Run

Valid on Solaris

Symptom:

I am trying to run a policy analysis report. The report fails with the following message:

Failed to retrieve data from the database.

Solution:

This error is related to one of the following problems:

The CRConfig.xml file is missing Java classes.

1. Navigate to *report_server_home/*CommonReporting3/bobje/java.

   report_server_home

   Specifies the Report Server installation path.

2. Verify that the Classpath section of the file contains the following classes:

   - smjavaagentapi.jar
   - smanalyzer.jar

3. Verify that the JavaBeans section includes the following class:

   webadmin-report-ds.jar

The connection between the Report Server and the Policy Server is broken.

Re–register the Report Server.

The report server did not start correctly.

Restart the Report Server.

More information:

How to Register the Report Server (see page 416)

Administrative UI Displays Missing File Error

Symptom:

I have installed and configured the Report Server. The Administrative UI displays a message stating that the report parameter definition file is not found.

Solution:

Reinstall the report templates.

More information:

How to Install the Report Templates (see page 411)

Chapter 14: Unattended Installation

Unattended Installation Introduced

After you install a CA SiteMinder® component, you can install the component again using an unattended installation. An unattended installation lets you complete the installation without user interaction. You can use an unattended installation to install the following components:

- A Policy Server
- An Administrative UI
- A Report Server

Unattended Installation Guidelines

Each CA SiteMinder® component is associated with its own properties file or files. The following guidelines apply to all properties files. Review them before starting an unattended installation:

- Back up the default properties file before modifying it.
- Do not add extra spaces between a parameter name, the equal sign (=), and the parameter value.
- Save the file after you change it.
- Do not manually edit encrypted passwords. These passwords are encrypted for security reasons and cannot be edited in plain text. If you want to add plain text passwords, comment out the encrypted password parameter and uncomment the plain text reference.

Default Properties Files

Use a text editor to modify the parameters in a default properties file. The default parameters reflect the information that was entered during the initial installation.

Policy Server Properties File

The Policy Server properties file has the following default name and location:

Name

ca-ps-installer.properties

Location

policy_server_home\siteminder\install_config_info

policy_server_home

Specifies the Policy Server installation path.

Administrative UI Properties Files

Silently installing the Administrative UI requires only one properties file. The required file depends on the installation option you select. The available properties files have the following default names and locations:

- smwamui-installer.properties

  If you are installing to an existing application server infrastructure, use this file.

  Location

  admin_ui_home\siteminder\adminui\install_config_info

  admin_ui_home

  Specifies the Administrative UI installation path.

- prerequisite-installer.properties

  If you are installing using the stand-alone installation option, use this file.

  Note: This file is only available if the Administrative UI was previously installed using the stand-alone installation option.

  Location

  admin_ui_home\siteminder\adminui\install_config_info

  admin_ui_home

  Specifies the Administrative UI installation path.

More information:

Administrative UI Installation Options (see page 366)

Reporting Properties File

Installing CA SiteMinder® reporting silently requires a response file for the Report Server and a response file for the CA SiteMinder® Report Server Configuration Wizard. These files have the following names and default locations:

- cabiresponse.ini

  Use this file to install the Report Server.

  Default location: *report_server_home*\CA\SC\CommonReporting3

  report_server_home

  Specifies the Report Server installation path.

- reportserver_config_installer.properties

  Use this file to install the CA SiteMinder® reporting templates.

  Default location: *report_server_home*\CommonReporting3\install_config_info

  report_server_home

  Specifies the Report Server installation path.

How to Run an Unattended Policy Server Install

To run an unattended Policy Server install, complete the following procedures:

1. Review the unattended installation guidelines.
2. Copy the Policy Server properties file from the Policy Server host system.
3. Complete one of the following steps:
   - If you are reinstalling the Policy Server, copy the file to a temporary location.
   - If you are installing the Policy Server to a new system, copy the file to a temporary location on that system.

   Note: (UNIX) Be sure that the UNIX user has the appropriate permissions to install from this directory.
4. Copy the Policy Server installation media to the same location as the properties file.
5. Modify the Policy Server installer properties file.
6. Run the Policy Server installer.
7. Verify the Policy Server installation.

More information:

Unattended Installation Guidelines (see page 497)

Modify the Policy Server Installer Properties Files

You modify the Policy Server installer properties file to define installation variables. The default parameters, passwords, and paths in this file reflect the information you entered during the initial Policy Server installation.

Important! The properties template includes a variable that specifies the Policy Server's FIPS mode of operation: CA_SM_PS_FIPS140. If you are reinstalling the Policy Server, do not modify the value of the variable. If required, change the FIPS mode of operation after reinstalling the Policy Server. More information on changing the Policy Server's FIPS mode of operation exists in the *Upgrade Guide*.

General Policy Server Information

The General Information section allows you to set the following:

DEFAULT_INSTALL_DIR

Specifies the location of the Policy Server installation.

DEFAULT_SHORTCUTS_DIR

Specifies the location of the CA SiteMinder® program icon.

Example: C:\\Documents and Settings\\All Users\\Start or /CA SiteMinder®

Note: The icon feature only works on Windows.

DEFAULT_JRE_ROOT

Specifies the JRE installation location.

DEFAULT_BROWSER

(UNIX only) Specifies the installation location of the browser.

Example: /usr/dt/appconfig/netscape/netscape

DEFAULT_SMPROFILE_CHOICE

(UNIX only) Specifies if smprofile.ksh should be added to the .profile file. Specify **true** for yes; specify **false** for no.

DEFAULT_ENCRYPTKEY

Allows you to enter a cleartext encryption key, which secures data sent between the Policy Server and the policy store.

Note: If you comment out the ENCRYPTED_ENCRYPTKEY parameter and uncomment DEFAULT_ENCRYPTKEY, then the unattended installer uses the cleartext encrypt key value from DEFAULT_ENCRYPTKEY. The DEFAULT_ENCRYPTKEY parameter is commented out by default after the initial Policy Server installation.

ENCRYPTED_ENCRYPTKEY

Shows the encrypted encryption key, which secures data sent between the Policy Server and the policy store. You entered this key during the initial Policy Server installation and cannot change it.

Important! Do not modify this encrypted value since any change will break the communication between the Policy Server and policy store when you run an unattended installation.

If you comment out the DEFAULT_ENCRYPTKEY parameter and uncomment ENCRYPTED_ENCRYPTKEY, then the unattended installer uses the encrypted encryption key value from ENCRYPTED_ENCRYPTKEY.

CA_SM_PS_FIPS140

Specifies the Policy Server's FIPS mode of operation.

Values: COMPAT, MIGRATE, or ONLY

Important! Do not modify the value if you are reinstalling the Policy Server.

Policy Server Features

The Feature Selection section lets you set the following parameters:

DEFAULT_OVMGUI_CHOICE

Determines if the Policy Server installer configures the OneView Monitor GUI on the selected web server.

Valid values: true and false.

true

The installer configures the OneView Monitor GUI.

Setting this value to true requires you to configure additional settings under OneView Monitor GUI and Web Servers.

false

The installer does not configure the OneView Monitor GUI.

DEFAULT_WEBSERVERS_CHOICE

Determines if the Policy Server installer configures the Federation Security Services UI with a specified web server.

Valid values: true and false.

true

The installer configures the component with the specified web server.

Setting this value to true requires you to configure additional settings under Web Servers.

false

The installer does not configure the component with a web server.

DEFAULT_SNMP_CHOICE

Determines if the Policy Server installer configures CA SiteMinder® SNMP support with the Policy Server.

Valid values: true and false.

true

The installer configures CA SiteMinder® SNMP support.

Setting this value to true requires you to configure additional settings under SNMP.

false

The installer does not configure CA SiteMinder® SNMP support.

DEFAULT_POLICYSTORE_CHOICE

Determines if the Policy Server installer configures a policy store automatically.

Valid values: true and false.

true

The installer configures a policy store.

Setting this value to true requires you to configure additional settings under Policy Store.

false

The installer does not configure a policy store.

OneView Monitor GUI

If you set the DEFAULT_OVMGUI_CHOICE parameter to true, then set the following:

DEFAULT_JDK_ROOT

Specifies the JDK installation location.

DEFAULT_SERVLETEXEC_INSTANCE_NAME

(UNIX only) Specifies the name of the ServletExec instance.

Example: se-testmachine-60psGUI

DEFAULT_SERVLETEXEC_ROOT

Specifies the ServletExec installation location.

Example: C:\\Program Files\\New Atlanta\\ServletExec ISAPI or /export/NewAtlanta/ServletExecAS

DEFAULT_SERVLETEXEC_PORT

(UNIX only) Specifies the port number of the ServletExec instance.

Example: 7676

SNMP

If you want to modify the SNMP password, do the following:

DEFAULT_ROOT_PW

Allows you to enter a cleartext SNMP password for the UNIX system's root user. If you comment out the ENCRYPTED_ROOT_PW parameter and uncomment DEFAULT_ROOT_PW, then the unattended installer uses the cleartext SNMP password from DEFAULT_ROOT_PW.

Default: The DEFAULT_ROOT_PW parameter is commented out after the initial Policy Server installation.

ENCRYPTED_ROOT_PW

Shows the encrypted SNMP password for the UNIX system's root user. You entered this password during the initial UNIX Policy Server installation and cannot change it.

Important! Do not modify this encrypted password since any change will break the communication between the Policy Server and the SNMP Agent. If you comment out the DEFAULT_ROOT_PW parameter and uncomment ENCRYPTED_ROOT_PW, then the unattended installer uses the encrypted password from ENCRYPTED_ROOT_PW.

Policy Store

If you set the DEFAULT_POLICYSTORE_CHOICE parameter to true, then set the following parameters:

DEFAULT_POLICYSTORE_TYPE

Specifies the type of store that is to function as the policy store.

Valid values: LDAP and RDB.

LDAP

Specifies an LDAP policy store.

RDB

Specifies an ODBC policy store.

DEFAULT_POLICYSTORE_IP

(LDAP) Specifies the IP address or name of the LDAP directory server host system.

Example: 172.16.0.0

DEFAULT_POLICYSTORE_PORT

(LDAP) Specifies the port on which the LDAP directory server is listening.

Example: 1356.

DEFAULT_POLICYSTORE_ADMINDN

(LDAP) Specifies the LDAP user name of an administrator who has permission to:

- Create schema.
- Create, read, modify, and delete objects in the LDAP tree under the policy store root object.

Example: cn=Directory Manager.

DEFAULT_POLICYSTORE_ADMINPW

(LDAP) Lets you enter a cleartext password for the administrator of the LDAP directory server.

If you comment ENCRYPTED_POLICYSTORE_ADMINPW and uncomment DEFAULT_POLICYSTORE_ADMINPW, then the unattended installer uses the cleartext password from DEFAULT_POLICYSTORE_ADMINPW.

Default: The DEFAULT_POLICYSTORE_ADMINPW parameter is commented out after the initial Policy Server installation.

ENCRYPTED_POLICYSTORE_ADMINPW

(LDAP) Represents the encrypted password for the administrator of the LDAP directory server. This password was entered the last time the Policy Server installer configured the policy store. You can use the existing encrypted value to provide the LDAP administrator password for the new policy store. This password cannot be changed.

Important! Do not modify this password. The password is encrypted. If you comment out the DEFAULT_POLICYSTORE_ADMINPW and uncomment ENCRYPTED_POLICYSTORE_ADMINPW, then the installer uses the encrypted password from ENCRYPTED_POLICYSTORE_ADMINPW.

DEFAULT_POLICYSTORE_ROOTDN

(LDAP) Specifies the root DN of the LDAP directory server.

Example: o=example.com.

DEFAULT_POLICYSTORE_USER_CHOICE

(LDAP) The DEFAULT_POLICYSTORE_ADMINDN parameter requires an LDAP administrator user name that has permission to create the schema. By default, the Policy Server uses this account to manage the policy store. An alternate LDAP user account can manage CA SiteMinder® data in the policy store after the policy store is configured. The alternate account must have permission to create, read, modify, and delete objects.

Valid values: true and false.

true

Specifies that an alternate LDAP user account is to manage the policy store after the policy store is configured.

false

Specifies that the LDAP administrator user account, which the DEFAULT_POLICYSTORE_ADMINDN parameter specifies, is to manage the policy store after the policy store is configured.

DEFAULT_POLICYSTORE_USERDN

(LDAP) Specifies the DN of the alternate LDAP user account.

Example:

`uid=SMAdmin,ou=people,o=security.com.`

DEFAULT_POLICYSTORE_USERPW

(LDAP) Lets you enter a cleartext password for the alternate LDAP user. If you comment ENCRYPTED_POLICYSTORE_USERPW and uncomment DEFAULT_POLICYSTORE_USERPW, then the unattended installer uses the cleartext password from DEFAULT_POLICYSTORE_USERPW.

Default: The DEFAULT_POLICYSTORE_USERPW parameter is commented out after the initial Policy Server installation.

ENCRYPTED_POLICYSTORE_USERPW

(LDAP) Represents the encrypted password for the alternate LDAP user. This password was entered the last time the Policy Server installer configured the policy store. You can use the existing encrypted value to set the alternate administrator password for the new policy store. This password cannot be changed.

Important! Do not modify this password. This password is encrypted.

If you comment DEFAULT_POLICYSTORE_USERPW and uncomment ENCRYPTED_POLICYSTORE_USERPW, then the installer uses the encrypted password from ENCRYPTED_POLICYSTORE_USERPW.

DEFAULT_INIT_POLICYSTORE_CHOICE

(LDAP/RDB) Specifies if the Policy Server installer must initialize the policy store.

Valid values: true and false.

true

The installer initializes the policy store.

false

The installer does not initialize the policy store.

DEFAULT_SM_ADMINPW

(LDAP/RDB) Lets you enter a cleartext password for the CA SiteMinder® superuser account.

If you comment ENCRYPTED_SM_ADMINPW and uncomment DEFAULT_SM_ADMINPW, then the installer uses the cleartext password from DEFAULT_SM_ADMINPW.

Default: The DEFAULT_SM_ADMINPW parameter is commented out after the initial Policy Server installation.

ENCRYPTED_SM_ADMINPW

(LDAP/RDB) Represents the encrypted password for the CA SiteMinder® superuser account. This password was entered the last time the Policy Server installer configured the policy store. You can use the existing encrypted value to set the CA SiteMinder® superuser password for the new policy store. This password cannot be changed.

Important! Do not modify this password. This password is encrypted.

If you comment DEFAULT_SM_ADMINPW and uncomment ENCRYPTED_SM_ADMINPW, then the installer uses the encrypted password from ENCRYPTED_SM_ADMINPW.

DEFAULT_RDB_DSN

(RDB) Specifies the name of the DSN that the Policy Server installer creates.

DEFAULT_RDB_DBSERVER

(RDB) Specifies the IP address or name of the database host system.

DEFAULT_RDB_DBNAME

(RDB) Specifies one of the following values:

- (SQL Server) the named instance or database name that is to function as the policy store.
- (Oracle) the service name of the Oracle database that is to function as the policy store.

DEFAULT_RDB_PORT

(RDB) Specifies the port on which the database is listening.

DEFAULT_RDB_USER_NAME

(RDB) Specifies the name of the database administrator account that has permission to:

- Create schema
- Create, read, modify, and delete objects.

DEFAULT_RDB_DBTYPE

Specifies the type of database that is to function as the policy store.

Valid values: DB_MSSQL and DB_ORACLE.

DB_MSSQL

Specifies a SQL Server policy store.

DB_ORACLE

Specifies an Oracle policy store.

DEFAULT_RDB_PASSWORD

(RDB) Lets you enter a cleartext password for the database administrator.

Default: This parameter is commented out after the initial Policy Server installation.

If you comment ENCRYPTED_RDB_PASSWORD and uncomment DEFAULT_RDB_PASSWORD, then the installer uses the cleartext password from DEFAULT_RDB_PASSWORD.

ENCRYPTED_RDB_PASSWORD

(RDB) Represents the encrypted value of the database administrator password that was entered the last time that the installer configured the policy store.

Default: This parameter is uncommented. The installer uses this value, unless you comment this parameter and uncomment DEFAULT_RDB_PASSWORD.

DEFAULT_KEYSTORE_CONFIG

Specifies if the installer must collocate the CA SiteMinder® key store with the policy store.

Valid values: true and false.

true

The installer collocates the key store with the policy store.

false

The installer does not configure a key store. You configure a stand–alone key store after configuring the policy store.

DEFAULT_SMKEYDB_IMPORT_CHOICE

Specifies if the default CA certificates must be imported into the certificate data store.

Valid values: true and false.

true

Import the default CA certificates.

false

Do not import the default CA certificates.

Enhanced Session Assurance with DeviceDNA™ Settings

The following items apply to Enhanced Session Assurance with DeviceDNA™:

MASTER_KEY=

Specifies the master encryption key for the advanced authentication server (which runs on the CA SiteMinder® SPS). Stores the master encryption key in plain-text format.

ENCRYPTED_MASTER_KEY=

Specifies the master encryption key for the advanced authentication server (which runs on the CA SiteMinder® SPS). Stores the master encryption key in an encrypted format.

IS_SA_ENABLED=true

Indicates if Enhanced Session Assurance with DeviceDNA™ is enabled. Do *not* edit this item.

Run the Policy Server Installer

You run an unattended installation to install the Policy Server without user interaction.

Before You Install

You install the Policy Server using the installation media on the Technical Support site.

Note: For a list of installation media names, see the *Policy Server Release Notes*.

Windows

To run an unattended Policy Server install, run the following command from the directory to which you copied the Policy Server installation executable and the properties file:

```
installation_media -f ca-ps-installer.properties -i silent
```

Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

installation_media

Specifies the Policy Server installation executable.

Note: If the properties file is not in the same directory as the installation media, specify its location. Use double quotes if the argument contains spaces.

-i silent

Specifies that the installer run silently.

Example:

```
installation_media -f "C:\Program
Files\CA\siteminder\install_config_info\ca-ps-installer.properties
" -i silent
```

The installation begins. The installer uses the parameters that you specified in the properties file to install the Policy Server.

UNIX

Follow these steps:

1. Open a shell.
2. Run the following command from the directory to which you copied the Policy Server installation executable and Policy Server installation properties file:

   ```
   ./installation_media -f ca-ps-installer.properties -i silent
   ```

   installation_media

   Specifies the Policy Server installation executable.

-i silent

Specifies that the installer run silently.

The installation begins. The installer uses the parameters that you specified in the properties file to install the Policy Server.

Troubleshoot the Policy Server Installation

Use the following files to troubleshoot the Policy Server installation:

- CA_SiteMinder_Policy_Server_*release*_InstallLog.log

  The installation log contains a summary section that lists the number of successes, warnings, non–fatal errors, and errors that occurred during the installation. Individual installation actions are listed with the respective status.

  release

  Specifies the Policy Server release.

  Location: *siteminder_home*\siteminder\install_config_info

- ca-ps-details.log

  The policy store log details the policy store status.

  Location: *siteminder_home*\siteminder\install_config_info

- smps.log

  The smps.log is created when you start the Policy Server. This log contains the following line if the Policy Server installed successfully:

  ```
  [Info] Journaling thread started, will delete commands older than 60 minutes.
  ```

  Location: *siteminder_home*\siteminder\log

  siteminder_home

  Specifies the Policy Server installation path.

Stop an Unattended Policy Server Installation

You stop an unattended Policy Server installation to prevent the Policy Server from installing on the specified Windows system.

To stop the installation:

- **Windows**

  Use the Windows Task Manager to stop the following processes:

  ```
  ca-ps-12.5-win32.exe
  ps_install.exe
  ```

- **UNIX**

  Press Ctrl+C.

How to Run an Unattended Administrative UI Install

To run an unattended Administrative UI install, complete the following procedures:

1. If you are:
   - Using the prerequisite installer, review the installation checklist (see page 367).
   - Installing to an existing application server infrastructure, review the installation checklist (see page 456).
2. Review the guidelines for silent installation.
3. Determine which properties file to use.

   Note: The Administrative UI installation option determines the properties file that you use.
4. From an Administrative UI host system, complete the following steps:
   a. Copy the properties file. If you are:
      - Reinstalling the Administrative UI, copy this file to a temporary location.
      - Installing the Administrative UI to a new system, copy this file to a temporary location on that system.

   b. If you are using the prerequisite installer, navigate to *admin_ui_home*\SiteMinder\adminui and review the JBoss license agreement (JBoss-ORG-ULA.txt). The prerequisite installer properties file includes a Lesser General Public License parameter. You update this parameter to verify that you have reviewed and agree to the JBoss license agreement.
5. Copy the installation media to the same location to which you copied the properties file.

   Note: The Administrative UI installation option determines the executable that you use.

6. Modify the properties file.
7. Run the Administrative UI installer.
8. Register the Administrative UI with a Policy Server.

More information:

Unattended Installation Guidelines (see page 497)
Administrative UI Properties Files (see page 498)

Modify the Prerequisite Installer Properties File

If you are using the stand-alone option to install the Administrative UI, modify the prerequisite installer properties file to define installation variables. The default values reflect the information entered during the last Administrative UI installation.

More information:

Administrative UI Properties Files (see page 498)

General Information

This section lets you specify the root folder of the Administrative UI installation:

DEFAULT_INSTALL_FOLDER

Specifies the root folder under which all sub-folders are created during the installation.

Server Information

This section lets you specify information about JBoss and the Administrative UI host system. This section contains the following parameters:

DEFAULT_APP_SERVER_PORT

Specifies the port on which JBoss should listen for HTTP requests.

DEFAULT_APP_SERVER_HOST

Specifies the fully qualified name of the Administrative UI host system.

End User Licensing Agreement

The prerequisite installer installs JBoss, which requires you to accept a Lesser General Public License. This section lets you indicate that you have reviewed and accept the License Agreement.

To accept the license:

1. Be sure that you have reviewed the JBoss License Agreement (JBossORG-EULA.txt).

   The license is available on an Administrative UI host system in the following location:

   admin_ui_home\siteminder\adminui.

   admin_ui_home

   Specifies the Administrative UI installation path.

2. If you accept the License Agreement, change the value of ACCEPT_LGPL_EULA to the following:

   YES

   Specifies that you have reviewed and accept the License Agreement.

Modify the Administrative UI Installer Properties File

If you are installing the Administrative UI to an existing application server infrastructure, modify the Administrative UI installer properties file to define installation variables. The default values in this file reflect the information entered during the last Administrative UI installation.

More information:

Administrative UI Properties Files (see page 498)

General Information

This section lets you specify the root folder of the Administrative UI installation:

DEFAULT_INSTALL_FOLDER

Specifies the root folder under which all sub-folders are created during the installation.

Application Server Information

This section lets you specify information about the application server to which the Administrative UI is to be deployed. This section contains the following parameters:

DEFAULT_APP_SERVER

Specifies the application server type. This parameter uses the following settings:

JBoss

Specifies that the application server type is JBoss.

WebLogic9

Specifies that the application server type is WebLogic.

WebSphere6

Specifies that the application server type is WebSphere.

DEFAULT_NETE_JAVA_HOME

Specifies the path to the required JDK or JRE for the application server. This value depends on the type of application server:

JBoss

Specifies the path to the minimum version of the required JDK.

WebLogic

Specifies the path to the minimum version of the required JDK or JRE.

WebSphere

Specifies the path to the minimum version of the required JDK or JRE.

DEFAULT_APP_SERVER_URL

Specifies the fully qualified URL of the system on which the application server is installed.

JBoss Information

This section lets you specify additional information about JBoss.

Note: If you did not enter JBoss as the value of DEFAULT_APP_SERVER, a value is not required for this section.

This section has the following parameter:

DEFAULT_JBOSS_FOLDER

Specifies the path to the JBoss installation directory.

Note: The path cannot contain spaces.

WebLogic Information

This section lets you specify additional information about WebLogic.

Note: If you do not enter WebLogic9 as the value of DEFAULT_APP_SERVER, values are not required for this section.

This section has the following parameters:

DEFAULT_BINARY_FOLDER

Specifies the path to the WebLogic installation directory.

DEFAULT_DOMAIN_FOLDER

Specifies the path to the WebLogic domain you created for the Administrative UI.

DEFAULT_SERVER_NAME

Specifies the name of the WebLogic server on which the WebLogic domain is configured.

WebSphere Information

This section lets you specify additional information about WebSphere.

Note: If you do not enter WebSphere6 as the value of DEFAULT_APP_SERVER, values are not required for this section.

This section has the following parameters:

DEFAULT_WEBSPHERE_FOLDER

Specifies the path to the WebSphere installation directory.

DEFAULT_WAS_NODE

Specifies the name of the node in which the application server is located.

DEFAULT_WAS_SERVER

Specifies the name of the application server.

DEFAULT_WAS_CELL

Specifies the name of the cell in which the application server is located.

WAS_PROFILE

Specifies the name of the profile being used for the Administrative UI.

Run the Administrative UI Installer

You run an unattended installation to install the Administrative UI without user interaction.

Before You Install

Consider the following items before installing the Administrative UI:

- You install the Administrative UI using the installation media on the Technical Support site.

  Note: For a list of installation media names, see the *Policy Server Release Notes*.

- **Important!** The installation zip contains a layout.properties file and a Framework folder at the same level as the installation media. If you moved the installation media after extracting the installation zip, move the following to the same location or the installation fails:

  - layout.properties file
  - Framework folder

- The installation zip contains the prerequisite installer and the Administrative UI installer.

  If you are installing the Administrative UI using the prerequisite installer, place both executables are in the same location. The prerequisite installer automatically calls the Administrative UI installer to complete the installation.

Windows

To run an unattended Administrative UI install, run the following command from the directory to which you copied the Administrative UI installation media and the properties file:

```
installation_media -f properties_file -i silent
```

Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

installation_media

Specifies the name of the Administrative UI installation executable. The Administrative UI installation option determines the executable that you use.

-f *properties_file*

Specifies the path to the properties file. The path must include the properties file name. The Administrative UI installation option determines the properties file that you use.

Note: Use double quotes if the argument contains spaces.

-i silent

Specifies that the installer run silently.

Example:

installation_media -f "C:Program Files\CA\SiteMinder\adminui\install_config_info\properties_file" -i silent

The installer uses the parameters in the properties file to install the Administrative UI.

You complete the installation by registering the Administrative UI with a Policy Server:

- If you installed the Administrative UI using the stand-alone option, see How to Register the Administrative UI (see page 375).
- If you installed the Administrative UI to an existing application server infrastructure, see How to Register the Administrative UI (see page 463).

UNIX

Follow these steps:

1. Open a shell
2. Run the following command from the directory to which you copied the Administrative UI installation media and the properties file:

   ```
   ./installation_media -f properties_file -i silent
   ```

   installation_media

   Specifies the name of the Administrative UI installation executable. The Administrative UI installation option determines the executable that you use.

   -f *properties_file*

   Specifies the path to the properties file. The path must include the properties file name. The Administrative UI installation option determines the properties file that you use.

   -i silent

   Specifies that the installer run silently.

   The installer uses the parameters in the properties file to install the Administrative UI.

3. Complete the installation by registering the Administrative UI with a Policy Server:
   - If you installed the Administrative UI using the stand-alone option, see How to Register the Administrative UI (see page 375).
   - If you installed the Administrative UI to an existing application server infrastructure, see How to Register the Administrative UI (see page 463).

How to Run an Unattended Report Server Install

To run an unattended Administrative UI install, complete the following procedures:

1. Review the installation checklists (see page 392).
2. Gather the required information for the installer.
3. Review the guidelines for silent installation.
4. Locate the Report Server response file and CA SiteMinder® Report Server Configuration Wizard properties file.
5. Copy the response and properties files to a temporary location on the Report Server host system.
6. Copy the Report Server and the CA SiteMinder® Report Server Configuration Wizard installation media to a temporary location on the Report Server host system.

   Note: You can download the installation media from the Technical Support site.
7. Modify the Report Server response file.
8. Modify the CA SiteMinder® Report Server Configuration Wizard properties file.
9. Run the Report Server installer.
10. Run the CA SiteMinder® Report Server Configuration Wizard.
11. Register the Report Server.

Modify the Report Server Response File for Windows

You modify the installer response file to define installation variables. The default values reflect the information that was entered when a Report Server was installed and a response file was saved.

Important! Consider the following items before you modify the file:

- Some of the parameters identify the type of database that is to function as the report (cms) database. Do not use the properties file to change the type of database that the installer is to configure. To change the report database type, use the installer to create another properties file.
- Passing a parameter in the command line overrides the respective setting in the response file.
- The installer generates some parameters automatically. Do not modify the following parameters:
  - DATABASECONNECT
  - DATACONNECTION
  - DATABASE_AUDIT_CONNSVR

- INSTALLDBTYPE
- INSTALL_DB_TYPE
- INSTALLLEVEL
- INSTALLSWITCH
- NEWCMSPASSWORD
- PRIVILEGED
- SINGLESERVER
- SKIP_DEPLOYMENT
- WCADOTNETINSTALL
- WCAJAVAINSTALL
- WCATOMCATINSTALL
- WDEPLOY_LANGUAGES
- WDEPLOY_LATER
- WEBSITE_METABASE_NUMBER
- WEBSITE_PORT
- ADDSOURCE
- ADVERTISE

Install

This section details the parameters in the Install section of the response file.

AS_ADMIN_IS_SECURE

Specifies that an administrator credential must be passed to access the web application server.

CA SiteMinder® setting: Leave the value empty. This parameter applies to a web application server that CA SiteMinder® does not support.

AS_ADMIN_PASSWORD

Specifies the password of the administrator account that accesses the web application server. If the embedded version of Apache Tomcat is installed, the value of this parameter is empty. CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: Leave the value empty.

AS_ADMIN_PORT

Specifies the port on which the web application server is listening. If the embedded version of Apache Tomcat is installed, the value defaults to 8080. CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: 8080

Be sure that this value matches the value of TOMCAT_CONNECTION_PORT.

AS_ADMIN_USERNAME

Specifies the account name of the administrator account that is used to access the web application server. If the embedded version of Apache Tomcat is installed, the value defaults to the following value:

```
admin
```

CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: admin

AS_DIR

Specifies the path to which the embedded version of Apache Tomcat is installed. The path is automatically set using the installation directory.

Note: Be sure that you escape the backslashes in the path with a backslash character.

Example: "C:\\Program Files\\CA\\SC\\CommonReporting3\\Tomcat55"

AS_INSTANCE

Specifies the name of the web application server instance. If the embedded version of Apache Tomcat is installed, the value defaults to localhost. CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: localhost

AS_SERVER

Specifies the type of Java web application server to deploy. If the embedded version of Apache Tomcat is installed, the value defaults to tomcat55. CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: tomcat55

AS_SERVICE_NAME

If the web application server is installed as a service on Windows, specifies the name of the service. If the embedded version of Apache Tomcat is installed, the value defaults to the following value:

```
BOE120Tomcat
```

CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: BOE120Tomcat

AS_VIRTUAL_HOST

If you are deploying the Report Server to a virtualized environment, specifies that the virtual host to which the application must be bound.

CA SiteMinder® setting: Leave the value empty.

AUDITINGALLOWED

If you are configuring a Microsoft SQL Server or Oracle report database, specifies that the Content Management Server Auditing Database component can be configured.

0

Indicates that auditing is allowed.

1

Indicates that auditing is not allowed.

CA SiteMinder® setting: 0

AUDITINGENABLED

If you are configuring a Microsoft SQL Server or Oracle report database, specifies that the Content Management Server Auditing Database is enabled. This parameter is not related to CA SiteMinder® audit–based reports.

The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®. A CA SiteMinder® audit database is required to run audit–based reports.

0

Indicates that auditing is enabled.

1

Indicates that auditing is not enabled.

CA SiteMinder® setting: 1

CANODE

Specifies the name of the Service Intelligence Agent (SIA) node.

Note: Do not use spaces or non–alphanumeric characters.

CADPORT

Specifies the port to which the SIA must connect and listen for requests.

Default: 6410

CLIENTAUDITINGREPORT

If the Content Management Server Auditing Database component is enabled, specifies the port on which the auditing service must listen. This parameter is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®.

A CA SiteMinder® audit database is required to run audit–based reports.

CA SiteMinder® setting: Leave the default value (6420).

CLIENTLANGUAGE

Specifies the language pack to install.

CA SiteMinder® setting: EN

CLUSTERCMS

Specifies if you are adding servers to an existing Content Management Server. If you must change this value, we recommend using the installer to create another response file.

CA SiteMinder® setting: False

CMSPASSWORD

Specifies the password for an existing SAP BusinessObjects Enterprise administrator account. This parameter only applies to a custom or web tier installation.

CA SiteMinder® setting: Leave the value empty.

DATABASEAUDITDRIVER

Specifies which driver to use for the Content Management Server Auditing Database. This parameter is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®.

A CA SiteMinder® audit database is required to run audit–based reports.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, leave the default value (MySQLDatabaseSubSystem).
- If you are configuring and a Microsoft SQL Server or Oracle report database, leave the value empty.

DATABASEAUTHENTICATION

If you are configuring a Microsoft SQL Server or Oracle report database, this parameter is automatically generated.

CA SiteMinder® setting: Leave the value empty.

DATABASEAUTHENTICATION_AUDIT

If you are configuring a Microsoft SQL Server or Oracle report database, this parameter is automatically generated.

CA SiteMinder® setting: Leave the value empty.

DATABASECONNECT

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: Leave the value empty.

DATABASECONNECT_AUDIT

If you are configuring a Microsoft SQL Server or Oracle report database, this parameter is automatically generated.

CA SiteMinder® setting: Leave the value empty.

DATABASEDB

Specifies the name of the report database.

CA SiteMinder® setting:

- If you are installing the embedded version of MySQL, leave the default value (BOE120).
- If you are configuring a Microsoft SQL Server report database, leave the default value (RSDB).
- If you are configuring an Oracle report database, leave the value empty.

DATABASEDB_AUDIT

Specifies the name of the auditing database for the Content Management Server. This parameter is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®.

A CA SiteMinder® audit database is required to run audit–based reports.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, leave the default value (BOE120_AUDIT).
- If you are configuring a Microsoft SQL Server or Oracle report database, leave the value empty.

DATABASEDRIVER

Specifies which driver to use for the report database.

CA SiteMinder® setting: Leave the default value. If you must change this value, use the installer to create another response file.

DATABASEDSN

Specifies the name of the ODBC connection for the report database.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, leave the default value (Business Objects CMS).
- If you are using an existing instance of Microsoft SQL Server, enter the DSN.
- If you are using an exiting instance of Oracle, leave the value empty.

DATABASEDSN_AUDIT

Specifies the name of the ODBC connection for the Content Management Sever Auditing Database. This parameter is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®.

A CA SiteMinder® audit database is required to run audit–based reports.

CA SiteMinder® settings: Leave the default value (Business Objects Audit Server).

DATABASENWLAYER_AUDIT

Specifies the Content Management Server Audit Database type. This parameter is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®.

A CA SiteMinder® audit database is required to run audit–based reports.

CA SiteMinder® setting: Leave the default value (ODBC).

DATABASEPORT

Specifies the port on which the report database must listen.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, enter a port.

  Default: 3306
- If you are configuring a Microsoft SQL Server or Oracle report database, leave the value empty.

DATABASEPORT_AUDIT

Specifies the port on which the Content Management Server Audit Database must listen. This parameter is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®.

A CA SiteMinder® audit database is required to run audit–based reports.

CA SiteMinder® settings: A value for this parameter is not required.

- If you are installing the embedded version of MySQL, enter a port.

  Default: 3306

- If you are configuring a Microsoft SQL Server or Oracle report database, leave the parameter empty. CA SiteMinder® does not require that you audit the Content Management Server.

DATABASEPWD

Specifies the password of the administrator account that can access the report database.

DATABASEPWD_AUDIT

Specifies the password of the administrator account that can access the Content Management Server Auditing Database. This parameter is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®.

A CA SiteMinder® audit database is required to run audit–based reports.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, match this value with the DATABASEPWD paramter.

- If you are configuring a Microsoft SQL Server or Oracle report database, leave the parameter empty.

DATABASEPWD_MYSQLROOT

If you are installing the embedded version of MySQL, specifies the password of the MySQL root user account that can access the report database.

DATABASERDMS_AUDIT

Specifies the Content Management Server Auditing Database type. This parameter is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®.

A CA SiteMinder® audit database is required to run audit–based reports.

CA SiteMinder® setting: Leave the default value of this parameter.

DATABASESERVER

If you are configuring an Oracle report database, specifies the name of the Oracle database service.

Note: This parameter appears in a response file that configures a Microsoft SQL Server report database. Leave this value empty.

DATABASESERVER_AUDIT

Specifies the name of the Content Management Server Auditing Database server host system. This parameter is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®.

A CA SiteMinder® audit database is required to run audit–based reports.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, leave the default value (localhost).
- If you are configuring a Microsoft SQL Server or Oracle report database, leave the parameter empty.

DATABASEDRIVER

Specifies which driver to use for the report database.

CA SiteMinder® setting: Leave the default value. If you must change this value, use the installer to create another response file.

DATABASEUID

Specifies the name of the administrator account that can access the report database.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, enter an account name. The installer creates the administrator account with the required privileges.
- If you are configuring Microsoft SQL Server, enter an account name with database owner (DBO) privileges.
- If you are configuring Oracle, enter an account name with the following privileges enabled: create session, create table, and create procedure.

  You can also enter an account name with the CONNECT and RESOURCE roles enabled. Be sure to disable the Admin Option setting for both roles.

DATABASE_UID_AUDIT

Specifies the name of the administrator account that can access the Content Management Server Auditing Database. This parameter is not related to CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®. A CA SiteMinder® audit database is required to run audit–based reports.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, match this value with the DATABASEUID parameter.
- If you are configuring a Microsoft SQL Server or Oracle report database, leave the value empty.

DATABASEUSER

If you are configuring a Microsoft SQL Server or Oracle report database, this parameter is automatically generated and matches the DATABASEUID value.

CA SiteMinder® setting: Be sure that this value matches the DATABASEUID value.

DATABASEUSER_AUDIT

If you are configuring a Microsoft SQL Server or Oracle report database, this parameter is automatically generated and is empty.

CA SiteMinder® setting: Leave the value empty.

DATABASE_AUDIT_CONNSVR

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: connsvr

ENABLELOGFILE

Specifies if the installer creates installation log files.

0

Do not create log files.

1

Create log files.

ENABLESERVERS

Specifies if servers must be enabled once the installation is complete.

0

Do not enable servers.

1

Enable servers.

CA SiteMinder® setting: 1

EXPANDCMS

If you are configuring a Microsoft SQL Server or Oracle report database, this parameter is automatically generated. Do not modify this parameter

CA SiteMinder® setting: 1

INSTALL.LP.EN.SELECTED

Specifies that the installer install the English Language pack.

CA SiteMinder® setting: 1

INSTALLDBTYPE

Do not modify this parameter. This parameter is automatically generated.

INSTALLDIR

Specifies the directory to which the Report Server is installed.

Note: Be sure that you escape the backslashes in the path with a backslash character.

Example: C:\\Program Files\\CA\\SC\\CommonReporting3\\

INSTALLLEVEL

Do not modify this parameter. This parameter is automatically generated.

INSTALLMODE

Specifies the installation method.

New

Install all required server and client components.

Custom

Select specific server and client components to install.

Web Tier

Install only the required web application server components.

CA SiteMinder® setting: New

INSTALL_DB_TYPE

Do not modify this parameter. This parameter is automatically generated.

MYSQLPORT

If you are using the embedded version of MySQL, specifies the port to which MySQL must connect and listen for requests.

Default: 3306.

Note: This parameter appears in the properties file that configures Microsoft SQL Server as a report database. Leave the default value.

MYSQLSERVER

If you are configuring a Microsoft SQL Server or Oracle report database, this parameter is automatically generated. Do not modify this parameter.

CA SiteMinder® setting: Leave the value empty.

MYSQLSERVER_AUDIT

If you are configuring a Microsoft SQL Server or Oracle report database, this parameter is automatically generated. Do not modify this parameter.

CA SiteMinder® setting: Leave the value empty.

NEWCMSPASSWORD

Specifies the password for the default SAP BusinessObjects Enterprise administrator account. This parameter is automatically generated.

CA SiteMinder® setting: Do not modify this parameter. If you must change this value, use the installer to create another response file.

MYSQL_REMOTE_ACCESS

If you are using the embedded version of MySQL to function as the report database, specifies if remote access is enabled.

CA SiteMinder® setting: Leave the value empty.

Note: This parameter appears in the properties file that configures Microsoft SQL Server as a report database. Leave the value empty.

NAMESERVER

Specifies the name of the Report Server host system.

NEWCMSPASSWORD

Specifies the password for the default SAP BusinessObjects Enterprise administrator account.

CA SiteMinder® setting: Do not modify this parameter. This parameter is automatically generated. If you must change this value, use the installer to create another response file.

NSPORT

Specifies the port on which the Content Management Server must listen.

Default: 6400.

REINITIALIZE_CMS_DB

If you are configuring a Microsoft SQL Server or Oracle report database, specifies that the database is reinitialized.

CA SiteMinder® setting: 1

SINGLESERVER

Do not modify this parameter. This parameter is automatically generated. Do not modify this parameter.

CA SiteMinder® setting: Leave the value empty.

SKIP_DEPLOYMENT

Do not modify this parameter. This parameter is automatically generated. Do not modify this parameter.

CA SiteMinder® setting: Leave the value empty.

SelectODBCDSN

If you are configuring a Microsoft SQL Server or Oracle report database, this parameter is automatically generated. Do not modify this parameter.

CA SiteMinder® setting: Leave the value empty.

TOMCAT_CONNECTION_PORT

Specifies the port to which the embedded version of Apache Tomcat must connect and wait for requests.

Default: 8080.

TOMCAT_REDIRECT_PORT

Specifies the port to which the embedded version of Apache Tomcat must redirect requests.

Default: 8443

TOMCAT_SHUTDOWN_PORT

Specifies the port to which the SHUTDOWN command for the embedded version of the Apache Tomcat must be issued.

Default: 8005

WCADOTNETINSTALL

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: False

WCAEXISTINGINSTALL

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: False

WCAJAVAINSTALL

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: False

WCATOMCATINSTALL

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: True

WDEPLOY_LANGUAGES

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: en

WDEPLOY_LATER

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: Leave this value blank.

WEBSITE_METABASE_NUMBER

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: 1

WEBSITE_NAME

If you are deploying an IIS web application server, specifies the name of the IIS website to which the SAP BusinessObjects Enterprise applications are deployed.

CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: Default Web Site

WEBSITE_PORT

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: 80

Features

This section details the parameters in the Features section of the response file.

REMOVE

Specifies which client, server, web tier, and other SAP BusinessObjects Enterprise components not to install.

CA SiteMinder® setting: Do not change the value of this parameter. To change this value, use the installer to create another response file.

ADDLOCAL

Specifies which client, server, web tier, and other SAP BusinessObjects Enterprise components to install.

CA SiteMinder® setting: Do not change the value of this parameter. To change this value, use the installer to create another response file.

ADDSOURCE

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: Leave the value empty.

ADVERTISE

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: Leave the value empty.

BIEK

This section details the parameters in the BIEK section of the response file.

BIEK_INSTALL_SAMPLES

Specifies if the installer must install CA templates. This parameter is not related to the CA SiteMinder® reporting templates. The CA SiteMinder® Report Server Configuration wizard installs the required reporting templates. You run the wizard after installing the Report Server.

0

Do not install sample templates.

1

Install sample templates.

CA SiteMinder® setting: 0

SUPPRESS_REBOOT

Specifies if the installer reboots the computer after a successful installation.

0

Lets the installer restart the system after a successful installation.

1

Prevents the installer from restarting the system after a successful installation. Restart the system manually to complete the installation.

CA SiteMinder® setting: 1

Modify the Report Server Response File for UNIX

You modify the installer response file to define installation variables. The default values reflect the information that you entered when you installed the Report Server and saved a response file.

Important! Consider the following items before you modify the file:

- Some parameters identify the type of database that is to function as the report database. Do not use the properties file to change the type of database that the installer is to configure. To change the report database type, use the installer to create another properties file.
- Passing a parameter in the command line overrides the respective setting in the response file.

The Report Server installer generates some parameters automatically. Do not modify the following parameters:

- PRODUCTID_NAME
- BOBJVERSION
- DATACONNECTION
- PRODUCTID_VER
- FUNCTION
- LANGUAGES_TO_INSTALL
- EXPANDSERVERS

Manual Settings

This section details the parameter in the Manual Settings section of the response file.

MACHINENAME

Specifies the name of the Report Server host. This value overrides the local server name. If you do not provide a value, the value defaults to the local host system name.

Paths

This section details the parameter in the Paths section of the response file.

BOBJEDIR

Specifies the path of the bobje directory. The bobje directory is automatically created in the common reporting directory.

Example: /opt/CA/SharedComponents/CommonReporting3/bobje/

CDDIR

Specifies the path to the Disk1 directory in the Report Server installation kit.

LICENSEDIR

Specifies the path to the directory that contains the product license.

Note: Installing the Report Server does not require you to supply a product license.

CA SiteMinder® setting: Leave the value empty.

Product Information

This section details the parameters in the Product Information section of the response file.

BOBJELANG

Specifies the language setting that the installation is to use.

CA SiteMinder® setting: en

PRODUCTID_NAME

Specifies the name of the product that is being installed.

CA SiteMinder® setting: BusinessObjects

BOBJEVERSION

Specifies the version of SAP BusinessObjects Enterprise.

CA SiteMinder® setting: 12.0

PRODUCTID_VER

Specifies the version of the product being installed.

CA SiteMinder® setting: 12.3

BOBJELICENSEKEY

Specifies the license key that is required to install the product. This value appears encrypted.

CA SiteMinder® setting: Do not modify this value.

PIDKEY

Specifies the product ID key. This value appears encrypted.

CA SiteMinder® setting: Do not modify this value.

Installation Information

This section details the parameters in the Installation Information section of the response file.

FUNCTION

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: install

INSTALLTYPE

Specifies the installation method.

new

Install all required server and client components.

custom

Select specific server and client components to install.

webtier

Install only the required web application server components.

CA SiteMinder® setting: new

INSTALLMODE

Specifies a comma–delimited list for the Report Server installation operating modes. This parameter supports the following options:

- install
- modify

- remove
- interactive

CA SiteMinder® setting: install

LOCALNAMESERVER

Specifies the name of the Report Server host system.

BOBJEINSTALLLOCAL

Specifies whether to execute a user or system installation.

CA SiteMinder® setting: user

LANGPACKS_TO_INSTALL

Specifies the language packs to install. CA SiteMinder® only supports the English language pack. The installer installs the English language pack by default.

CA SiteMinder® setting: Leave the value empty.

LANGUAGES_TO_INSTALL

Specifies all languages included in SAP BusinessObjects Enterprise. These values represent the available languages, not the language packs to install.

CA SiteMinder® setting: Leave the comma–delimited list of values.

BOBJEUSERNAME

Specifies the name of the non–root user account.

CA SiteMinder® setting: Be sure that this value matches the value of BIEK_INSTALL_USER in the BIEK section of the response file.

EXPANDSERVERS

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: Leave the value empty.

Tomcat

This section details the parameters in the Tomcat section of the response file.

INSTALLTOMCAT

Specifies if the embedded version of Apache Tomcat must be installed.

CA SiteMinder® setting: yes

Note: Although the installer lets you configure an existing instance of a web application server, CA SiteMinder® only supports the embedded version of Apache Tomcat.

CONNECTORPORT

Specifies the port to which the embedded version of Apache Tomcat must connect and wait for requests.

Default: 8080.

REDIRECTPORT

Specifies the port to which the embedded version of Apache Tomcat must redirect requests.

Default: 8443

SHUTDOWNPORT

Specifies the port to which the SHUTDOWN command for the embedded version of the Apache Tomcat must be issued.

Default: 8005

Application Server

This section details the parameters in the Application Server section of the response file.

AS_DIR

Specifies the path to which the embedded version of Apache Tomcat is installed. The path is automatically set using the installation directory.

Example: /opt/CA/SharedComponents/CommonReporting3//bobje/tomcat/

AS_SERVER

Specifies the type of Java web application server to deploy. If the embedded version of Apache Tomcat is installed, the value defaults to tomcat55. CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: tomcat55

AS_INSTANCE

Specifies the name of the web application server instance. If the embedded version of Apache Tomcat is installed, the value defaults to localhost. CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: localhost

AS_VIRTUAL_HOST

If you are deploying the Report Server to a virtualized environment, specifies the virtual host to which the application must be bound.

CA SiteMinder® setting: Leave the value empty.

AS_ADMIN_PORT

Specifies the port on which the web application server is listening. If the embedded version of Apache Tomcat is installed, the value is empty. CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: Leave the value empty.

AS_ADMIN_USERNAME

Specifies the account name of the administrator account that is used to access the web application server. If the embedded version of Apache Tomcat is installed, the value is empty. CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: Leave the value empty.

AS_ADMIN_PASSWORD

Specifies the password of the administrator account that can access the web application server. If the embedded version of Apache Tomcat is installed, the value is empty. CA SiteMinder® only supports the embedded version of Apache Tomcat.

CA SiteMinder® setting: Leave the value empty.

AS_ADMIN_SECURE

Specifies that an administrator credential must be passed to access the web application server. This parameter applies to a web application server that CA SiteMinder® does not support.

CA SiteMinder® setting: false

AS_APPSERVER_ID

Specifies the name of the application server. This parameter applies to a web application server that CA SiteMinder® does not support.

CA SiteMinder® setting: Leave the value empty.

AS_GROUP_ID

Specifies the group ID of the application server. This parameter applies to a web application server that CA SiteMinder® does not support.

CA SiteMinder® setting: Leave the value empty.

WEBDEPLOYACTION

Specifies the action to perform on the web application server.

CA SiteMinder® setting: deploy

REDEPLOYWEBAPPS

Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: true

CMS Cluster

This section details the parameters in the CMS Cluster section of the response file.

CMSCLUSTER

Specifies if you are adding servers to an existing Content Management Server.

CA SiteMinder® setting: no

CLUSTER_NAMESERVER

If you are clustering servers to a Content Management Server, specifies the name of the Content Management Server.

CA SiteMinder® setting: Leave the value empty.

CLUSTERPORTNUMBER

If you are clustering servers to a Content Management Server, specifies the port on which the Content Management Server is listening. This value defaults to the value of the CMSPORTNUMBER parameter. The parameter is located in the CMS section of the response file.

CA SiteMinder® setting: Be sure that this value matches the value of CMSPORTNUMBER.

CMS

This section details the parameters in the CMS section of the response file.

DBTYPE

Specifies the type of database that is to function as the report database.

CA SiteMinder® settings:

- MySQL

Important! CA SiteMinder® only supports the embedded version of MySQL.

- Oracle

Important! The Report Server is a CA common component that CA products can share. As such, the installer lets you configure the report database to database types and versions that other products support, but CA SiteMinder® does not. For a list of supported database types and versions, see the CA SiteMinder® 12.52 Platform Support Matrix.

SERVICENAME

Specifies the service name of the Oracle database functioning as the report database.

Note: If you are configuring MySQL, this value defaults to BOE120. Leave the default value.

DATABASEUID

Specifies the name of the administrator account that is used to access the report database.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, enter an account name. The installer creates the administrator account with the required privileges.
- If you are configuring Oracle, enter an account name with the following privileges enabled: create session, create table, and create procedure.

  You can also enter an account name with the CONNECT and RESOURCE roles enabled. Be sure to disable the Admin Option setting for both roles.

DATABASEPASSWORD

Specifies the password of the administrator account that is used to access the report database.

CMSNAMESERVER

Specifies the name of the Report Server host system.

CA SiteMinder® setting: Be sure that this value matches the value of LOCALNAMESERVER in the Installation Information section of the response file.

CMSPORTNUMBER

Specifies the port to which the Content Management Server must connect and wait for requests.

Default: 6400

CMSPASSWORD

Specifies the password for the administrator account that is to access the Central Management Server. This password is for the SAP BusinessObjects Enterprise system administrator account.

SIANODENAME

Specifies the name of the Service Intelligence Agent (SIA) node.

Note: Do not use spaces or non–alphanumeric characters.

SIAPORTNUMBER

Specifies the port to which the SIA must connect and wait for requests.

Default: 6410

REINIT

Specifies if the report database must be reinitialized. Do not modify this parameter. This parameter is automatically generated.

CA SiteMinder® setting: yes

MySQL

This section details the parameters in the MySQL section of the response file.

INSTALLMYSQL

Specifies if the embedded version of MySQL must be installed.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, enter yes.
- If you are configuring an Oracle report database, leave the value empty.

SERVICEPORT

If you are installing the embedded version of MySQL, specifies the port to which MySQL must connect and listen for requests.

Default: 3306

Note: If you are configuring an Oracle report database, leave the default value.

MYSQLHOSTNAME

If you are installing the embedded version of MySQL, specifies the IP address of the MySQL host system. The MySQL host system is the same as the Report Server host system.

MYSQLROOTPASSWORD

If you are installing the embedded version of MySQL, specifies the password of the MySQL root user account.

Audit

This section details the parameters in the Audit section of the response file.

These parameters are not related to the CA SiteMinder® audit–based reports. The Content Management Server Auditing Database is used to audit activities specific to the Report Server and is not used for CA SiteMinder®.

A CA SiteMinder® audit database is required to run audit–based reports.

AUDITINGENABLED

Specifies if the Content Management Server Auditing Database is enabled.

- If you are installing the embedded version of MySQL, the Auditing Database is automatically enabled.

  CA SiteMinder® setting: yes

- If you are configuring an Oracle report database, auditing the Content Management Server is not required.

  CA SiteMinder® setting: no

SERVICENAME_AUDIT

Specifies the name of the audit service that the Content Management Server uses. This value defaults to BOE120_AUDIT, even if you are not enabling the Audit Database.

CA SiteMinder® setting: Leave the default value.

SERVICEPORT_AUDIT

Specifies the port number to which the Content Management Server Audit Database must connect and listen for requests. This value defaults to 3306.

CA SiteMinder® setting:

- If you are installing the embedded version of MySQL, match this value to the SERVICEPORT parameter in the MySQL section of the response file.
- If you are configuring an Oracle report database, leave the default value.

MYSQLHOSTNAME_AUDIT

Specifies the IP address of Content Management Server Audit Database host system.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, match this value to the MYSQLHOSTNAME parameter in the MySQL section of the response file.
- If you are configuring an Oracle report database, leave the value empty.

DATABASEUID_AUDIT

Specifies the name of the administrator account that is used to access the Content Management Server Auditing Database.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, match this value to the DATABASEUID parameter in the MySQL section of the response file.
- If you are configuring an Oracle report database, leave the value empty.

DATABASEPWD_AUDIT

Specifies the password of the administrator account that is used to access the Content Management Server Auditing Database.

CA SiteMinder® settings:

- If you are installing the embedded version of MySQL, match this value to the MYSQLROOTPWD parameter in the MySQL section of the response file.
- If you are configuring an Oracle report database, leave the value empty.

Marketing Products

This section details the parameters in the Marketing Products section of the response file.

ENABLEMP

Specifies which client, server, web tier, and other SAP BusinessObjects Enterprise to enable manually.

CA SiteMinder® setting: Leave the value empty.

DISABLEMP

Specifies which client, server, web tier, and other SAP BusinessObjects Enterprise components disable manually.

CA SiteMinder® setting: Leave the value of this parameter empty.

BIEK

This section details the parameters in the BIEK section of the response file.

BIEK_INSTALL_USER

Specifies the non–root user account that the installer must use.

BIEK_INSTALL_GROUP

Specifies the group to which the non–root user belongs.

BIEK_CASHCOMP

Specifies the full path to which the CA Shared Components environment variable (CASHComp) must be set. If CASHComp is already set, the installer ignores this value.

BIEK_INSTALL_SAMPLES

Specifies if the installer must install CA templates. This parameter is not related to the CA SiteMinder® reporting templates. The CA SiteMinder® Report Server Configuration wizard installs the required reporting templates. You run the wizard after installing the Report Server.

0

Do not install sample templates.

1

Install sample templates.

CA SiteMinder® setting: 0

BIEK_MIGRATE_CMS_DATA

Do not modify this parameter. This parameter is for upgrades only.

CA SiteMinder® setting: 0

BIEK_SOURCE_CMS_PASSWORD

Do not modify this parameter. This parameter is for upgrades only.

CA SiteMinder® setting: Leave the value empty.

Modify the CA SiteMinder® Report Server Configuration Wizard Properties File

You modify the Report Server Configuration Wizard properties file to define configuration variables. The default parameters, passwords, and paths in this file reflect the information entered the last time the wizard ran.

The properties file has the following parameters:

DEFAULT_BOXI_INSTALL_PATH

Specifies the Report Server installation path.

DEFAULT_BOXI_PASSWORD

Specifies the password of the default BusinessObjects administrator account.

Note: If you are using encrypted value in ENCRYPTED_BOXI_PASSWORD, this parameter does not require a value.

ENCRYPTED_BOXI_PASSWORD

Specifies the encrypted password of the default BusinessObjects administrator account.

Important! Do not change the encrypted value. To enter another password, comment the encrypted password and specify a value for DEFAULT_BOXI_PASSWORD.

DEFAULT_AUDIT_DATABASE_TYPE

Specifies the type of database functioning as the CA SiteMinder® audit store.

Note: You do not have to configure a CA SiteMinder® audit database before running the Report Server Configuration Wizard.

Values: 1 or 2

1

Specifies Microsoft SQL Server.

2

Specifies Oracle.

Run the Report Server Installer

You run an unattended installation to install the Report Server without user interaction.

Before You Install

Consider the following items before installing the Report Server:

- You install the Report Server using the installation media on the Technical Support site.

  Note: For a list of installation media names, see the *Policy Server Release Notes*.

- The Report Server is compiled as 32–bit native binary and is designed to use 32–bit data source middleware connectivity. If you are installing to a Windows 64–bit operating system, be sure to create the DSN using odbcad32.exe. This executable is located in the following location:

  install_home\Windows\SysWOW64.

  install_home

  Specifies the installation path of the Windows operating system.

- The Report Server installation includes the following components that run as processes:

  - The Content Management Server
  - The Server Intelligence Agent

  These components require TCP/IP ports to communicate. The installer lets you modify the default settings to prevent port conflicts on the Report Server host system.

- **Important!** The installation zip contains multiple folders. The Report Server installer requires this folder structure. If you moved the Reports Server installer after extracting the zip, copy the entire folder structure to the same location. Be sure that you execute the installation media from the folder structure.

Windows

Follow these steps:

1. Exit all applications that are running.
2. Open a command prompt.
3. Change the directory to *temporary_location*.

   temporary_location

   Specifies the location to which you copied the installation media.

4. Enter the following command:

   ```
   installation_media silent path_to_response_file
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   installation_media

   Specifies the name of the Report Server installation executable.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.

   path_to_response_file

   Specifies the path to the file. The path must include the response file name.

   Note: The response file does not have to be in the same directory as the installation executable.

   The silent installation begins.

UNIX

Follow these steps:

1. Exit all applications that are running.
2. Be sure that you are using an account with root–user privileges.
3. Open a Bourne shell and navigate to *temporary_location*.

   temporary_location

   Specifies the location to which you copied the installation media.

4. Enter the following command:

   ```
   ./installation_media silent path_to_response_file
   ```

   installation_media

   Specifies the name of the Report Server executable.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.

   path_to_response_file

   Specifies the path to the response file. The path must include the response file name.

   Note: The response file does not have to be in the same directory as the installation executable.

   The silent installation begins.

Install the Report Templates

You run an unattended installation to install the CA SiteMinder® report templates without user interaction.

Before You Install

You install the CA SiteMinder® report templates using the installation media on the Technical Support site.

Note: For a list of installation media names, see the *Policy Server Release Notes*.

Windows

Follow these steps:

1. Exit all applications that are running.
2. Be sure that the Report Server is started (see page 426).
3. Open a command prompt.
4. Change the directory to temporary to which you copied the installation media.
5. Enter the following command:

   ```
   installation_media -f properties_file -i silent
   ```

   Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   installation_media

   Specifies the name of the CA SiteMinder® Report Server Configuration Wizard installation executable.

   Note: For a list of installation media names, see the *Policy Server Release Notes*.

   -f *properties_file*

   Specifies the path to the properties file. The path must include the properties file name.

   Note: The properties file does not have to be in the same directory as the installation executable.

-i silent

Specifies that the installer run silently.

The report templates installation begins.

6. After the installation finishes, restart the Report Server.

Note: You are required to register the Report Server before you can create reports.

More information:

How to Register the Report Server (see page 416)

UNIX

Follow these steps:

1. Exit all applications that are running.
2. Be sure that the Report Server is started (see page 426).
3. Open a shell and navigate to where the installation media is located.
4. Enter the following command:

```
./installation_media -f properties_file -i silent
```

installation_media

Specifies the name of the CA SiteMinder® Report Server Configuration Wizard installation media.

Note: For a list of installation media names, see the *Policy Server Release Notes*.

-f *properties_file*

Specifies the path to the properties file. The path must include the properties file name.

Note: The properties file does not have to be in the same directory as the installation executable.

-i silent

Specifies that the installer run silently.

The report template installation begins.

5. After the installation finishes, restart the Report Server.

Note: You are required to register the Report Server before you can create reports.

More information:

How to Register the Report Server (see page 416)

Appendix A: Configuring the Policy Server for an International Environment

This section contains the following topics:

Policy Servers in an International Environment

The Policy Server supports CA SiteMinder® data stores residing in an Oracle or SQL Server database, and LDAP servers for an international environment.

Planning Considerations Before Installing the Policy Server

Consider the following items before you install the Policy Server:

- Use supported operating system and third–party software.
- Create supported databases:
  - Before creating databases for storing policy or session data, be sure that they are formatted with UTF–8 encoding.
  - User store databases are not limited to UTF–8 encoding. You can create user databases in the local character set encoding.

    Note: The Active Directory namespace does not support multi–byte characters. Regardless of the code page you are using, CA SiteMinder® treats characters as they are defined in Unicode. Although your code page can reference a special character as single-byte, CA SiteMinder® treats it as a multi–byte character if Unicode defines it as such.
- All Administrative UI fields support multi–byte characters.
- Some Policy Server components support multi–byte and ASCII characters in an internationalized environment.
- CA SiteMinder® supports multi–byte character (MBCS) URLs.

Note: For a list of supported CA and third-party components, refer to the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support site.

Policy Server Components Supporting Multi-byte Characters

The following Policy Server components support multi–byte and ASCII characters in an internationalized environment:

- Administrative UI
- Policy Server Management Console
- Authentication Schemes
  - HTML Forms
  - X.509 Client Certificate
  - X.509 Client Certificate and HTML Forms
  - X.509 Client Certificate or HTML Forms
  - RADIUS CHAP/PAP
  - SecurID Authentication
  - Anonymous Authentication
  - Custom Authentication
  - Impersonation Authentication
- Password Services

  Note: Password Services are limited to ASCII characters, but can support a multi–byte character URL as a redirection URL.
- Responses
- Post Preservation
- CA SiteMinder® Test Tool
- Audit logging to text files
- Audit logging to ODBC databases
- smobjimport
- XPSExport and XPSImport
- Java Agent API

Support for Multi-Byte Character URLs

CA SiteMinder® supports URLs that contain multi-byte characters (MBCS). MBCS URL support includes support for:

- **Internationalized domain names** - An *internationalized domain name* (IDN) is an Internet domain name that can contain non-ASCII characters, including letters with diacritics and characters from non-Latin scripts, such as Arabic and Chinese.
- **Internationalized resource identifiers** - An *internationalized resource identifier* (IRI) is the international equivalent of a uniform resource identifier (URI). An IRI can contain ASCII characters and characters from a MBCS set; a URI is limited to a subset of ASCII characters.

MBCS URL support lets:

- CA SiteMinder® protect resources that are accessed through MBCS URLs.
- You configure specific authentication schemes using an IDN and an IRI.

How to Enable MBCS URL Support

Support for MBCS URLs in a CA SiteMinder® environment requires that:

- The Web browsers used to access the protected resources meet specific requirements.
- The Web server implementation in your environment meets specific requirements.
- Specific default bad characters are removed from the Web Agent Configuration Object.

To enable support for MBCS URLs:

1. Ensure that the Web browsers meet the requirements for MBCS URLs.
2. Ensure that the Web servers meet the requirements for MBCS URLs.
3. Configure the Web Agent Configuration Object.

Web Browser Requirements for MBCS URLs

Web browsers must be able to send requests to Web servers that serve resources in UTF-8 format and whose domain names contain non-ASCII characters.

The Web browsers used to access the protected resources must be able to:

- Support Internationalized Domain Names (IDNs).
- Support Internationalized Resource Identifiers (IRIs).
- Send requests in UTF-8 format.

Web Server Requirements for MBCS URLs

A Web server can support MBCS URLs if it meets at least one of the following requirements:

- The Web server can convert UTF-8 requests to the local character set encoding.

  or

- The Web server can store files in UTF-8 format. This lets the Web server serve the file when it receives the IRI request from the Web browser in UTF-8 format.

Enable Multi-byte Character Support

MBCS support requires that you remove specific high-bit ASCII character values from the Web Agent Configuration Object.

Note: Removing the high-bit ASCII characters prevents the Web Agent from blocking the specific characters.

To enable MBCS support

1. Open the Administrative UI
2. Click Infrastructure, Agents.
3. Click Agent Configuration, Modify Agent Configuration.

   The Modify Agent Configuration pane appears.
4. Enter search criteria and click Search.

   Agent configuration objects matching the search criteria appear.
5. Select the Agent configuration object you want and click Select.

   Agent Configuration parameters are listed in the Parameters group box.
6. Click the Edit icon for BadURLChars.

   The Edit Parameter pane appears.
7. Remove the following from the Values field:
   - %00-%1f
   - %7f-%ff
8. Click OK.

   The edited values appear in the BadURLChars field.
9. Click Submit.

   The Web Agent Configuration Object is configured to support MBCS URLs.

Protect a Resource with MBCS URLs

Support for MBCS URLs lets CA SiteMinder® protect resources that are accessed through URLs that contain non-ASCII characters.

When creating a realm and the associated rule or rules to protect the resource, you can enter a MBCS URL in the Resource field. Users can access the protected resource using a browser that supports IDNs and IRIs.

Note: More information on creating realms and rules exists in the *Policy Server Configuration Guide*.

Authentication Schemes Supporting MBCS URLs

You can configure the following authentication schemes with an IDN in the Server Name field and an IRI in the Target field:

- Basic over SSL
- HTML Form Template
- HTML Form Template over SSL
- X509 Client Cert
- X509 Client Cert and Forms

Note: Netscape and Firefox do not accept redirections to URLs that contain an IDN. Entering an IDN for a forms-related authentication scheme results in a failure unless Punycode http://en.wikipedia.org/wiki/Punycodeis used. More information about configuring authentication schemes exists in the *Policy Server Configuration Guide*.

Configure CA SiteMinder® Data Stores Supporting International Characters

You can configure CA SiteMinder® data stores in SQL Server or Oracle databases. When configuring these data stores, be aware that the Policy Server only supports UTF-8 encoding and, as a result, you must use databases that support this encoding type.

Note: This section applies to configuring CA SiteMinder® data stores in relational databases. More information on configuring these stores in LDAP servers exists in LDAP Directory Servers as a Policy Store or Key Store.

Configure an International CA SiteMinder® Data Store in SQL Server

To create policy, keys, session, or key stores, configure a CA SiteMinder® data store in the SQL Server database.

Note: By default, SQL Server supports UTF-8 character encoding.

Configure an International CA SiteMinder® Data Store in Oracle

To configure an international CA SiteMinder® data store in Oracle

1. On the machine where Oracle is installed, create a custom Oracle database that supports UTF-8 character encoding.

   Note: For more information and instructions, see Oracle's documentation.

   To verify if an existing Oracle database supports UTF-8 character encoding, run the following query:

   Select * from nls_database_parameters where parameter = 'NLS_CHARACTERSET'

2. Create policy, keys, session, or key stores for the Policy Server, by configuring a CA SiteMinder® data store in the Oracle database.

Solaris/LINUX Red Hat Policy Server Logging UTF-8 Characters to an Oracle Database

A Solaris/LINUX Red Hat Policy Server can log UTF-8 characters to an Oracle audit log database. To enable this configuration, you need to set the following environment variables:

For a simplified Chinese operating system

- LANG=zh_CN.utf8

For a Japanese operating system

- LANG=jp_JP.UTF-8

You set the LANG variable system-wide or just for the Policy server process.

Note: To avoid impacting any other applications, make sure that you set this variable for the Policy Server process only.

Database Driver Variable

- IANAAppCodePage=utf-8

You set this variable in the appropriate data source definition section of the system_odbc.ini file, installed in *<policy_server_installation>*/db.

Oracle Client Settings

Since the Policy Server uses the Oracle wire protocol driver, an Oracle client is not necessary. However, if you need an Oracle SQLPLUS client in your environment to read data from the audit log database, you may have to set one or both of the following environment variables to correctly display the multi-bytes characters:

For a simplified Chinese operating system

- LANG=zh_CN.utf8

For a Japanese operating system

- LANG=jp_JP.UTF-8

For the Oracle SQLPlus Client

- NLS_LANG (For example, NLS_LANG=Japanese_Japan.UTF8)

Note: For more information, see the operating system and database client configuration manual.

Configure a User Store that Supports Unicode in SQL Server

Using the smsampleusers_sqlserver.sql file installed with the Policy Server, you can configure a user store in a SQL Server database. This file is installed in the *siteminder_installation*\db\SQL directory.

Note: User stores are not limited to UTF-8 format. You can create a user store in the local character set encoding.

Follow these steps:

1. Edit the smsampleusers_sqlserver.sql file, by doing the following:
   a. Replace every varchar instance with **nvarchar**.
   b. Place an **N** before any insert statement with international strings.

Japanese example:

```
insert into SmUser ( UserID , Name, Password,
LastName, FirstName, ...)

values (12, N'やまもと',
'siteminder','guest','guest','guest@mycompany.com...)
```

1. Import the smsampleusers_sqlserver.sql file.

   Note: More information on importing the smsampleusers_sqlserver.sql file exists in Sample User Directories.

2. Open the Policy Server User Interface's SiteMinder ODBC Query Scheme dialog and modify the policy store's SQL query scheme by placing an **N** before every %s reference in any = %s statement.

Example:

The following sample query scheme statements:

select Name, 'User' from SmUser where Name = '%s' Union select Name, 'Group' from SmGroup where Name = '%s'

should become:

select Name, 'User' from SmUser where Name = **N**'%s' Union select Name, 'Group' from SmGroup where Name = **N**'%s'

1. Stop and restart the Policy Server.

   The user store configuration is complete and now supports multi-byte characters.

Configure a Japanese User Store in Oracle

Using the smsampleusers_oracle.sql file installed with the Policy Server, you can configure a user store in an Oracle database. This file is installed in the <*siteminder_installation*>\db\SQL directory.

Note: User stores are not limited to UTF-8 format. You can create a user store in the local character set encoding.

To configure a Japanese user store in Oracle

1. Create a database for the user data that supports Oracle's UTF-8 NLS_CHARACTERSET encoding.
2. Using Oracle's SQL-Plus, import the smsampleusers_oracle.sql file.

   Note: More information on importing the smssampleusers_oracle.sql file exists in Sample User Directories. Be aware that if you are inserting Japanese characters, import the file from a Japanese operating system.

   The user store configuration is complete.

Appendix B: Modified Environment Variables

This section contains the following topics:

Modified Windows Environment Variables

Policy Server

The Policy Server installation adds and modifies the following environment variables in a Windows environment:

- NETE_PS_ROOT = $INSTALL_PATH$
- NETE_PS_PATH = $INSTALL_PATH$$/$bin;
$INSTALL_PATH$$/bin/$thirdparty;$INSTALL_PATH$$/$lib
- NETEGRITY_LICENSE_FILE = %NETE_PS_ROOT%$/$license$/$license.dat
- NETE_JVM_OPTION_FILE = %NETE_PS_ROOT%$/$config$/$JVMOptions.txt
- NETE_DOC_ROOT=$INSTALL_PATH$$/$netegrity_documents
- NETE_PS_OPACK="INSTALLED"
- NETE_JRE_ROOT = HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Runtime Environment\1.7 in JAVAHOME value
- NETE_JAVA_PATH=%NETE_JRE_ROOT%$/$bin;%NETE_JRE_ROOT%$/$bin$/$server
- NETE_JDK_ROOT = HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Development Kit\1.7 in JAVAHOME value
- NETE_SHORTCUTS = C:\Documents and Settings\All Users\Start Menu\Programs\CA SiteMinder®

  Note: This is the default location.

Administrative UI

The Administrative UI installation does not add environment variables in a Windows environment.

Report Server

The Report Server installation adds and modifies the following environment variables in a Windows environment:

- IAM_RPTSRV_HOME=$REPORT_SERVER_LOC$
- BOE_SSL_JVMOPTIONS="-Dcom.ca.rptsrv.home=%IAM_RPTSRV_HOME% -Djava.library.path=%IAM_RPTSRV_HOME%/external/bin"

Modified UNIX Environment Variables

Policy Server

The Policy Server installation adds and modifies the following environment variables in a UNIX environment:

- NETE_PS_ROOT = $INSTALL_PATH$
- NETE_PS_PATH = $INSTALL_PATH$$/$bin;
$INSTALL_PATH$$/$bin$/$thirdparty;$INSTALL_PATH$$/$lib
- NETEGRITY_LICENSE_FILE = %NETE_PS_ROOT%$/$license$/$license.dat
- NETE_JVM_OPTION_FILE = %NETE_PS_ROOT%$/$config$/$JVMOptions.txt
- NETE_DOC_ROOT=$INSTALL_PATH$$/$netegrity_documents
- NETE_PS_OPACK="INSTALLED"
- NETE_JDK_ROOT = $JDK_PATH$
- NETE_JRE_ROOT = $JRE_PATH$
- NETE_JAVA_PATH=%NETE_JRE_ROOT%$/$bin;%NETE_JRE_ROOT%$/$bin$/$server

Administrative UI

The Administrative UI installation does not add environment variables in a UNIX environment.

Report Server

The Report Server installation adds and modifies the following environment variables in a UNIX environment:

- IAM_RPTSRV_HOME=$REPORT_SERVER_LOC$
- BOE_SSL_JVMOPTIONS="-Dcom.ca.rptsrv.home=$IAM_RPTSRV_HOME -Djava.library.path=$IAM_RPTSRV_HOME%/external/bin"

Index