



Policy Server Installation Guide

r12.0 SP2



This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be used or disclosed by you except as may be permitted in a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print 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 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 THE END USER 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 is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

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

Copyright © 2009 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Product References

This document references the following CA products: CA SiteMinder®

Contact CA

Contact Technical Support

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

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

Provide Feedback

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

If you would like to provide feedback about CA product documentation, complete our short [customer survey](#), which is also available on the CA Support website, found at <http://ca.com/docs>.

Contents

Chapter 1: Installation Overview	15
Intended Audience	15
Sample SiteMinder Installation	15
Policy Server	16
Federation Security Services Administrative UI	17
Policy Store	17
SiteMinder Administrative UI	17
CA Business Intelligence	18
SiteMinder Audit Database	19
Agents	19
Administrative User Interfaces Overview	20
SiteMinder Documentation	20
Install the Bookshelf on Windows	21
Install the Bookshelf on UNIX	22
Use the SiteMinder Bookshelf	23
Pre-Installation Checklist	23
 Chapter 2: Policy Server Installation Requirements	 25
Policy Server System Requirements	25
Windows	25
UNIX	26
 Chapter 3: Administrative UI Installation Requirements	 27
System Requirements	27
Windows	27
UNIX	28
 Chapter 4: Report Server Installation Requirements	 29
System Requirements	29
Windows	29
UNIX	30
Solaris Required Patch Clusters	30
Report Database Requirements	30
Connectivity Requirements	31

Chapter 5: Installing the Policy Server on Windows Systems 33

Installation Road Map	34
Before You Install the Policy Server	35
How to Install the Policy Server	35
Policy Server Component Considerations	36
Policy Store Considerations	38
FIPS Considerations	38
Gather Information for the Installer	40
Run the Policy Server Installer	44
Troubleshoot the Policy Server Installation	46
Enable SNMP Event Trapping	46
Configure a Policy Store	47
Unattended Policy Server Installation	47
Policy Server Configuration Wizard	47
How to Use the Configuration Wizard	48
Reinstall the Policy Server	53
Uninstall the Policy Server and Documentation	54
How to Uninstall the Policy Server	54
Uninstall the Documentation	57
Scripting Interface	57

Chapter 6: Installing the Policy Server on UNIX Systems 59

Installation Road Map	60
Solaris 10 Zone Support	61
Global Zone Support	61
Sparse-root Zone Support	61
Whole-root Zone Support	62
Solaris and HP-UX Patches	62
How to Prepare for the Policy Server Installation	63
Create a New UNIX Account	63
Modify the UNIX System Parameters	63
Unset Localization Variables	64
Unset the LANG Environment Variable	64
Before You Install the Policy Server	65
How to Install the Policy Server	66
Policy Server Component Considerations	66
Policy Store Considerations	68
FIPS Considerations	68
Gather Information for the Installer	70
Install the Policy Server in GUI Mode	74
Install the Policy Server in Console Mode	76

Troubleshoot the Policy Server Installation	78
Restart the SNMP Daemon	79
Configure a Policy Store	79
Configure Auto Startup	79
Unattended Policy Server Installation	80
Policy Server Configuration Wizard	80
How to use the Configuration Wizard	81
Backup Versions of Obj.conf and Magnus.conf Files	88
Uninstall the Policy Server and Documentation	88
How to Uninstall the Policy Server	88
How to Uninstall the Documentation	92
Scripting Interface	93

Chapter 7: Configuring LDAP Directory Servers as a Policy or Key Store 95

LDAP Directory Servers as a Policy or Key Store	95
Installation Road Map	96
Important Considerations	97
CA Directory as a Policy Store	97
Gather Directory Server Information	97
How to Configure the Policy Store	98
Sun Java System Directory Server as a Policy Store	110
Gather Directory Server Information	110
How to Configure the Policy Store	111
Active Directory as a Policy Store	121
Gather Directory Server Information	122
How to Configure the Policy Store	123
Support for Active Directory ObjectCategory Indexing Attribute	131
Enable or Disable ObjectCategory Attribute Support	132
Microsoft ADAM/AD LDS as a Policy Store	132
ADAM/AD LDS Prerequisites	133
Gather Directory Server Information	134
How to Configure the Policy Store	135
SiteMinder Key Store Overview	144
Configure a Key Store in an Existing Policy Store	144
Configure a Separate Key Store	144

Chapter 8: Configuring SiteMinder Data in a Relational Database 147

Relational Databases as a Policy or Key Store	147
Installation Road Map	148
Important Considerations	149
Schema Files for Relational Databases	149

SQL Server Schema Files	150
Oracle Schema Files	151
Configure a SQL Server Policy Store	151
Gather Database Information	152
How to Configure the Policy Store	153
Configure an Oracle Policy Store	165
Prerequisites for an Oracle 10g Database	166
Gather Database Information	168
How to Configure the Policy Store	169
Configure SQL Server Data Stores	186
How to Store Key Information in SQL Server	187
How to Store Audit Logs in SQL Server	193
How to Store Token Data in SQL Server	199
How to Store Session Information in SQL Server	206
Configure Oracle Data Stores	212
How to Store Key Information in Oracle	212
How to Store Audit Logs in Oracle	224
How to Store Token Information in Oracle	235
How to Store Session Information in Oracle	247
Sample User Directories	258
Configure an Oracle Sample User Directory	259
Configure a SQL Server Sample User Directory	259

Chapter 9: Installing the Administrative UI 261

Installation Road Map	261
Administrative UI Installation Options	262
Trusted Relationship with a Policy Server	263
Administrative UI Installation Checklist	264
How to Install the Administrative UI	264
Gather Information for the Installer	265
Reset the Administrative UI Registration Window	265
Install the Administrative UI	267
Troubleshoot the Administrative UI Installation	272
How to Register the Administrative UI	272
Start the Application Server	273
Register the Administrative UI	274
Stop the Application Server	275
Administrator Credentials	275
Administrative UI High Availability	276
How to Configure Additional Policy Server Connections	276
Run the Registration Tool	277
Gather Registration Information	279

Register the Audit Database with the Administrative UI	332
Audit Database and Report Server Connectivity	333
Stop the Report Server	334
How to Uninstall Reporting	335
Uninstall the Report Server from Windows	335
Uninstall the Report Server from UNIX	336
Uninstall the Report Server Configuration Wizard from Windows	336
Uninstall the Report Server Configuration Wizard from UNIX	337
Remove Windows Items	337
Remove UNIX Items	338
Delete a Report Server Connection to the Administrative UI	338
Reinstall the Report Server	339

Chapter 12: Configuring the OneView Monitor 341

OneView Monitor Overview	341
System Requirements for OneView Monitor	342
Configure the OneView Monitor	342
Limitation of OneView Monitor GUI/IIS Web Agent on Same Machine	342
How to Configure the OneView Monitor GUI on Windows/IIS	343
Prerequisites to Installing ServletExec on Windows	343
Install ServletExec/ISAPI on Windows 2003/IIS	343
Set Permissions for IIS Users After Installing ServletExec	344
How to Configure the OneView Monitor GUI on UNIX/Sun Java System	344
Prerequisites to Installing ServletExec	344
Disable Servlets in Sun Java System 6.0	344
Install ServletExec/AS on UNIX/Sun Java System	345
Start the OneView Monitor Service	347
Access the OneView Monitor GUI	347
Monitor a Policy Server Cluster	347

Chapter 13: SNMP Support 349

SNMP Support Overview	349
Prerequisites for Windows and UNIX Systems	351
Windows Prerequisites	351
UNIX Systems Prerequisites	351
Configure the SNMP Agent on Windows	352
How to Configure SNMP Event Trapping on Windows	353
Configure the SNMP Agent on UNIX Systems	354
How to Configure SNMP Event Trapping on UNIX Systems	355
Test SNMP Gets for Red Hat Enterprise Linux Advanced Server	356
Test SNMP Gets for HP-UX	356

Appendix A: Installing the Administrative UI to an Existing Application Server **357**

Administrative UI Installation Options	357
Administrative UI Installation Requirements	358
Administrative UI System Requirements	358
Application Server Requirements	359
Trusted Relationship with a Policy Server	362
Administrative UI Installation Checklist	362
How to Install the Administrative UI	363
Gather Application Server Information	363
Install the Administrative UI	366
How to Register the Administrative UI	369
Reset the Administrative UI Registration Window	370
Start the Application Server	372
Register the Administrative UI	373
Stop the Application Server	374
Administrator Credentials	375
Administrative UI High Availability	376
Uninstall the Administrative UI on Windows	376
Uninstall the Administrative UI on UNIX	377

Appendix B: Installation Worksheets **379**

Policy Server Worksheets	379
Required Information Worksheet	379
OneView Monitor Information Worksheet	379
Microsoft ADAM/AD LDS Server Information Worksheet	380
Sun Java System Directory Server Information Worksheet	380
SM Key Database Information Worksheet	381
Policy and Data Store Worksheets	381
CA Directory Information Worksheet	381
Sun Java System Directory Server Information Worksheet	382
Active Directory Information Worksheet	382
Microsoft ADAM/AD LDS Information Worksheet	383
SQL Server Information Worksheet	383
Oracle Information Worksheet	384
Oracle RAC Information Worksheet	384
Administrative UI Installation Worksheets	385
Prerequisite Installer Worksheet	385
JBoss Worksheet	385
WebLogic Worksheet	386
WebSphere Worksheet	386

Policy Server Registration Worksheet	387
Reporting Worksheets.....	387
Installation Credentials Worksheet.....	387
MySQL Report Database Worksheet.....	388
SQL Server Report Database Worksheet	388
Oracle Report Database Worksheet	388
Apache Tomcat Worksheet	389
Report Server Configuration Worksheet.....	389
Report Server Registration Worksheet	389

Appendix C: Troubleshooting **391**

Policy Server Troubleshooting	391
NETE_PS_ALT_CONF_FILE Environment Variable on Solaris	391
Policy Server Fails to Start After Installation	392
Winsock error 10054 message.....	392
Policy Store Troubleshooting	393
Policy Stores with Large Numbers of Objects	393
SSL initialization failed: error -8174 (security library: bad database.)	393
ODBC Policy Store Import Fails with UserDirectory Error	394
OneView Monitor Troubleshooting	395
Fix Modified UNIX/Sun Java System Web Server Configuration Files	395
Windows/IIS Virtual Path to /sitemindermonitor Does Not Exist	396
Administrative UI Troubleshooting	397
Cannot Register a Policy Server Connection	397
API Error Appears.....	397
Registration Not on File Error Appears	398
Invalid Registration File Error Appears	399
Registration Fails without Timeout	400
Cannot Find the Administrative UI Registration Log	401
Search Fails with Timeout Error.....	401
Cannot Find the Default Logging File	402
Default Log File does not Provide Enough Information	403
FSS Administrative UI Troubleshooting	403
FSS Administrative UI Fails to Start in IE	404
FSS Administrative UI does not appear on Windows	404
FSS Administrative UI Fails to Start on a Sun Java Web Server	405
Report Server Troubleshooting	406
Report Server Installation Fails with Error Regarding Characters	406
Audit-based Reports Return No Results	406
Java Error Messages When Uninstalling	407
Set the JRE in the PATH Variable on Windows	407
Set the JRE in the PATH Variable on Solaris	407

Adobe Acrobat Reader Won't Install	408
Problem With Using Active Directory as a User Store	408
AE failed to load library 'smjavaapi'. System error	408

Appendix D: Unattended Installation 411

Silent Installation	411
Silent Installation Guidelines	411
Default Properties Files	412
Policy Server Properties File	412
Administrative UI Properties Files	412
Reporting Properties File	413
How to Silently Install a Policy Server	413
Modify the Policy Server Installer Properties Files	414
Run the Policy Server Installer	419
Troubleshoot the Policy Server Installation	421
Stop an Unattended Policy Server Installation	422
How to Silently Install the Administrative UI	422
Modify the Prerequisite Installer Properties File	423
Modify the Administrative UI Installer Properties File	424
Silently Install the Administrative UI	426
How to Silently Install Reports	429
Modify the Report Server Properties File	429
Modify the SiteMinder Report Server Configuration Wizard Properties File	437
Silently Install the Report Server	438
Silently Install Report Templates	440

Appendix E: Configuring the Policy Server for an International Environment 443

Policy Servers in an International Environment	443
Planning Considerations Before Installing the Policy Server	443
User Interface Fields Supporting Multi-byte Characters	444
Policy Server Components Supporting Multi-byte Characters	446
Support for Multi-Byte Character URLs	447
Configure SiteMinder Data Stores Supporting International Characters	449
Configure an International SiteMinder Data Store in SQL Server	449
Configure an International SiteMinder Data Store in Oracle	450
Configure a Japanese User Store in SQL Server	451
Configure a Japanese User Store in Oracle	452

Appendix F: Modified Environment Variables 453

Modified Windows Environment Variables	453
Modified UNIX Environment Variables	454

Appendix G: Platform Support and Installation Media	455
Locate the SiteMinder Platform Support Matrix	455
Locate the Bookshelf	456
Locate the Installation Media	456
 Index	 459

Chapter 1: Installation Overview

This section contains the following topics:

[Intended Audience](#) (see page 15)

[Sample SiteMinder Installation](#) (see page 15)

[Administrative User Interfaces Overview](#) (see page 20)

[SiteMinder Documentation](#) (see page 20)

[Pre-Installation Checklist](#) (see page 23)

Intended Audience

This guide is intended for users who have a working knowledge of:

- directory servers
- relational databases
- Web servers

This guide assumes you are familiar with Java, J2EE standards, and application server technology, and that you have the following technical knowledge:

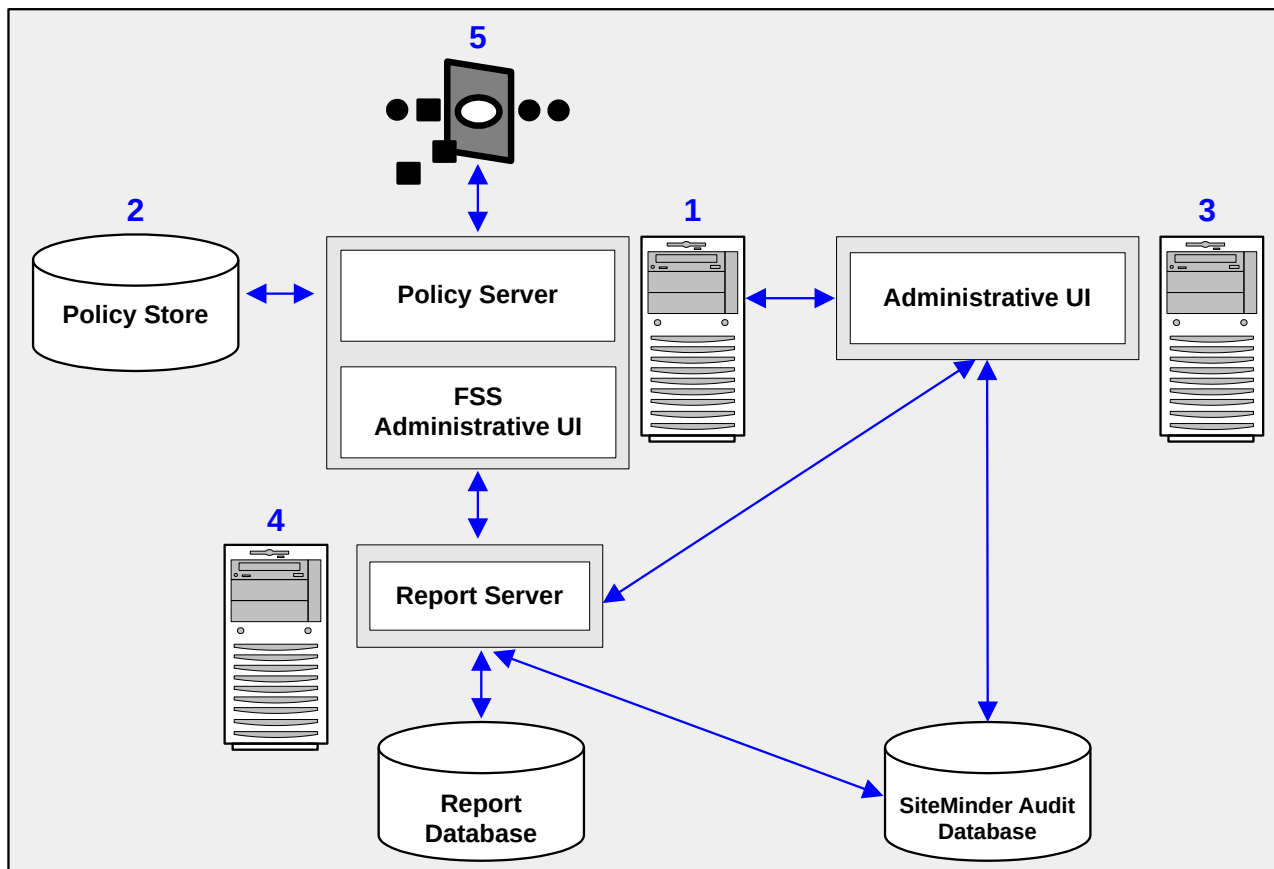
- An understanding of J2EE application servers and multi-tier architecture.
- Experience with managing an application server.

Sample SiteMinder Installation

Installing SiteMinder requires you to install and configure several components. The following diagram shows:

- The Policy Server, SiteMinder Federation Security Services UI (FSS Administrative UI), and policy store installed and configured on one system.
- The SiteMinder Administrative UI (Administrative UI) installed on a second system.

- CA Business Intelligence (Report Server) installed and configured on a third system.
- The order in which you install and configure each component.



Policy Server

(Required) A SiteMinder Policy Server (Policy Server) acts as the Policy Decision Point (PDP). The purpose of the Policy Server is to evaluate and enforce access control policies, which it communicates to a SiteMinder Agent. A Policy Server provides the following:

- Policy-based user management
- Authentication services
- Authorization services
- Password services
- Session management
- Auditing services

The Policy Server interacts with all other major components to perform these tasks.

Federation Security Services Administrative UI

(Optional) The SiteMinder Federation Security Services Administrative UI (FSS Administrative UI) is an applet-based application that is optionally installed with the Policy Server. Federation Security Services components consist of the affiliates (consumers, service providers, resource partners) and SAML authentication schemes that you configure to support federated communication between two partners.

The FSS Administrative UI is intended for only managing tasks related to SiteMinder Federation Security Services.

Policy Store

(Required) The SiteMinder policy store (policy store) is an entitlement store that resides in an LDAP directory server or ODBC database. The purpose of this component is to store all policy-related objects, including the:

- Resources SiteMinder is protecting
- Methods used to protect those resources
- Users or groups that can or cannot access those resources
- Actions that must take place when users are granted or denied access to protected resources

The Policy Server uses this information, collectively known as a policy, to determine if a resource is protected and if an authenticated user is authorized to access the requested resources.

Note: For more information about configuring a policy store, see the documentation roadmap.

SiteMinder Administrative UI

(Required) The SiteMinder Administrative UI (Administrative UI) is a web-based administration console that is installed independent of the Policy Server. The Administrative UI functions as the primary UI in a SiteMinder implementation and is intended for managing all tasks related to access control, such as:

- Authentication and authorization policies
- Enterprise Policy Management (EPM)
- Reporting and policy analysis

The Administrative UI is intended for viewing, modifying, and deleting all Policy Server objects, except objects related to Federation Security Services (FSS). All federation-related configuration tasks are managed using the FSS Administrative UI.

CA Business Intelligence

(Optional) CA Business Intelligence is a set of reporting and analytic software that various CA products use for the purposes of presenting information and supporting business decisions. CA products use CA Business Intelligence to integrate, analyze, and then present, through various reporting options, information required for effective enterprise IT management.

Included in CA Business Intelligence is BusinessObjects Enterprise XI 2.1, a complete suite of information management, reporting, and query and analysis tools. CA Business Intelligence installs BusinessObjects Enterprise XI as a stand-alone component. In this guide, this stand-alone component is referred to as the Report Server. Installing the Report Server is a separate step within the overall SiteMinder installation process. Installing the Report Server separately from SiteMinder-specific components lets other CA products share the same Business Intelligence Services.

The Report Server compiles reports to help you analyze your SiteMinder environment. The purpose of this component is to create the following types of reports:

- Audit
- Policy analysis

The Report Server communicates with the following components to compile reports:

- The Central Management Server (CMS) database (report database)
- An Administrative UI
- A Policy Server
- A SiteMinder audit database

SiteMinder Audit Database

(Optional) By default, the Policy Server writes audit events to a text file, which is known as the Policy Server log. The purpose of audit logs is to track information about all user activity, including:

- All successful authentications
- All failed authentications
- All successful authorization attempts
- All failed authorization attempts
- All administrative login attempts
- All administrative actions, such as changes to administrator passwords, the creation of policy store objects, and changes to policy store objects

However, you can configure a stand-alone SiteMinder audit database (audit database). When deciding where to store audit events, consider that:

- The Report Server requires a connection to an audit database to create audit-based reports. The Report Server cannot create audit-based reports from a Policy Server log written to a text file.
- Storing audit logs to a database is more secure than logging the information to a text file.
- If supported, a policy store can also function as an audit database.

Note: For more information about configuring an audit database, see the documentation roadmap.

Agents

(Required) A SiteMinder Agent can reside on a web server, a J2EE application server, an Enterprise Resource Planning (ERP) system, or custom application. An Agent acts as the Policy Enforcement Point (PEP), intercepting user requests for resources and communicating with a Policy Server to determine if the resource is protected.

If the resource is not protected, the Agent allows access. If the resource is protected, the Agent continues to communicate with the Policy Server to authenticate and authorize users. A successful authorization prompts the Agent to let the resource request proceed to the server. Agents also:

- Provide information to web applications to enable content personalization
- Cache information about authenticated users and protected resources to allow quicker access to resources
- Enable single sign-on (SSO)

Administrative User Interfaces Overview

There are two graphical user interfaces (GUIs), which configure specific SiteMinder policy objects, as follows:

- **SiteMinder Administrative UI** (Administrative UI)—The Administrative UI is a web-based administration console that is installed independent of the Policy Server. The Administrative UI is the tool for configuring most tasks related to access control, such as authentication and authorization policies, Enterprise Policy Management (EPM), reporting and policy analysis.

Use the Administrative UI to view, modify, and delete all Policy Server objects, except objects related to Federation Security Services. All federation-related configuration tasks can be managed using the FSS Administrative UI.

- **SiteMinder Federation Security Services Administrative UI** (FSS Administrative UI)—The FSS Administrative UI is an applet-based application that is installed with the Policy Server. Federation Security Services components consist of the affiliates (consumers, service providers, resource partners) and SAML authentication schemes that you configure to support federated communication between two partners. Use the FSS Administrative UI to configure only SiteMinder Federation Security Services.

The intent of the FSS Administrative UI is to let you manage SiteMinder Federation Security Services. If you are familiar with previous versions of the SiteMinder Policy Server User Interface, you will notice that all SiteMinder objects appear in the FSS Administrative UI. The only objects that do not appear are objects related to Enterprise Policy Management (EPM) and reports. You can use the FSS Administrative UI to manage the SiteMinder objects. If you need information while using the FSS Administrative UI, consult the FSS Administrative UI online help system.

Note: Although installed with the Policy Server, the FSS Administrative UI must be registered with the Policy Server before it can be used. Registering the FSS Administrative UI requires the use of the Administrative UI. Therefore, install and configure the Administrative UI before registering the FSS Administrative UI. If your organization is not federating with a partner, you can safely leave the Federation Security Services on the Policy Server host system without registering it.

SiteMinder Documentation

You can find complete information about SiteMinder by installing the SiteMinder bookshelf. The SiteMinder bookshelf lets you:

- Use a single console to view all documents published for SiteMinder.
- Use a single alphabetical index to find a topic in any document.
- Search all documents for one or more words.

SiteMinder product documentation is installed separately. We recommend that you install the documentation before beginning the installation process.

Install the Bookshelf on Windows

Install the SiteMinder bookshelf using the installation media on the Technical Support site.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

To install the bookshelf on Windows

1. Exit all applications that are running.
2. Double-click the installation executable.
The installation wizard starts.
3. Enter the required information and review the installation settings.
4. Click Install.

The installer begins the installation.

5. Click Done.

The bookshelf is installed.

More information:

[Locate the Bookshelf](#) (see page 456)

Install the Bookshelf on UNIX

Install the SiteMinder bookshelf using the installation media on the Technical Support site.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

To install the bookshelf using a wizard

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

```
.installation_media gui
```

installation_media

Specifies the name of the SiteMinder bookshelf installation executable.

The installer starts.

4. Enter the required information and review the installation summary.
5. Click Install.

The installer begins the installation.

6. Click Done.

The bookshelf is installed.

To install the bookshelf using a UNIX console

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

```
.installation_media -i console
```

installation_media

Specifies the name of the SiteMinder bookshelf installation executable.

The installer starts.

4. Enter the required information and review the installation summary dialog.
5. Press Enter.

The installer installs the bookshelf.

More information:

[Locate the Bookshelf](#) (see page 456)

Use the SiteMinder Bookshelf

To use the bookshelf

1. Navigate to *bookshelf_home*\CA\ca_documents.

bookshelf_home

Specifies the bookshelf installation path.

Note: This folder contains a readme.txt file that details the location of the release notes, the PDF versions of the guides, the Javadoc (HTML) files, and the Perl POD files.

2. Open the ca-siteminder-bookshelf folder.
3. Open the CA-SiteMinder-*version*-BookShelf folder.

version

Specifies the current SiteMinder version.

4. Use one of the following methods to open the bookshelf:
 - If the bookshelf is on the local system and you are using Internet Explorer:
 - Double-click Bookshelf.hta
 - or
 - Click Start, Programs, SiteMinder documentation
 - If you are using Mozilla Firefox, double-click Bookshelf.html
 - If the bookshelf is on a remote system, double-click Bookshelf.htmlThe bookshelf opens.
5. Add the bookshelf to your Internet Explorer favorites or create a Mozilla Firefox bookmark to return to the bookshelf.

Pre-Installation Checklist

You may want to print the following to use as a checklist to help ensure you meet all of the necessary system and software requirements before installing a Policy Server, an Administrative UI, and a Report Server.

- ☐ Install the SiteMinder [bookshelf](#) (see page 20).
- ☐ Confirm that the Windows or UNIX system that is to host the Policy Server meets the minimum [system requirements](#) (see page 25).
- ☐ Confirm that the Windows or UNIX system that is to host the Administrative UI meets the minimum [system requirements](#) (see page 27).

- ☐ Confirm that the Windows or UNIX system that is to host the Report Server meets the minimum [system requirements](#) (see page 29).
- ☐ Confirm that your environment includes a database instance that meets the [report database requirements](#) (see page 30).

Chapter 2: Policy Server Installation Requirements

This section contains the following topics:

[Policy Server System Requirements](#) (see page 25)

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 to which you are installing the Policy Server must meet the following minimum system requirements:

- **CPU**—Intel Pentium III or better.
- **Memory**—512 MB system RAM.
- **Available disk space:**
 - 270 MB free disk space in the install location.
 - 180 MB of free space in the system's temporary file location.

Note: These requirements are based on a medium size policy database of approximately 1,000 policies.
- **JRE**—The required JRE version is installed on the system to which you are installing the Policy Server.
- **LDAP directory server or relational database**—Be sure that LDAP directory server or relational database you plan on using as a policy store is supported.
- **Web server**—A supported Web server.

Note: For a list of supported CA and third-party components, refer to the SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

UNIX

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

- **Memory**—512 MB RAM.
- **Available disk space:**
 - 300 MB free disk space.
 - 200 MB free disk space in /tmp.

Note: Typically, 10 MB or less free disk space in /tmp is required for the daily operation of the Policy Server. The Policy Server creates files and named pipes under /tmp. The path to which these files and pipes are created cannot be changed.
- **JRE**—The required JRE version is installed on the system to which you are installing the Policy Server.
- **LDAP directory server or relational database**—Be sure that the LDAP directory server or relational database you plan on using as a policy store is supported.
- **Web server**—A supported Web server.

Note: For a list of supported CA and third-party components, refer to the SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Chapter 3: Administrative UI Installation Requirements

This section contains the following topics:

[System Requirements](#) (see page 27)

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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Administrative UI Installation Options](#) (see page 262)

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Windows

The Windows system to which you are installing the Administrative UI must meet the following minimum system requirements:

- **CPU**—Single or dual-processor, Intel Pentium III (or compatible), 700-900 MHz.
- **Memory**—512 MB system RAM. We recommend 1 GB.
- **Available disk space**—540 MB.
- **Temp directory space**—450 MB.
- **Screen resolution**—1024 x 768 or higher resolution with 256 colors or better to view the Administrative UI properly.

UNIX

The UNIX system to which you are installing the Administrative UI must meet the following minimum system requirements:

- **CPU**
 - Solaris—Sparc Workstation 440 MHz.
 - Red Hat Linux—Single or dual-processor, Intel Pentium III (or compatible), 700-900 MHz.
- **Memory**—512 MB system RAM. We recommend 1 GB.
- **Available disk space**—540 MB.
- **Temp directory space**—450 MB.
- **Screen resolution**—1024 x 768 or higher resolution with 256 colors or better to view the Administrative UI properly.

Chapter 4: Report Server Installation Requirements

This section contains the following topics:

[System Requirements](#) (see page 29)

[Report Database Requirements](#) (see page 30)

[Connectivity Requirements](#) (see page 31)

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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Windows

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

- **CPU**—Single or dual-processor, Intel Pentium III (or compatible), 2.5 GHz.
- **Memory**—2 GB RAM.
- **Available disk space**—10 GB.

Note: This requirement is the space required to install the Report Server. This requirement does not account for the disk space 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**—Sparc Workstation 2.5 GHz.
- **Memory**—2 GB RAM.
- **Available disk space**—10 GB.

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

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 SiteMinder does not. For a list of supported database types and versions, see the SiteMinder r12.0 SP2 Platform Support Matrix.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

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 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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Chapter 5: Installing the Policy Server on Windows Systems

This section contains the following topics:

[Installation Road Map](#) (see page 34)

[Before You Install the Policy Server](#) (see page 35)

[How to Install the Policy Server](#) (see page 35)

[Unattended Policy Server Installation](#) (see page 47)

[Policy Server Configuration Wizard](#) (see page 47)

[Reinstall the Policy Server](#) (see page 53)

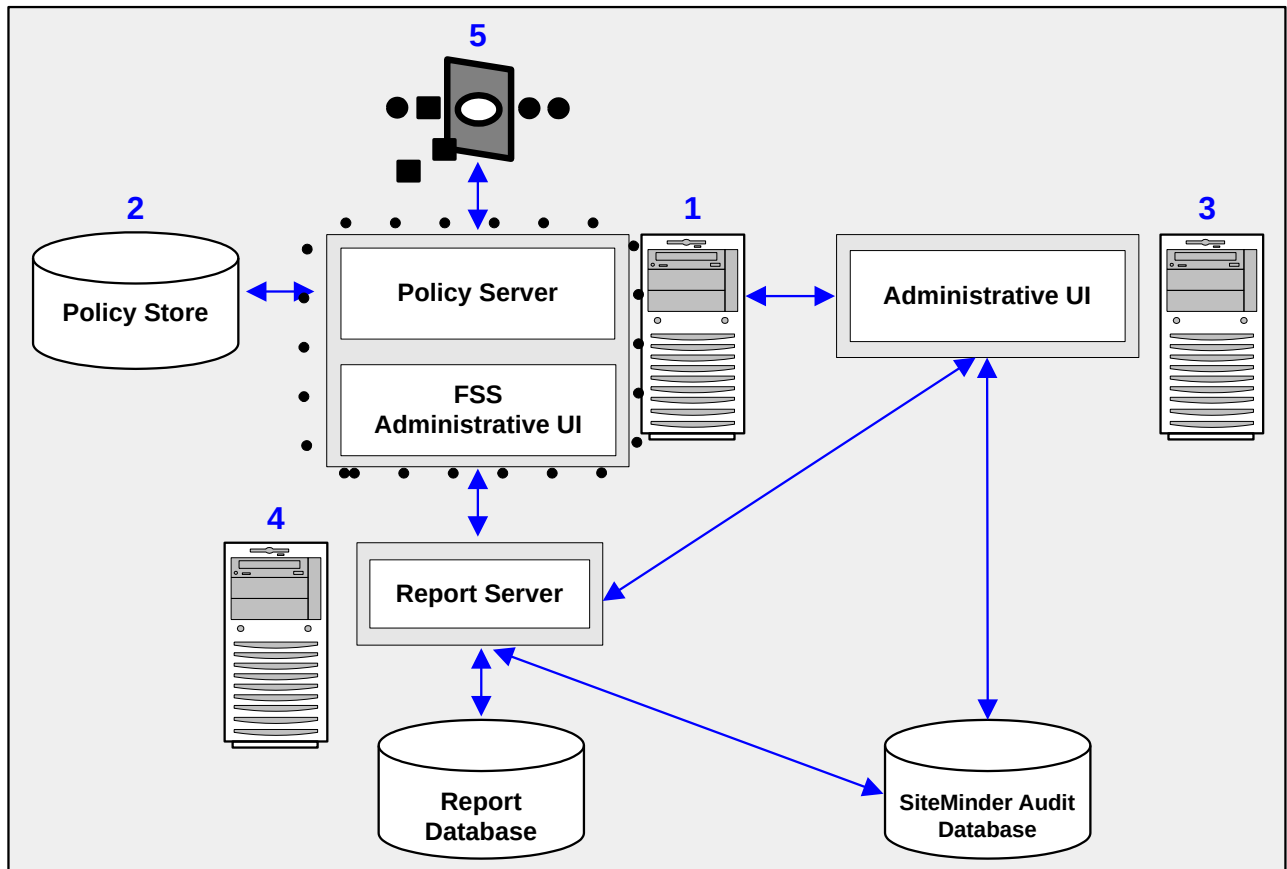
[Uninstall the Policy Server and Documentation](#) (see page 54)

[Scripting Interface](#) (see page 57)

Installation Road Map

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

- Confirm that the Policy Server host system meets the minimum system requirements. We recommend doing so before installing the Policy Server.
- The components surrounded by the dotted line are the Policy Server and the FSS Administrative UI, which you install now.



More information:

[Policy Server](#) (see page 16)

[Administrative User Interfaces Overview](#) (see page 20)

Before You Install the Policy Server

Be aware of the following before installing the Policy Server:

- **Administrator privileges**—You must be logged into a Windows account with local administrator privileges to install the Policy Server.
- **System path length**—The Policy Server installation fails if the system path length exceeds 1024 characters, including or excluding the SiteMinder added directories.

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

- **Web Server instance**—Be sure that the Sun Java System or IIS Web server instance is stopped. Stopping the Web server lets the Policy Server installer configure the FSS Administrative UI to operate with the selected Web server instance.
- **Environment variables**—The Policy Server and documentation installations each modify environment variables.
- **IBM Directory Server only**—Using an IBM Directory Servers in your SiteMinder environment requires that you edit the V3.matchingrules file by adding the following line:

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

The Directory store will not be configured correctly and the necessary SiteMinder objects for the policy store cannot be created if the V3.matchingrules file does not contain the change.

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. Verify the Policy Server installation.
7. (Optional) Enable SNMP event trapping.

8. (Optional) Configure the policy store.

Note: A SiteMinder environment must contain at least one policy store. This step is optional only if you plan on using the Policy Server installer to automatically configure ADAM or a Sun Java System Directory Server as the policy store. Otherwise, you must configure a policy store in a supported LDAP directory server or relational database.

More information:

[Reinstall the Policy Server](#) (see page 53)

Policy Server Component Considerations

The Policy Server installer can configure the following components. Review the following before running the Policy Server installer:

- **FSS Administrative UI**—The FSS Administrative UI is installed with the Policy Server and is for managing Federation Security Services. If your organization is not federating with a partner, use of the FSS Administrative UI is not required. Although part of the core Policy Server installation, the FSS Administrative UI must be registered with the Policy Server before it can be used. Registering the FSS Administrative UI requires the use of the Administrative UI. Therefore, you install and configure the Administrative UI before registering the FSS Administrative UI.
- **Web Server**—A supported web server is required to configure the FSS Administrative UI. The Policy Server installer configures the FSS Administrative UI with the selected web server.
- **OneView Monitor**—The OneView Monitor enables the monitoring of SiteMinder components.

Note: To use the OneView Monitor, you must have the supported Java SDK and ServletExec ISAPI Windows/IIS installed.
- **SNMP**—Be sure that you have an SNMP Service (Master OS Agent) installed with your Windows operating system before installing the Policy Server.

Note: More information about installing the SNMP service exists in the Windows online help system.
- **Policy Store**—The policy store is the repository for Policy Server objects and policy information.

- **SiteMinder Key Database (smkeydatabase)**—The key database is a key store used for signing, verification, encryption, and decryption between a SiteMinder consuming authority and a SiteMinder producing authority. The key database is required only if you:

- Plan on using features related to Federation Security Services.
- Plan on configuring a SiteMinder Information Card Authentication Scheme, for example, for the support of Microsoft CardSpace.

If you decide to configure the key database during installation, you are prompted to install the default certificate authority (CA) certificates. You can add additional certificates and private keys to a key database after installation.

Note: For more information about the key database and how to add additional certificates and private keys, see the *Federation Security Services Guide*.

- **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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Policy Store Considerations

Consider the following 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 directory servers as a policy store:

- Microsoft Active Directory in Application Mode (ADAM)
- Microsoft Active Directory Lightweight Directory Services (AD LDS)

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

- Sun Java Directory System Server (formerly Sun ONE/iPlanet)

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.

- 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 guide.

More information:

[ADAM/AD LDS Prerequisites](#) (see page 133)

[Configuring LDAP Directory Servers as a Policy or Key Store](#) (see page 95)

[Configuring SiteMinder Data in a Relational Database](#) (see page 147)

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 used to accredit cryptographic modules that meet the Advanced Encryption Standard (AES). The libraries provide a FIPS mode of operation when a 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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

- **FIPS-compatibility mode**—The default FIPS mode of operation during installation is FIPS-compatibility mode. In FIPS-compatibility mode, the environment uses existing SiteMinder algorithms to encrypt sensitive data and is compatible with previous versions 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 r12.0 SP2 environment running in FIPS-compatibility mode to FIPS-only mode.

In FIPS-migration mode, the r12.0 SP2 Policy Server continues to use existing SiteMinder encryption algorithms as you migrate the r12.0 SP2 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 r12.0 SP2 and is configured to use only FIPS-compliant algorithms.

Important! An r12.0 SP2 environment that is running in FIPS-only mode cannot operate with, or be backward compatible to, earlier versions of SiteMinder. This includes 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. Re-link all such software with the r12.0 SP2 versions of the respective SDKs to achieve the required support for Full FIPS mode.

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

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

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.

- **JRE location** - Identify the folder in which the installer can locate the supported JRE and ensure that the JAVA_HOME system variable is set to the correct location. The installer cannot locate the JRE if the JAVA_HOME system variable is incorrectly set.
- **Policy Server installation location** - Determine where the installer should install the Policy Server.

Default: C:\Program Files\CA

- **Encryption key value** - Determine the encryption key value. An *encryption key* is a case-sensitive, alphanumeric key that secures data sent between the Policy Server and the policy store. All Policy Servers that share a policy store must be configured using the same encryption key. For stronger protection, define a long encryption key.

Limits: 6 to 24 characters.

More information:

[Required Information Worksheet](#) (see page 379)

SiteMinder Key Database Information

You only have to gather SiteMinder key database (smkeydatabase) information if you:

- Plan on using features related to Federation Security Services.
- Plan on configuring a SiteMinder Information Card Authentication scheme, for example, for the support of Microsoft CardSpace.

The Policy Server installer requires that you enter a password when configuring the smkeydatabase. The smkeydatabase password is used to encrypt the key and certificate data in the key database. You can use the SiteMinder Key Database Information Worksheet to record your value.

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.

More information:

[OneView Monitor Information Worksheet](#) (see page 379)

ADAM and AD LDS Server Information

If you are configuring Microsoft ADAM or AD LDS to function as a policy store gather the following required information:

- **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, 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 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.

- **SiteMinder super user password**—The default SiteMinder super user account (siteminder) has maximum permissions. Determine the password for the default super user account.

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 super user for day-to-day operations. Rather, use the default super user to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Microsoft ADAM/AD LDS Information Worksheet](#) (see page 383)

Sun Java System Directory Server Information

If you are configuring Sun Java™ System Directory Server to function as a policy store, use the Sun Java System Directory Server worksheet to gather the following required information:

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

Default: 389

- **Root DN**—Identify the root DN of the Sun Java System 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 Sun Java System Directory Server administrator.

- **Alternate LDAP administrator**—By default, 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 SiteMinder in this way.

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

- **SiteMinder Super User password**—The default SiteMinder super user account (siteminder) has maximum permissions. Determine the password for the default super user account.

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 super user for day-to-day operations. Rather, use the default super user to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Sun Java System Directory Server Information Worksheet](#) (see page 380)

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 based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

To run the Policy Server installer

1. Be sure that the system meets the windows requirements.
2. Exit all applications that are running.
3. 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 when running the installer:
 - You are prompted to select a FIPS mode of operation. The use of FIPS-compliant algorithms in your environment is optional. If your organization does not require this type of encryption, install the Policy Server in FIPS-compatibility mode.
 - When prompted to select the components you want configured:
 - Clear the Policy Store check box if you plan on using a relational database or a directory server other than ADAM, AD LDS, or Sun Java System Directory Server as a policy store. You manually configure any other supported relational database or directory server after installing the Policy Server.
 - If you plan on using features related to Federation Security Services, be sure that the Web Server(s) and Create SM Key Database/Change SM Key Database Password check boxes are selected.

Note: Configuring a web server installs the FSS Administrative UI. If you do not plan on using Federation Security Services, the FSS Administrative UI is not required.

- If you plan on configuring the SiteMinder Information Card Authentication Scheme, for example, for the support of Microsoft CardSpace, select the Create SM Key Database/Change SM Key Database Password check box.

Note: If you decide to create a SiteMinder key database, you are prompted to install the default CA certificates. Leave the Import default CA certificates check box selected and install these certificates. You can add additional certificates and private keys to a key database after installation.

- If you are initializing a policy store, you are prompted to enter a password for the default SiteMinder user account. The default account name is siteminder.
- If you are using IPv6 addresses, be sure that entries include 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 any selected components are installed and configured.

Note: If you chose to install the FSS Administrative UI, register the FSS Administrative UI with the Policy Server after installing and registering the Administrative UI.

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:

[Locate the Installation Media](#) (see page 456)

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 `XPSCConfig` 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 349)

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 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 Silently Install a Policy Server](#) (see page 413)

Policy Server Configuration Wizard

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

- The FSS Administrative UI
- The OneView Monitor GUI
- SNMP support

- A SiteMinder key database
- An ADAM policy store
- An AD LDS policy store
- A Sun Java Systems Directory Server policy store

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 *SiteMinder Upgrade Guide*.

Important! If you have a Sun Java System web server instance configured for the OneView Monitor GUI or SNMP, do not configure new instances using the Policy Server Configuration wizard. Running the wizard to configure new web server instances can cause the existing configured web server instance to fail.

How to Use the Configuration Wizard

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

1. Review the Policy Store considerations.
2. Gather information for the wizard if you are configuring:
 - The SiteMinder key database (smkeydatabase)
 - The OneView Monitor
 - An ADAM server policy store
 - An AD LDS policy store
 - A Sun Java System Directory Server policy store
3. Run the Policy Server Configuration wizard.

Policy Store Considerations

Consider the following 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 directory servers as a policy store:

- Microsoft Active Directory in Application Mode (ADAM)
- Microsoft Active Directory Lightweight Directory Services (AD LDS)

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

- Sun Java Directory System Server (formerly Sun ONE/iPlanet)

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.

- 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 guide.

More information:

[ADAM/AD LDS Prerequisites](#) (see page 133)

[Configuring LDAP Directory Servers as a Policy or Key Store](#) (see page 95)

[Configuring SiteMinder Data in a Relational Database](#) (see page 147)

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.

SiteMinder Key Database Information

You only have to gather SiteMinder key database (smkeydatabase) information if you:

- Plan on using features related to Federation Security Services.
- Plan on configuring a SiteMinder Information Card Authentication scheme, for example, for the support of Microsoft CardSpace.

The Policy Server installer requires that you enter a password when configuring the smkeydatabase. The smkeydatabase password is used to encrypt the key and certificate data in the key database. You can use the SiteMinder Key Database Information Worksheet to record your value.

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.

More information:

[OneView Monitor Information Worksheet](#) (see page 379)

ADAM and AD LDS Server Information

If you are configuring Microsoft ADAM or AD LDS to function as a policy store gather the following required information:

- **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, 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 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.

- **SiteMinder super user password**—The default SiteMinder super user account (siteminder) has maximum permissions. Determine the password for the default super user account.

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 super user for day-to-day operations. Rather, use the default super user to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Microsoft ADAM/AD LDS Information Worksheet](#) (see page 383)

Sun Java System Directory Server Information

If you are configuring Sun Java™ System Directory Server to function as a policy store, use the Sun Java System Directory Server worksheet to gather the following required information:

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

Default: 389

- **Root DN**—Identify the root DN of the Sun Java System 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 Sun Java System Directory Server administrator.

- **Alternate LDAP administrator**—By default, 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 SiteMinder in this way.

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

- **SiteMinder Super User password**—The default SiteMinder super user account (siteminder) has maximum permissions. Determine the password for the default super user account.

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 super user for day-to-day operations. Rather, use the default super user to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Sun Java System Directory Server Information Worksheet](#) (see page 380)

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.

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 46)

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.

More information:

[How to Install the Policy Server](#) (see page 35)

Uninstall the Policy Server and Documentation

You uninstall the Policy Server and documentation when it is no longer required on the system. The following sections detail how to uninstall the Policy Server and the SiteMinder documentation.

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.

Uninstall the Policy Server

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

To uninstall the Policy Server

1. Open the Windows Control Panel and double-click Add/Remove Programs.
A list of installed programs appears.
2. Select SiteMinder Policy Server, and click Add/Remove.
3. Follow the instructions in the uninstallation wizard.

Note: If the system displays a remove shared file message, click No to All.

4. If requested, reboot the system.

The Policy Server is uninstalled.

Remove Leftover Items

Manually remove the following folders, registry settings, and virtual directories after uninstalling the Policy Server to keep the system as clean as possible.

- **Windows system**

- *Siteminder_home\bin*
- *Siteminder_home\install_config_info*

Note: If you are planning on reinstalling the Policy Server, ensure these folders are removed.

- **AdventNet software registry entry** - Delete the AdventNet software registry entry only if the software was not on the system prior to installing the Policy Server. You can find the registry entry under Registry entries under HKEY_LOCAL_MACHINE\SOFTWARE\Advent,Inc.
- **IIS virtual directories** - Delete the following SiteMinder virtual directories using the IIS Microsoft Management Console
 - 'SiteMinder'
 - 'SiteMinderCgi'
 - 'SiteMinderMonitor'
 - 'netegrity_docs'

Remove Leftover Services

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

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

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

The leftover services are removed.

Uninstall the Documentation

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

To uninstall the documentation

1. Open the Windows Control Panel, and double-click Add/Remove Programs.
A list of installed programs appears.
2. Select CA SiteMinder Documentation, and click Add/Remove.
3. Follow the instructions in the uninstallation wizard.

Note: If the system displays a remove shared file message, click No to All.

The documentation is removed from the system.

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 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 6: Installing the Policy Server on UNIX Systems

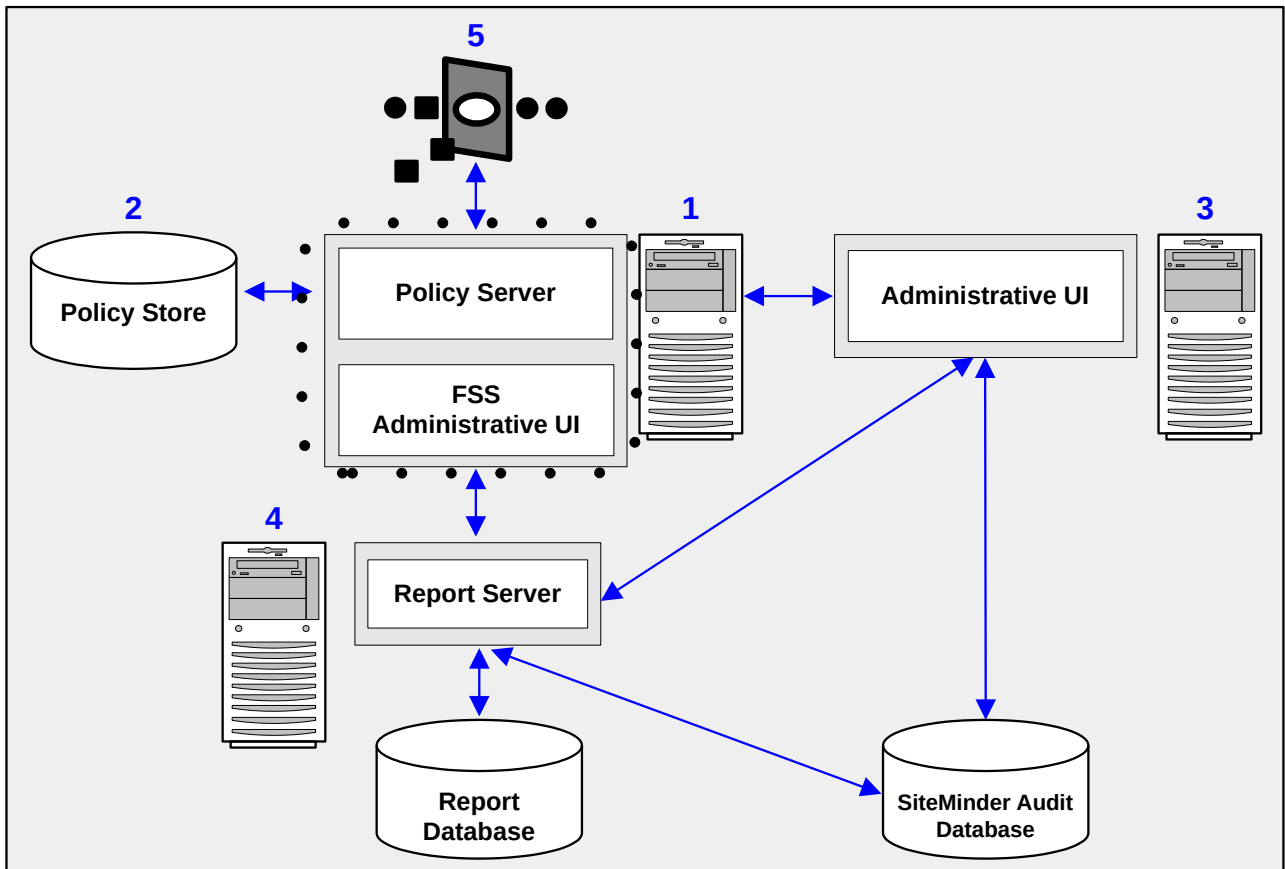
This section contains the following topics:

- [Installation Road Map](#) (see page 60)
- [Solaris 10 Zone Support](#) (see page 61)
- [Solaris and HP-UX Patches](#) (see page 62)
- [How to Prepare for the Policy Server Installation](#) (see page 63)
- [Before You Install the Policy Server](#) (see page 65)
- [How to Install the Policy Server](#) (see page 66)
- [Configure Auto Startup](#) (see page 79)
- [Unattended Policy Server Installation](#) (see page 80)
- [Policy Server Configuration Wizard](#) (see page 80)
- [Uninstall the Policy Server and Documentation](#) (see page 88)
- [Scripting Interface](#) (see page 93)

Installation Road Map

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

- Confirm that the Policy Server host system meets the minimum system requirements. We recommend doing so before installing the Policy Server.
- The components surrounded by the dotted line are the Policy Server and the FSS Administrative UI, which you install now.



More information:

[Policy Server](#) (see page 16)

[Administrative User Interfaces Overview](#) (see page 20)

Solaris 10 Zone Support

A SiteMinder Policy Server is supported in:

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

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

Global Zone Support

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

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

Example: Global zone support

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.

Solaris and HP-UX Patches

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

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. Create a New UNIX Account.
2. Modify the UNIX System Parameters.
3. Unset the Localization Variables.
4. Unset the LANG Environment Variable.

Create a New UNIX Account

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

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

After the Policy Server installation is complete, run the Policy Server Configuration Wizard (located in `siteminder_installation\install_config_info\ca-ps-config.bin`) as root to configure the FSS Administrative UI or the OneView Monitor GUI.

Modify the UNIX System Parameters

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

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

```
$ ulimit -a
time(seconds)                unlimited
file(blocks)                  unlimited
data(kbytes)                   2097148
```

stack(kbytes)	8192
coredump(blocks)	unlimited
nofiles(descriptors)	256
vmemory(kbytes)	unlimited

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

You must increase this parameter value for proper Policy Server operation under load. You can change this value by running the `ulimit -n` command. For example, to set `nofiles` to 1024, place the `ulimit -n 1024` command in the `.profile` or `smprofile.ksh` of the `smuser` account. The Policy Server is bound by the `nofiles` parameter within `smuser`'s `ulimit` for the number of connections to it.

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

Unset Localization Variables

The `LC_*` variables are sometimes set by default in the `.profile` or `smprofile.ksh` files of the `smuser` account. Use of the `LC_*` environment variables are not permitted and use must unset them before installing the Policy Server.

To unset the `LC_*` environment variables open the `.profile` or `smprofile.ksh` files of the `smuser` account and unset them.

Unset the LANG Environment Variable

The `LANG` environment variable are not permitted and you must unset it before installing the Policy Server.

To unset the variable, add the `unset LANG` command to the `smprofile.ksh` file.

Before You Install the Policy Server

Consider the following before installing the Policy Server:

- **Administrator privileges**—Ensure you have created a new UNIX account and understand which components require root administrator privileges.

Note: More information on the required administrator privileges exists in How to Prepare for the Policy Server Installation.

- **Free space in /tmp**—The Policy Server install requires 200 MB of free space in /tmp.
- **System path length**—The Policy Server installation fails if the system path length exceeds 1024 characters, including or excluding the SiteMinder added directories.

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

- **Web Server instance**—Ensure that the Sun Java System Web server instance is stopped before installing the Policy Server.
- **Telnet or other terminal emulation software**—If you plan on installing the Policy Server using Telnet or other terminal emulation software, you should install using a console window. The installer throws a Java exception and exits if you try to run a GUI through a telnet window.
- **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 may cause text in the dialog box to truncate due to unavailable fonts using Exceed. This limitation has no effect on the Policy Server installation or configuration.
- **Environment variables**—The Policy Server and documentation installations each modify environment variables.
- **IBM Directory Server only**—Using an IBM Directory Servers in your SiteMinder environment requires that you edit the V3.matchingrules file by adding the following line:

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

The Directory store will not be configured correctly and the necessary SiteMinder policy store objects cannot be created if the V3.matchingrules file does not contain the change.

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. Verify the Policy Server installation.
7. (Optional) Restart the SNMP daemon.
8. (Optional) Configure the policy store.

Note: A SiteMinder environment must contain at least one policy store. This step is optional only if you plan on using the Policy Server installer to automatically configure an ADAM or Sun One LDAP directory server as the policy store. Otherwise, you must configure a policy store in a supported LDAP directory server or relational database.

Policy Server Component Considerations

The Policy Server installer can configure the following components. Consider the following before running the Policy Server installer:

- **FSS Administrative UI**—The FSS Administrative UI is installed with the Policy Server and is for managing Federation Security Services. If your organization is not federating with a partner, use of the FSS Administrative UI is not required. Although part of the core Policy Server installation, the Federation Security Services must be registered with the Policy Server before it can be used. Registering the FSS Administrative UI requires the use of the Administrative UI. Therefore, install and configure the Administrative UI before registering the FSS Administrative UI.
- **Web Server**—A supported web server is required to configure the FSS Administrative UI. The Policy Server installer configures the FSS Administrative UI with the selected web server.
- **OneView Monitor**—The OneView Monitor enables the monitoring of SiteMinder components.

Note: To use the OneView Monitor, you must have the supported Java SDK and ServletExec ISAPI Windows/IIS installed.

- **SNMP**—You must have the password of the root user and have a native SunSolstice Master Agent to enable SNMP support.

- **Policy Store**—The policy store is the repository for Policy Server objects and policy information.
- **SiteMinder Key Database (smkeydatabase)**—The key database is a key store used for signing, verification, encryption, and decryption between a SiteMinder consuming authority and a SiteMinder producing authority. The key database is required only if you:
 - Plan on using features related to Federation Security Services.
 - Plan on configuring a SiteMinder Information Card Authentication Scheme, for example, for the support of Microsoft CardSpace.

If you decided to configure the key database during installation, you are prompted to install the default certificate authority (CA) certificates. You can add additional certificates and private keys to a key database after installation.

Note: For more information about the key database and how to add additional certificates and private keys, see the *Federation Security Services Guide*.

- **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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Policy Store Considerations

Consider the following 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 directory servers as a policy store:
 - Microsoft Active Directory in Application Mode (ADAM)
 - Microsoft Active Directory Lightweight Directory Services (AD LDS)
Note: Be sure that you have met the prerequisites for configuring ADAM or AD LDS as a policy store.
 - Sun Java Directory System Server (formerly Sun ONE/iPlanet)
- **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.
- 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 guide.

More information:

[ADAM/AD LDS Prerequisites](#) (see page 133)

[Configuring LDAP Directory Servers as a Policy or Key Store](#) (see page 95)

[Configuring SiteMinder Data in a Relational Database](#) (see page 147)

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 used to accredit cryptographic modules that meet the Advanced Encryption Standard (AES). The libraries provide a FIPS mode of operation when a 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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

- **FIPS-compatibility mode**—The default FIPS mode of operation during installation is FIPS-compatibility mode. In FIPS-compatibility mode, the environment uses existing SiteMinder algorithms to encrypt sensitive data and is compatible with previous versions 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 r12.0 SP2 environment running in FIPS-compatibility mode to FIPS-only mode.

In FIPS-migration mode, the r12.0 SP2 Policy Server continues to use existing SiteMinder encryption algorithms as you migrate the r12.0 SP2 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 r12.0 SP2 and is configured to use only FIPS-compliant algorithms.

Important! An r12.0 SP2 environment that is running in FIPS-only mode cannot operate with, or be backward compatible to, earlier versions of SiteMinder. This includes 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. Re-link all such software with the r12.0 SP2 versions of the respective SDKs to achieve the required support for Full FIPS mode.

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

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

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.

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

Limits: 6 to 24 characters.

More information:

[Required Information Worksheet](#) (see page 379)

SiteMinder Key Database Information

You only have to gather SiteMinder key database (smkeydatabase) information if you:

- Plan on using features related to Federation Security Services.
- Plan on configuring a SiteMinder Information Card Authentication scheme, for example, for the support of Microsoft CardSpace.

The Policy Server installer requires that you enter a password when configuring the smkeydatabase. The smkeydatabase password is used to encrypt the key and certificate data in the key database. You can use the SiteMinder Key Database Information Worksheet to record your value.

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.

More information:

[OneView Monitor Information Worksheet](#) (see page 379)

ADAM and AD LDS Server Information

If you are configuring Microsoft ADAM or AD LDS to function as a policy store gather the following required information:

- **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, 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 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.

- **SiteMinder super user password**—The default SiteMinder super user account (siteminder) has maximum permissions. Determine the password for the default super user account.

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 super user for day-to-day operations. Rather, use the default super user to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Microsoft ADAM/AD LDS Information Worksheet](#) (see page 383)

Sun Java System Directory Server Information

If you are configuring Sun Java™ System Directory Server to function as a policy store, use the Sun Java System Directory Server worksheet to gather the following required information:

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

Default: 389

- **Root DN**—Identify the root DN of the Sun Java System 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 Sun Java System Directory Server administrator.

- **Alternate LDAP administrator**—By default, 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 SiteMinder in this way.

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

- **SiteMinder Super User password**—The default SiteMinder super user account (siteminder) has maximum permissions. Determine the password for the default super user account.

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 super user for day-to-day operations. Rather, use the default super user to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Sun Java System Directory Server Information Worksheet](#) (see page 380)

Install the Policy Server in GUI Mode

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

- Depending on your permissions, you may need to add executable permissions to the install file by running 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.

To install the Policy Server

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

```
.installation_media gui
```

installation_media

Specifies the Policy Server installer executable.

The installer starts.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

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

Consider the following when running the installer:

- The installer prompts you to select a FIPS mode of operation. The use of FIPS-compliant algorithms in your environment is optional. If your organization does not require this type of encryption, install the Policy Server in FIPS-compatibility mode.
- The installer prompts you to select components you want to configure:
 - If you plan on using a relational database or a directory server other than ADAM, AD LDS, or Sun Java System Directory Server as a policy store, clear the Policy Store check box. You manually configure a relational database or any other supported directory server after installing the Policy Server.

- If you plan on using features related to Federation Security Services, be sure that the Web Server(s) and Create SM Key Database/Change SM Key Database Password check boxes are selected. Configuring a web server installs the FSS Administrative UI. If you do not plan on using Federation Security Services, you do not require the FSS Administrative UI.

Note: If you are installing the Policy Server for the first-time on this system, do not configure a web server or the OneView Monitor GUI. You are installing the Policy Server using the smuser UNIX account. The installer modifies the web server configuration files, for which the smuser account does not have the appropriate root privileges. When the Policy Server installation is complete, run the Policy Server Configuration Wizard as root to configure the web server for the FSS Administrative UI or the OneView Monitor GUI.

- If you plan on configuring the SiteMinder Information Card Authentication Scheme, be sure that the Create SM Key Database/Change SM Key Database Password check box is selected. For example, you can use the SiteMinder Information Card Authentication Scheme for the support of Microsoft CardSpace.

Note: If you decide to create a key database, you are prompted to install the default CA certificates. Leave the Import default CA certificates selected and install these certificates.

- If you are initializing a policy store, you are prompted to enter a password for the default SiteMinder user account. The default account name is siteminder.
- If you are using IPv6 addresses, be sure that entries include 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 any selected components are installed and configured.

Note: The installation can take several minutes.

6. Click Done.

The installer closes.

Note: If you chose to install the FSS Administrative UI, register the FSS Administrative UI with the Policy Server after installing and registering the Administrative UI. For more information about registering the FSS Administrative UI, see Registering the Federation Security Services UI.

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:

[Locate the Installation Media](#) (see page 456)

[Troubleshoot the Policy Server Installation](#) (see page 78)

Install the Policy Server in Console Mode

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

- Depending on your permissions, you may need to add executable permissions to the install file by running 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.

To install the Policy Server

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

```
.installation_media -i console
```

installation_media

Specifies the Policy Server installer executable.

The installer starts.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

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

Consider the following when entering information:

- The installer prompts you to select a FIPS mode of operation. The use of FIPS-compliant algorithms in your environment is optional. If your organization does not require this type of encryption, install the Policy Server in FIPS-compatibility mode.
- The installer prompts you to select components you want to configure. Enter the numbers separated by commas (,). To select none of the features, enter only a comma.
 - If you plan on using a relational database or a directory server other than ADAM, AD LDS, or Sun Java Directory System Directory Server as a policy store, do not select Policy Store. You manually configure a relational database or any other supported directory server after installing the Policy Server.
 - If you plan on using features related to Federation Security Services, be sure to select Web Server(s) and Create SM Key Database/Change SM Key Database Password. Configuring a web server installs the FSS Administrative UI. If you do not plan on using Federation Security Services, you do not require the FSS Administrative UI.

Note: If you are installing the Policy Server for the first-time on this system, do not configure a web server or the OneView Monitor GUI. You are installing the Policy Server using the smuser UNIX account. The installer modifies the web server configuration files, for which the smuser account does not have the appropriate root privileges. When the Policy Server installation is complete, run the Policy Server Configuration Wizard as root to configure the web server for the FSS Administrative UI or the OneView Monitor GUI.

- If you plan on configuring the SiteMinder Information Card Authentication Scheme, be sure that Create SM Key Database/Change SM Key Database Password is selected. For example, you can use the SiteMinder Information Card Authentication Scheme for the support of Microsoft CardSpace.

Note: If you decide to create a key database, you are prompted to install the default certificate authority (CA) certificates. Leave the Import default CA certificates selected and install these certificates.

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

- If you are using IPv6 addresses, be sure that entries include brackets.

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

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

5. Review the installation settings and press Enter.

The Policy Server and selected components are installed and configured.

Note: The installation can take several minutes.

6. Press Enter.

The installer closes.

Note: If you chose to install the FSS Administrative UI, register the FSS Administrative UI with the Policy Server after installing and registering the Administrative UI. For more information about registering the FSS Administrative UI, see Registering the Federation Security Services UI.

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:

[Locate the Installation Media](#) (see page 456)

[Troubleshoot the Policy Server Installation](#) (see page 78)

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 Solaris system is rebooted.

To configure auto startup

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

Example: `/export/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's service when the Solaris system is rebooted.

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

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 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 Silently Install a Policy Server](#) (see page 413)

Policy Server Configuration Wizard

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

- The FSS Administrative UI
- The OneView Monitor GUI
- SNMP support
- A SiteMinder key database

- An ADAM policy store
- An AD LDS policy store
- A Sun Java Systems Directory Server policy store

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 *SiteMinder Upgrade Guide*.

Important! If you have a Sun Java System web server instance configured for the OneView Monitor GUI or SNMP, do not configure new instances using the Policy Server Configuration wizard. Running the wizard to configure new web server instances can cause the existing configured web server instance to fail.

How to use the Configuration Wizard

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

1. Review the Configuration Wizard System Requirements.
2. Review the Policy Store Considerations.
3. Gather Information for the wizard if you are configuring:
 - The SiteMinder key database (smkeydatabase)
 - The OneView Monitor
 - An ADAM server policy store
 - An AD LDS policy store
 - A Sun Java Systems Directory Server policy store
4. Run the Configuration Wizard.

Note: You can run the Configuration wizard in either GUI or console mode.

Configuration Wizard Requirements

Ensure you 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.
Run the wizard as a UNIX user that has sufficient privileges to modify the Web server's configuration files.

Policy Store Considerations

Consider the following 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 directory servers as a policy store:
 - Microsoft Active Directory in Application Mode (ADAM)
 - Microsoft Active Directory Lightweight Directory Services (AD LDS)
Note: Be sure that you have met the prerequisites for configuring ADAM or AD LDS as a policy store.
 - Sun Java Directory System Server (formerly Sun ONE/iPlanet)
- **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.
- 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 guide.

More information:

[ADAM/AD LDS Prerequisites](#) (see page 133)

[Configuring LDAP Directory Servers as a Policy or Key Store](#) (see page 95)

[Configuring SiteMinder Data in a Relational Database](#) (see page 147)

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.

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.

- **JRE location**—Identify the folder in which the installer can locate the supported JRE and ensure that the JRE is set correctly in the PATH variable. The installer cannot locate the JRE if the JRE is not set correctly in the PATH variable.

- **Policy Server Installation location**—Determine where the installer should install the Policy Server.
- **Encryption key value**—Determine the encryption key value. An *encryption key* is a case-sensitive, alphanumeric key that secures data sent between the Policy Server and the policy store. All Policy Servers that share a policy store must be configured using the same encryption key. For stronger protection, define a long encryption key.
Limits: 6 to 24 characters.

More information:

[Required Information Worksheet](#) (see page 379)

SiteMinder Key Database Information

You only have to gather SiteMinder key database (smkeydatabase) information if you:

- Plan on using features related to Federation Security Services.
- Plan on configuring a SiteMinder Information Card Authentication scheme, for example, for the support of Microsoft CardSpace.

The Policy Server installer requires that you enter a password when configuring the smkeydatabase. The smkeydatabase password is used to encrypt the key and certificate data in the key database. You can use the SiteMinder Key Database Information Worksheet to record your value.

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.

More information:

[OneView Monitor Information Worksheet](#) (see page 379)

ADAM and AD LDS Server Information

If you are configuring Microsoft ADAM or AD LDS to function as a policy store gather the following required information:

- **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, 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 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.

- **SiteMinder super user password**—The default SiteMinder super user account (siteminder) has maximum permissions. Determine the password for the default super user account.

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 super user for day-to-day operations. Rather, use the default super user to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Microsoft ADAM/AD LDS Information Worksheet](#) (see page 383)

Sun Java System Directory Server Information

If you are configuring Sun Java™ System Directory Server to function as a policy store, use the Sun Java System Directory Server worksheet to gather the following required information:

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

Default: 389

- **Root DN**—Identify the root DN of the Sun Java System 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 Sun Java System Directory Server administrator.

- **Alternate LDAP administrator**—By default, 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 SiteMinder in this way.

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

- **SiteMinder Super User password**—The default SiteMinder super user account (siteminder) has maximum permissions. Determine the password for the default super user account.

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 super user for day-to-day operations. Rather, use the default super user to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Sun Java System Directory Server Information Worksheet](#) (see page 380)

Run the Configuration Wizard in GUI Mode

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

To run the Configuration wizard in GUI mode

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

```
./ca_ps_env.ksh
```

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

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: When prompted to initialize the LDAP instance do so only 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 components you selected 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 78)

Run the Configuration Wizard in Console Mode

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

To run the Configuration wizard in console mode

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

```
./ca_ps_env.ksh
```

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

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: When prompted to initialize the LDAP instance do so only 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 78)

Backup Versions of Obj.conf and Magnus.conf Files

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

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

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

Uninstall the Policy Server and Documentation

You uninstall the Policy Server and documentation when it is no longer required on the system. The following sections detail how to uninstall the Policy Server and the SiteMinder documentation.

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 SiteMinder Processes.
5. Uninstall the Policy Server.
6. Remove SiteMinder References from IWS.
7. Remove SiteMinder References from ServletExec/AS

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 SiteMinder Processes

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

To stop all SiteMinder processes

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

Uninstall the Policy Server

You uninstall the Policy Server when it is no longer required on the system. Removing the Policy Server involves deleting the SiteMinder installation directory and removing smprofile.ksh from .profile.

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

To uninstall the Policy Server

1. 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.

2. Run the following command:

```
./uninstall
```

The uninstallation program appears.

3. Press Enter.

A status indicator shows the Policy Server is being uninstalled and prompts successful completion.

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

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

5. Enter **\$ rm -rf siteminder** and press Enter.

The SiteMinder installation directory is removed.

6. Open .profile from the HOME directory.

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

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

8. Save. profile.

The Policy Server is uninstalled.

Remove SiteMinder References from IWS

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

To remove 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="/sitemindermonitor" dir="/<siteminder_installation>/monitor"
NameTrans fn="pfx2dir" from="/sitemindercgi" 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_Instal>/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.

SiteMinder references are removed from IWS.

The SiteMinder references no longer appear in IWS.

Remove SiteMinder References from StartServletExec

You manually remove SiteMinder references from StartServletExec after uninstalling the Policy Server.

To remove SiteMinder references from StartServletExec

1. Log into an account that has privileges to access and modify the ServletExec configuration.

Go to the following at the Solaris command line:

```
/usr/NewAtlanta/ServletExecAS/<ServletExec_instance name> folder
```

2. Remove the following lines from the StartServletExec script:

```
CLASSPATH=${NA_ROOT}/lib/ServletExec42.jar:${NA_ROOT}/lib/servlet.jar:${JL}/tools.jar:${NA_ROOT}/lib/jaxp.jar:${NA_ROOT}/lib/crimson.jar:${NA_ROOT}/lib/indi.jar:${NA_ROOT}/se-${SEINSTANCE}/classes
CLASSPATH=${NA_ROOT}/lib/ServletExec42.jar:${NA_ROOT}/lib/servlet.jar:${JL}/tools.jar:${NA_ROOT}/lib/jaxp.jar:${NA_ROOT}/lib/crimson.jar:${NA_ROOT}/lib/indi.jar:${NA_ROOT}/se-${SEINSTANCE}/classes:/export/smuser/siteminder/monitor/smongui.jar:/<siteminder_installation>/lib/smconapi.jar/e<siteminder_installation>/lib/smonclientapi.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_installation>/monitor"
```

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

SiteMinder references no longer exist in the StartServletExec.

You have finished uninstalling the Policy Server.

How to Uninstall the Documentation

Complete the following procedures to uninstall the Policy Server:

1. Set the JRE in the PATH Variable.
2. Uninstall the documentation.

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.

Uninstall the Documentation

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

To uninstall the documentation

1. Change to one of the following directory in a console window:

- If you installed the documentation before the policy server:

```
doc_home
```

- If you installed the documentation after the policy server:

```
policy_server_home/ca_documents/install_config_info
```

doc_home

Specifies the bookshelf installation path.

Default: CA/ca-documents

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

```
./ca-sm-doc-uninstall.sh
```

The documentation is uninstalled.

You have finished uninstalling the documentation.

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 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 7: Configuring LDAP Directory Servers as a Policy or Key Store

This section contains the following topics:

[LDAP Directory Servers as a Policy or Key Store](#) (see page 95)

[Installation Road Map](#) (see page 96)

[Important Considerations](#) (see page 97)

[CA Directory as a Policy Store](#) (see page 97)

[Sun Java System Directory Server as a Policy Store](#) (see page 110)

[Active Directory as a Policy Store](#) (see page 121)

[Microsoft ADAM/AD LDS as a Policy Store](#) (see page 132)

[SiteMinder Key Store Overview](#) (see page 144)

LDAP Directory Servers as a Policy or Key Store

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

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

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

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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Installation Road Map

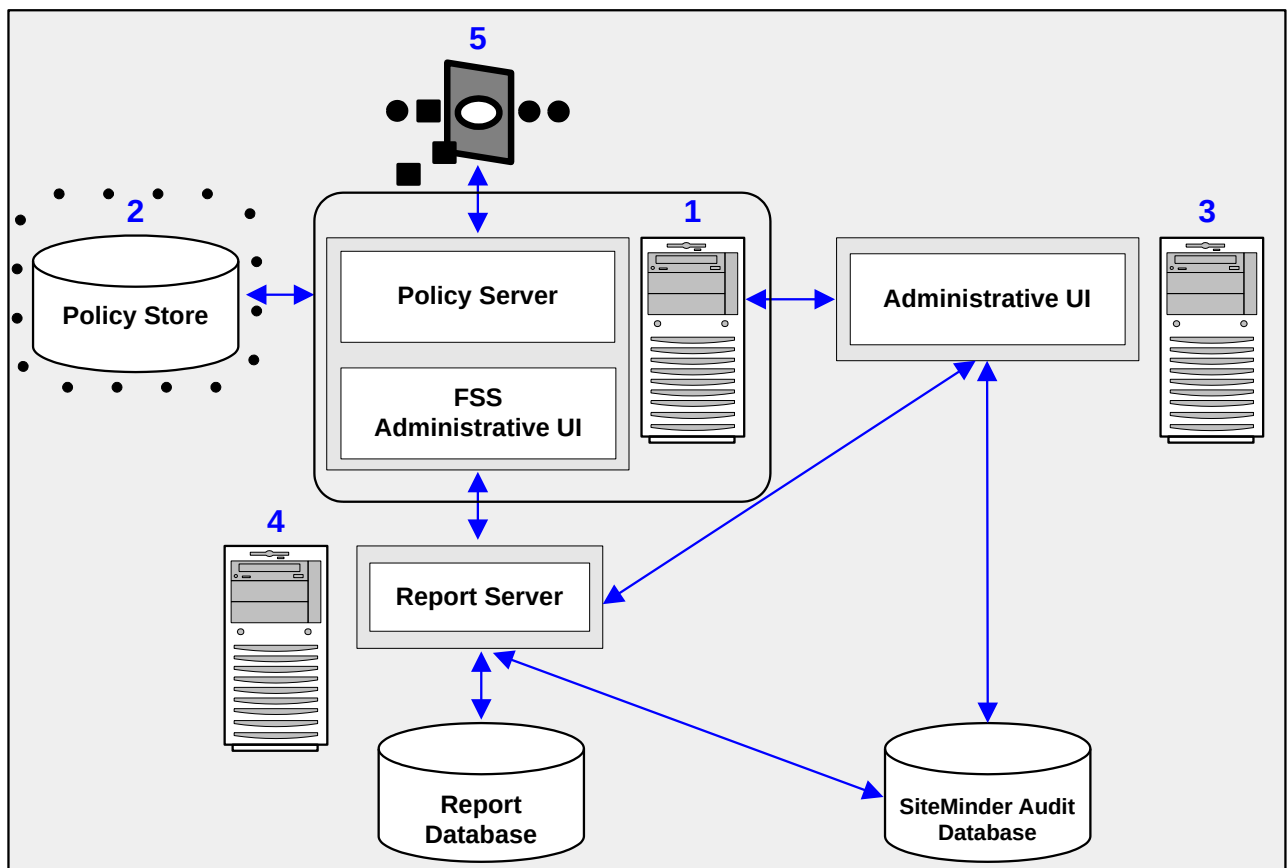
The following diagram illustrates a sample SiteMinder installation and lists the order in which you install and configure each component.

- A solid line surrounds the components that are required before configuring a policy store. They include the following:
 - A Policy Server
 - A non-registered FSS Administrative UI

If a Policy Server is not part of your environment, do not continue with the installation process.

- The component surrounded by a green dotted line is the policy store, which you configure 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.



Note: If you are trying to configure or upgrade a SiteMinder store listed in the SiteMinder Platform Support Matrix and cannot find the procedures in this guide, see the *Directory Configuration Guide*.

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.

CA Directory as a Policy Store

Policy Servers installed on either Windows or UNIX systems can use CA Directory as a policy store. The following sections detail how to configure your directory server as a policy 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 SiteMinder data store. You can print the applicable worksheet and 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 user with the privileges to create, read, modify, and delete objects in the DSA.
- **Administrative password**—Determine the password for the administrative user.

More information:

[CA Directory Information Worksheet](#) (see page 381)

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.
2. Create the policy store schema.
3. Open the DSA.
4. Create the base tree structure for policy store data.
5. Create a super user administrator for the DSA.
6. Point the Policy Server to the policy store.
7. Set the SiteMinder super user password.
8. Verify the CA Directory cache configuration.
9. Import the default policy store objects.
10. Import the policy store data definitions.
11. Prepare for the Administrative UI registration.

Create a DSA for the Policy Store

Create the DSA by running one of the following commands:

■ **r8.1**

```
dxnewdsa DSA_Name Database_Name port c country_code o DSA_Name
```

Note: The command creates the database if it does not exist.

DSA_Name

Specifies the name of the DSA.

Database_Name

Specifies the name of the new or existing database.

Note: The command creates the database if it does not exist.

port

Specifies the port on which the DSA is to listen.

c* *country_code* *o* *DSA_Name

Specifies the DSA prefix.

Example: *c* US *o* psdsa

- **r12.x**

`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 and store SiteMinder objects.

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 *policy_server_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.

2. Copy the following files into the CA Directory *DXHOME*\bin directory.

- `etrust_schema.txt`
- `schema.txt`

Note: The `etrust_schema.txt` file is installed with the Policy Server in *policy_server_home*\xps\db. The `schema.txt` file is installed with the Policy Server in *siteminder_home*\eTrust.

3. Create a new SiteMinder schema file by copying the `default.dwg` schema file and renaming it.

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

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

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

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

5. Edit the DSA's DXI file (*DSA_Name.dxi*) by changing the schema from `default.dwg` to the new SiteMinder schema file.

DSA_Name

Represents the name of the DSA you created using the `dxnewdsa` utility.

Note: the DSA's DXI file is located in *DXHOME*\config\servers.

6. Add the following lines to the end of the DSA's DXI file:

- **r8.1**

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

- **r12.x**

```
# 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.

7. Open the DSA's default DXC file (default.dxc).

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

8. Edit the settings to match the following:

■ **r8.1**

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

■ **r12.x**

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

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

9. Save the DXC file.
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.

To create a view into the CA Directory Server

1. Launch the JXplorer GUI.
2. Select the connect icon.
Connection settings appear.

3. 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.

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

port_number

Specifies the port on which the DSA is listening.

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

Example: *o=psdsa,c=US*

6. 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 SiteMinder called:
PolicySvr4

The base tree structure is created.

Create a Super User Administrator for the DSA

You only have to create a Super User administrator if you do not have an administrator name and password that has the rights to create, delete, or modify the dsa. The Policy Server requires this information to connect to the policy store.

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

Note: Take note of administrator user name and password. You will use this information 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.

To point the Policy Server to the policy store

1. Open the Policy Server Management Console.
2. Click the Data tab.
Database settings appear.
3. Select Policy Store from the Database list.
4. Select LDAP from the Storage list.
5. Configure the following settings in the LDAP Policy Store group box.
 - LDAP IP Address
 - Admin Username
 - Password
 - Confirm Password

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

6. Click Apply.
The policy store settings are saved.
7. Click Test LDAP Connection.
SiteMinder returns a confirmation that the Policy Server can access the policy store.

Set the SiteMinder Super User Password

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

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

To set the super user password

1. Copy the smreg utility to *policy_server_home*\bin.
policy_server_home
Specifies the Policy Server installation path.

2. Run the following command:

```
smreg -su password
```

password

Specifies the password for the default SiteMinder administrator.

Limits:

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

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

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

The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day-to-day operations. Use the default super user to import the default policy store objects, and to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Locate the Installation Media](#) (see page 456)

Verify the CA Directory Cache Configuration

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

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

To verify that the cache is enabled

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

```
telnet DSA_Host DXconsole_Port
```

DSA_Host

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

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

DXConsole_Port

Specifies the port on which the DXconsole is listening.

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

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

The DSA Management Console appears.

2. Enter the following command:

```
get cache;
```

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

Import the Default Policy Store Objects

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

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

To import the default policy store objects

1. Run the following command:

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

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

Windows example: smobjimport

```
-i"C:\Program Files\CA\sitefinder\db\smdif\smpolicy.smdif" -d"SM Admin" -wPassword -v
```

UNIX example: smobjimport

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-v

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

Default value: stdout

-cf

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

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

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

2. Run the following command:

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:

- **Windows**—*policy_server_home*\xps\dd
- **UNIX**—*policy_server_home*/xps/dd

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

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

```
XPSDDInstall SmObjects.xdd
```

XPSDDInstall imports the required data definitions.

3. Run the following command:

```
XPSDDInstall EPMSObjects.xdd
```

XPSDDInstall imports the required data definitions.

4. Run the following command:

```
XPSDDInstall SecCat.xdd
```

XPSDDInstall imports the required data definitions.

5. Run the following command:

```
XPSDDInstall FssSmObjects.xdd
```

You have imported all required policy store data definitions.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first-time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components. You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Note: 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.

To prepare for the Administrative UI registration

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

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

passphrase

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

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

-adminui-setup

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

-t *timeout*

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

Unit of measurement: minutes

Default: 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 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.

Sun Java System Directory Server as a Policy Store

Policy Servers installed on either Windows or UNIX systems can use a Sun Java System Directory Server as a policy store. The following sections detail how to manually configure your directory server as a policy 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 SiteMinder data store. You can print the applicable worksheet and use it to record required information before beginning.

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

More information:

[Active Directory Information Worksheet](#) (see page 382)

[Policy and Data Store Worksheets](#) (see page 381)

[Sun Java System Directory Server Information Worksheet](#) (see page 382)

How to Configure the Policy Store

To configure a Sun Java System Directory Server as a policy store, complete the following procedures:

1. (Optional) If applicable, use the LDAP vendor software to create an LDAP Directory Server instance.
2. (Optional) If applicable, review the Sun One 5.x Directory Server Considerations.
3. (Optional) If applicable, use the LDAP vendor software to create a user with privileges to create, read, modify, and delete objects in the LDAP tree underneath the policy store root object.
4. Point the Policy Server to the directory server.

5. Create the policy store schema.
6. Set the SiteMinder super user password.
7. Import the default SiteMinder objects.
8. Import the policy store data definitions.
9. Restart the Policy Server.
10. Prepare for the Administrative UI registration.

Sun ONE LDAP Directory Server Considerations

Consider the following if you plan on using a Sun ONE 5.x directory server as a policy store.

smldapsetup and Sun Java System Directory Server Enterprise Edition

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

root

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

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

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

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

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

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

Note: For more information about root and sub suffixes, see the Sun Microsystems [documentation](#).

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

For Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet), SiteMinder r12.0 SP2 creates a `UserRoot` and a `PolicySvr4` database. The `PolicySvr4` database has suffix mappings pointing to it. To replicate this policy store, set up a replication agreement for the `PolicySvr4` database directory.

Note: More information about a replication agreement, see the Sun Microsystems [documentation](#).

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

To replicate SiteMinder indexes

1. Generate the SiteMinder indexes:

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

Important! If you are running a SiteMinder utility or executable on Windows Server 2008, be sure to open the command-line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Set up the indexes on a replica server:

```
smldapsetup ldmod -x -findexes.ldif -h host -p replicaport  
-d AdminDN -w AdminPW
```

host

Specifies the replica host.

replicaport

Specifies the replica port number.

AdminDN

Specifies the replica administrator DN.

Example: cn=directory manager

AdminPW

Specifies the replica administrator password.

The SiteMinder indexes are replicated.

Point the Policy Server to the Directory Server

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

To point the Policy Server to the directory server

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

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

-hhost

Specifies the IP Address of the LDAP server host system.

-pport

Specifies the port on which the LDAP server is listening.

-dAdminDN

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

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

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

-wAdminPW

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

-rroot

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

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

-ssl1|0

Specifies an SSL connection.

Limits: 0=no | 1=yes

Default: 0

-ccert

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

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

2. Run the following command:

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

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

Create the Policy Store Schema

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

To create the policy store schema

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

```
smldapsetup ldgen -file_name
```

file_name

Specifies the name of the LDIF file you are creating.

An LDIF file with the SiteMinder schema is created.

2. Run the following command:

```
smldapsetup ldmod -file_name
```

file_name

Specifies the name of the LDIF you created.

smldapsetup imports the policy store schema.

3. Run the following command:

```
smldapsetup ldmod -fpolicy_server_home/xps/db/SunOne.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 SiteMinder Super User Password

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

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

To set the super user password

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

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

```
smreg -su password
```

password

Specifies the password for the default SiteMinder administrator.

Limits:

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

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

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

The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day-to-day operations. Use the default super user to import the default policy store objects, and to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Locate the Installation Media](#) (see page 456)

Import the Default Policy Store Objects

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

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

To import the default policy store objects

1. Run the following command:

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

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

Windows example: smobjimport

```
-i"C:\Program Files\CA\site\sm\smdif\smpolicy.smdif" -d"SM Admin" -wPassword -v
```

UNIX example: smobjimport

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-v

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

Default value: stdout

-cf

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

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

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

2. Run the following command:

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:

- **Windows**—*policy_server_home*\xps\dd
- **UNIX**—*policy_server_home*/xps/dd

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

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

```
XPSDDInstall SmObjects.xdd
```

XPSDDInstall imports the required data definitions.

3. Run the following command:

```
XPSDDInstall EPMSObjects.xdd
```

XPSDDInstall imports the required data definitions.

4. Run the following command:

```
XPSDDInstall SecCat.xdd
```

XPSDDInstall imports the required data definitions.

5. Run the following command:

```
XPSDDInstall FssSmObjects.xdd
```

You have imported all required policy store data definitions.

Restart the Policy Server

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

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

To restart the Policy Server

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.
The Policy Server stops as indicated by the red stoplight.
3. Click Start.
The Policy Server starts as indicated by the green stoplight.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first-time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components. You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Note: 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.

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 log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

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

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

-adminui-setup

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

-t timeout

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

Unit of measurement: minutes

Default: 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 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.

Active Directory as a Policy Store

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

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

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

Gather Directory Server Information

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

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

Host information

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

Port information

(Optional) Specifies a non-standard port.

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

Administrative DN

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

Administrative password

Specifies the password for the Administrative DN.

Policy store root DN

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

SSL client certificate

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

Limit: SSL only

More information:

[Active Directory Information Worksheet](#) (see page 382)

[Policy and Data Store Worksheets](#) (see page 381)

[Sun Java System Directory Server Information Worksheet](#) (see page 382)

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 LDAP vendor software to create an LDAP Directory Server instance.
2. (Optional) If applicable, use the LDAP vendor software to create a user with privileges to create, read, modify, and delete objects in the LDAP tree underneath the policy store root object.

Note: You do not have to complete this procedure if you have gathered the LDAP user name of a user with privileges to create, read, modify, and deleting objects 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 SiteMinder super user password.
6. Import the default SiteMinder objects.
7. Import the policy store data definitions.
8. Restart the Policy Server.
9. Prepare for the Administrative UI registration.

Point the Policy Server to the Directory Server

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

To point the Policy Server to the directory server

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

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

-hhost

Specifies the IP Address of the LDAP server host system.

-pport

Specifies the port on which the LDAP server is listening.

-dAdminDN

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

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

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

-wAdminPW

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

-rroot

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

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

-ssl1|0

Specifies an SSL connection.

Limits: 0=no | 1=yes

Default: 0

-ccert

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

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

2. Run the following command:

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

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

Create the Policy Store Schema

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

To create the policy store schema

1. 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 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 *policy_server_home*\xps\db and open the following file:

ActiveDirectory.ldif

4. Manually replace each instance of <RootDN> with the actual value of the root DN.

Example: 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 SiteMinder Super User Password

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

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

To set the super user password

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

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

```
smreg -su password
```

password

Specifies the password for the default SiteMinder administrator.

Limits:

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

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

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

The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day-to-day operations. Use the default super user to import the default policy store objects, and to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Locate the Installation Media](#) (see page 456)

Import the Default Policy Store Objects

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

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

To import the default policy store objects

1. Run the following command:

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

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

Windows example: smobjimport

```
-i"C:\Program Files\CA\sitefinder\db\smdif\smpolicy.smdif" -d"SM Admin" -wPassword -v
```

UNIX example: smobjimport

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-v

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

Default value: stdout

-cf

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

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

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

2. Run the following command:

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:

- **Windows**—*policy_server_home*\xps\dd
- **UNIX**—*policy_server_home*/xps/dd

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

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

```
XPSDDInstall SmObjects.xdd
```

XPSDDInstall imports the required data definitions.

3. Run the following command:

```
XPSDDInstall EPMSObjects.xdd
```

XPSDDInstall imports the required data definitions.

4. Run the following command:

```
XPSDDInstall SecCat.xdd
```

XPSDDInstall imports the required data definitions.

5. Run the following command:

```
XPSDDInstall FssSmObjects.xdd
```

You have imported all required policy store data definitions.

Restart the Policy Server

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

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

To restart the Policy Server

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.
The Policy Server stops as indicated by the red stoplight.
3. Click Start.
The Policy Server starts as indicated by the green stoplight.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first-time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components. You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Note: 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.

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 log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

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

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

-adminui-setup

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

-t timeout

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

Unit of measurement: minutes

Default: 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 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\Netegrity\SiteMinder\CurrentVersion\DS\LDAPProvider.
 - a. To enable support, set the EnableObjectCategory value to 1.
 - b. To disable support, set the EnableObjectCategory value to 0.

Note: The default value is 0.

On UNIX systems:

To enable or disable ObjectCategory attribute support

1. In a text editor, open the SiteMinder sm.registry file, located in
<siteminder_installation>/registry.
2. Locate the key
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\
Ds\LDAPProvider.
 - a. To enable support, set the EnableObjectCategory value to 1.
 - b. To disable support, set the EnableObjectCategory value to 0.

Note: The default value is 0.

Microsoft ADAM/AD LDS as a Policy Store

Policy Servers installed on either Windows or UNIX systems can use Microsoft ADAM or AD LDS as a policy store. The following sections detail how to configure the policy store manually.

Note: You can use the Policy Server Configuration wizard to configure this type of LDAP directory server as a policy store automatically.

ADAM/AD LDS Prerequisites

Be sure that you meet the following prerequisites before configuring the policy store:

1. Be sure that you have created a policy store partition.
2. (ADAM) Patch ADAM.
3. Be sure that users can be created in the configuration partition. Only an administrative user in the configuration partition can import the policy store schema.

Patch the ADAM Server

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

Allow User Creation in the Configuration Partition

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

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

To allow users to be created in the configuration partition

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. Do one of the following:
 - (ADAM 2000 and 2003) Click Add ADAM Account and paste the full DN of the user you created in the configuration partition.
 - (AD LDS) Click Add DN and paste the full DN of the user you created in the configuration partition.
- e. Go to the properties of the user you created and verify the value for the following object:
msDS-UserAccountDisabled

Be sure that the value is set false.

The administrative user has rights over the configuration partition and all application partitions, including the policy store partition.

Gather Directory Server Information

Configuring ADAM or AD 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 SiteMinder data store. You can print the applicable worksheet and 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 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.

More information:

[Policy and Data Store Worksheets](#) (see page 381)

[Microsoft ADAM/AD LDS Information Worksheet](#) (see page 383)

How to Configure the Policy Store

To configure ADAM or AD LDS as a policy store, complete the following procedures:

1. Be sure that you have met the ADAM/AD LDS prerequisites.
2. Be sure that you have gathered the necessary information.
3. Point the Policy Server to the directory server.
4. Create the policy store schema.
5. Set the SiteMinder super user password.
6. Import the default SiteMinder objects.
7. Import the policy store data definitions.
8. Restart the Policy Server.
9. Prepare for the Administrative UI registration.

Point the Policy Server to the Directory Server

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

To point the Policy Server to the directory server

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

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

-hhost

Specifies the IP Address of the LDAP server host system.

-pport

Specifies the port on which the LDAP server is listening.

-dAdminDN

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

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

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

-wAdminPW

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

-rroot

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

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

-ssl1|0

Specifies an SSL connection.

Limits: 0=no | 1=yes

Default: 0

-ccert

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

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

2. Run the following command:

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

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

Create the Policy Store Schema

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

To create the policy store schema

1. Run the following command:

```
smldapsetup ldgen -file_name
```

file_name

Specifies the name of the LDIF file you are creating.

An LDIF file with the SiteMinder schema is created.

2. Run the following command:

```
smldapsetup ldmod -file_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 one of the following:

- ADAM.ldif
- 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/file_name.ldif
```

siteminder_home

Specifies the Policy Server installation path.

file_name

Specifies one of the following:

- ADAM
- ADLDS

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

Set the SiteMinder Super User Password

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

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

To set the super user password

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

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

```
smreg -su password
```

password

Specifies the password for the default SiteMinder administrator.

Limits:

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

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

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

The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day-to-day operations. Use the default super user to import the default policy store objects, and to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Locate the Installation Media](#) (see page 456)

Import the Default Policy Store Objects

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

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

To import the default policy store objects

1. Run the following command:

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

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

Windows example: smobjimport

```
-i"C:\Program Files\CA\sitefinder\db\smdif\smpolicy.smdif" -d"SM Admin" -wPassword -v
```

UNIX example: smobjimport

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-v

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

Default value: stdout

-cf

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

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

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

2. Run the following command:

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:

- **Windows**—*policy_server_home*\xps\dd
- **UNIX**—*policy_server_home*/xps/dd

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

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

```
XPSDDInstall SmObjects.xdd
```

XPSDDInstall imports the required data definitions.

3. Run the following command:

```
XPSDDInstall EPMSObjects.xdd
```

XPSDDInstall imports the required data definitions.

4. Run the following command:

```
XPSDDInstall SecCat.xdd
```

XPSDDInstall imports the required data definitions.

5. Run the following command:

```
XPSDDInstall FssSmObjects.xdd
```

You have imported all required policy store data definitions.

Restart the Policy Server

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

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

To restart the Policy Server

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.
The Policy Server stops as indicated by the red stoplight.
3. Click Start.
The Policy Server starts as indicated by the green stoplight.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first-time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components. You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Note: 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.

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 log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

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

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

-adminui-setup

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

-t timeout

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

Unit of measurement: minutes

Default: 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 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.

SiteMinder Key Store Overview

Web Agents use Agent keys to encrypt and decrypt SiteMinder cookies so the data they contain can be read. The Agent uses the key to encrypt cookies before sending them to a user's browser and to decrypt cookies received from other Web Agents. When a Web Agent starts up and makes a management call request, the Policy Server supplies the current set of keys. Each time that the Web Agent polls the Policy Server, the Agent again makes the management call. The Web Agent receives the updated keys. These keys are stored in either the policy store or in a separate store.

Configure a Key Store in an Existing Policy Store

To configure a key store in an existing policy store

1. Start the Policy Server Management Console.
Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.
2. Select the Data tab to move it to the front.
3. In the Database drop-down list, select Key Store.
4. Select Use Policy Store database check box.
5. Click Apply to save the settings.
6. On the Data tab, click Test LDAP Connection to verify connectivity to the policy store in the LDAP directory.

Configure a Separate Key Store

To configure a separate key store

1. Start the Policy Server Management Console.
Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.
2. Select the Data tab to move it to the front.
3. In the Database drop-down list, select Key Store.
4. In the Storage drop-down list, select LDAP.
5. (Optional) If applicable, deselect the Use Policy Store database check box.

6. In the LDAP Key Store group box, enter the following:
 - a. In the LDAP IP Address field, enter the IP address (or host name) and port number of the LDAP directory, separated by a colon (:).
Example, enter 123.123.12.12:321. If the port is not specified, SiteMinder uses port 389 as the default.
 - b. In the Root DN field, enter the LDAP branch under which the SiteMinder policy store is located.
Example: o=airius.com.
 - c. In the Admin Username field, enter the DN of the LDAP directory administrator for the Policy Server being configured.
 - d. Example, cn=Directory Manager.
 - e. In the Password field, enter the LDAP directory administrator password.
 - f. In the Confirm Password field, re-enter the LDAP directory administrator password.
 - g. (Optional) If your system is communicating with the LDAP directory over SSL, select the Use SSL check box.
 - h. Click Apply.
7. (Optional) If you are using SSL, enter the name of the certificate database in the Netscape Certificate Database File field on the Settings tab.
8. Click Apply to save the settings.
9. On the Data tab, click Test LDAP Connection to verify connectivity to the LDAP directory server.
10. Click OK to save the settings and close the Console.

Chapter 8: Configuring SiteMinder Data in a Relational Database

This section contains the following topics:

[Relational Databases as a Policy or Key Store](#) (see page 147)

[Installation Road Map](#) (see page 148)

[Important Considerations](#) (see page 149)

[Schema Files for Relational Databases](#) (see page 149)

[Configure a SQL Server Policy Store](#) (see page 151)

[Configure an Oracle Policy Store](#) (see page 165)

[Configure SQL Server Data Stores](#) (see page 186)

[Configure Oracle Data Stores](#) (see page 212)

[Sample User Directories](#) (see page 258)

Relational Databases as a Policy or Key Store

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

When you install the Policy Server, you can automatically configure several directory servers as a policy store. However, if you are implementing a relational database as a policy store, you manually configure the 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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

In addition to policy store support, you can use a relational database to store SiteMinder keys, audit logs, token data, and session data. Storing keys in a separate database may be required to implement single sign-on functionality.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Installation Road Map

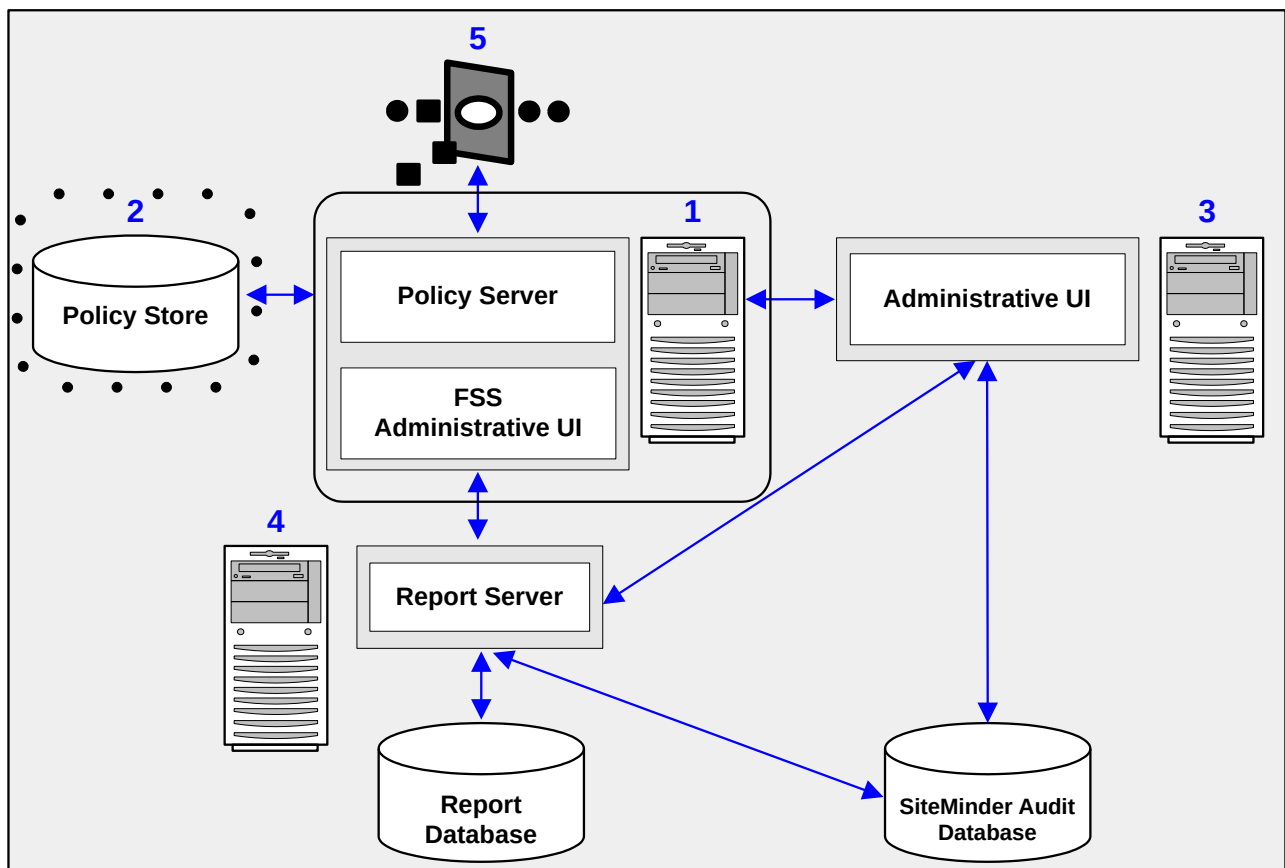
The following diagram illustrates a sample SiteMinder installation and lists the order in which you install and configure each component.

- A solid line surrounds the components that are required before configuring a policy store. They include the following:
 - A Policy Server
 - A non-registered FSS Administrative UI

If a Policy Server is not part of your environment, do not continue with the installation process.

- The component surrounded by a green dotted line is the policy store, which you configure 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.



Note: If you are trying to configure or upgrade a SiteMinder store listed in the SiteMinder Platform Support Matrix and cannot find the procedures in this guide, see the *Directory Configuration Guide*.

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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Schema Files for Relational Databases

SiteMinder provides schema files to create the individual schema for storing policies; keys; logs; session data; token data, such as Encotone TeleID data; and sample users. You can store SiteMinder data in a single SQL Server or Oracle database, or run each script on its own to create a separate:

- policy store
- key store
- logging database
- token store

- session store
- sample users database

Note: The SiteMinder schema files are installed with the Policy Server. If the Policy Server is installed on a UNIX system, copy the schema files from <sitefinder_home>/db/SQL directory to a temporary directory (C:\temp) on the Windows system to which the database is installed.

SQL Server Schema Files

The following SQL Server schema files are provided in the *policy_server_home*\db\SQL directory:

policy_server_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 SiteMinder audit logs in a SQL Server database.

sm_mssql_token.sql

Creates the schema for storing token data, such as Encotone TeleID data, in a SQL Server database.

sm_mssql_ss.sql

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

smsampleusers_sqlserver.sql

Creates the schema for SiteMinder sample users in a SQL Server database and populates the database with sample users. For example, if you look in the script, you can see a sample user named GeorgeC with a password of sitefinder.

The following SQL Server schema file is provided in *policy_server_home*\xps\db:

SQLServer.sql

Creates the XPS schema for a SQL Server policy store.

Oracle Schema Files

The following Oracle schema files are provided in the *policy_server_home*\db\SQL directory.

policy_server_home

Specifies the Policy Server installation path.

sm_oracle_ps.sql

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

sm_oracle_logs.sql

Creates the schema for SiteMinder audit logs in an Oracle database.

sm_oracle_token.sql

Creates the schema for storing token data, such as Encotone TeleID data, in an Oracle database.

sm_oracle_ss.sql

Creates the schema for the Session Server in an Oracle database.

smsampleusers_oracle.sql

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

The following Oracle schema file is provided in the *policy_server_home*\xps\db directory.

Oracle.sql

Creates the XPS schema for an Oracle policy store.

Configure a SQL Server Policy Store

Policy Servers installed on either Windows or UNIX systems can use a single SQL Server database to function as a:

- policy store
- key store
- token store

- session store
- logging database

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

Note: The database must be installed on a Windows system. Additionally, the 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.

Gather Database Information

Configuring a single SQL Server database to function as a policy store or any other type of 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 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 SiteMinder data store. You can print the applicable worksheet and 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.
- (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.

More information:

[SQL Server Information Worksheet](#) (see page 383)

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 SiteMinder data is accessible from the Policy Server system.
2. Using the SQL Server Enterprise Manager, create the database instance for the SiteMinder data store.

Example: smdatastore.

3. Create the SiteMinder Schema.
4. Configure a SQL Server data source for 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 SiteMinder super user password.
7. Import the default SiteMinder objects.
8. Import the policy store data definitions.
9. Restart the Policy Server.
10. Prepare for the Administrative UI registration.

Create the SiteMinder Schema

You create the SiteMinder schema so that SQL Server database can store policy, key, token session, and audit logging information.

The following warnings are displayed when running the policy store and audit logging schema files and 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.

To create the SiteMinder Schema

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 a logging database, token store, and session store.

The respective schema files are:

- sm_mssql_logs.sql
- sm_mssql_token.sql
- sm_mssql_ss.sql

The respective SiteMinder schema is added to the database.

Note: You are not required to configure the policy store to store additional SiteMinder data. You can configure individual databases to function as one or more separate logging databases, key stores, token stores, and session stores.

The database can store SiteMinder data.

Configure a SQL Server Data Source for SiteMinder

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

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.

To create the data source on Windows

1. Click Start and select Programs, Administrative Tools, ODBC Data Sources.
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 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: 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 SiteMinder ODBC data sources are configured using a `system_odbc.ini` file, which you create by renaming `sqlserverwire.ini`, located in `policy_server_installation/db`, to `system_odbc.ini`. This `system_odbc.ini` file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [SiteMinder Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding a SQL Server Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the `system_odbc.ini` file if you create a new service name or want to use a different driver. You should have entries for the Oracle or SQL drivers under [SiteMinder Data Source].

Again, to configure a 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 SiteMinder should use 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 and rename `oraclewire.ini` to `system_odbc.ini`, which is located in `<policy_server_installation>/db`.

The `system_odbc.ini` file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

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

SiteMinder Data Source=DataDirect 5.3 SQL Server 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/NSmass23.so
Description=DataDirect 5.3 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 may cause ODBC connections to fail.

nete_ps_root

Specifies an explicit path, rather than one with an environment variable.

Example: export/smuser/siteminder

SiteMinder Data

Specifies the SQL Server database instance name.

myhost

Specifies the IP Address of the SQL Server database.

1433

Represents the default listening port for SQL Server.

4. Save the file.

The wire protocol driver is configured.

Point the Policy Server to the Database

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

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.
Database settings appear.
2. Select ODBC from the Storage list.
ODBC settings appear.
3. Select Policy Store from the Database list.
4. Enter the name of the data source in the Data Source Information field.
 - **Windows** - this entry must match the name you entered in the Data Source field of the ODBC Oracle Wire Protocol Driver Setup dialog when you created the Oracle data source or the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog when you created the SQL data source.
 - **UNIX** - this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, ensure that you enter the correct value.
5. Enter and confirm the username and password of the database account that has full access rights to the database instance in the respective fields.

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

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

7. Click Apply.

The settings are saved.

8. Select Key Store from the Database list.

Data source information appears.

9. Select the Use the policy store database check box and click Apply.

10. Select Audit Logs from the Database list.

Data source settings appear.

11. Select the Use the policy store database check box and click Apply.

12. Select Token Data from the Database list.

Data source settings appear.

13. Select the User policy store database check box and click Apply.

14. Click Test Connection.

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

15. Click OK.

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

Set the SiteMinder Super User Password

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

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

To set the super user password

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

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

```
smreg -su password
```

password

Specifies the password for the default SiteMinder administrator.

Limits:

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

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

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

The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day-to-day operations. Use the default super user to import the default policy store objects, and to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Locate the Installation Media](#) (see page 456)

Import the Default Policy Store Objects

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

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

To import the default policy store objects

1. Run the following command:

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

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

Windows example: smobjimport

```
-i"C:\Program Files\CA\sitefinder\db\smdif\smpolicy.smdif" -d"SM Admin" -wPassword -v
```

UNIX example: smobjimport

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-v

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

Default value: stdout

-cf

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

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

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

2. Run the following command:

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:

- **Windows**—*policy_server_home*\xps\dd
- **UNIX**—*policy_server_home*/xps/dd

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

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

```
XPSDDInstall SmObjects.xdd
```

XPSDDInstall imports the required data definitions.

3. Run the following command:

```
XPSDDInstall EPMSObjects.xdd
```

XPSDDInstall imports the required data definitions.

4. Run the following command:

```
XPSDDInstall SecCat.xdd
```

XPSDDInstall imports the required data definitions.

5. Run the following command:

```
XPSDDInstall FssSmObjects.xdd
```

You have imported all required policy store data definitions.

Restart the Policy Server

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

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

To restart the Policy Server

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.
The Policy Server stops as indicated by the red stoplight.
3. Click Start.
The Policy Server starts as indicated by the green stoplight.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first-time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components. You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Note: 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.

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 log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

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

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

-adminui-setup

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

-t timeout

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

Unit of measurement: minutes

Default: 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 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

Policy Servers installed on either Windows or UNIX systems can use a single Oracle database to function as a:

- policy store
- key store

- token store
- session 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 SiteMinder data.

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:

[Create an Oracle 10g User to Manage the Policy Store's Table Space](#) (see page 167)

Create an Oracle 10g User to Manage the Policy Store's Table Space

Creating a user to manage table space for the policy store is a prerequisite for an Oracle 10g database only.

To create a user to manage table space for the policy store

1. On the Oracle global database's configuration screen, select Administration, Users.
2. On the Create Tablespaces screen, click Create.
3. On the Create User screen, enter the:
 - Name for the user.
Example: NETE
 - Password for the user.
 - Default Tablespace that you created.
 - Temporary tablespace.
Example: TEMP
4. Click Roles.
5. Select Modify.
6. On the Modify Roles screen:
 - a. Select CONNECT and RESOURCE as a roles for this user.
 - b. Click Apply.
7. Start sqlplus in a command window, by entering:
 - a. sqlplus
 - b. the credentials for the policy store user created on the Create User screen.

You have completed the prerequisites for an Oracle 10g database, and can now configure a SiteMinder data store for the database.

Gather Database Information

Configuring a single Oracle database to function as a policy store or any other type of 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 SiteMinder data store. You can print the applicable worksheet and use it to record required information before beginning.

More information:

[Oracle Information Worksheet](#) (see page 384)

[Oracle RAC Information Worksheet](#) (see page 384)

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 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 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 Information

Gather the following information only if you are configuring a supported Oracle RAC database as a policy store or any other 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 =
(AADDRESS = PROTOCOL = TCP)(HOST = nete_servername1)(PORT=1521
(AADDRESS = PROTOCOL = TCP)(HOST = nete_servername2)(PORT=1521)
(AADDRESS = 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.

How to Configure the Policy Store

To configure a single Oracle database as policy store, key store, token store, session 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 SiteMinder data is accessible from the Policy Server system. Test the communication using tnsping or sqlplus.
2. Create the SiteMinder Schema.
3. Configure an Oracle data source for 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 SiteMinder super user password.
6. Import the default policy store objects.
7. Import the policy store data definitions.
8. Restart the Policy Server.
9. Prepare for the Administrative UI registration.

Create the SiteMinder Schema

You create the SiteMinder schema so a single Oracle database can store policy, key, token, session, and audit logging information.

To create the 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 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 policy store and key store schema is added to the database.

3. Import the following script

```
$NETE_PS_ROOT/xps/Oracle.sql
```

The policy store schema is extended.

4. Import the following scripts to use the policy store as a logging database, token store, and/or session store.

The respective schema files are:

- sm_oracle_logs.sql
- sm_oracle_token.sql
- sm_oracle_ss.sql

The respective SiteMinder schema is created in the database.

Note: You are not required to configure the policy store to store additional SiteMinder data. You can configure individual databases to function as one or more separate logging databases, key stores, token stores, and session stores.

The database can store SiteMinder data.

Configure an Oracle Data Source for SiteMinder

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

Create an Oracle Data Source on Windows**To create an Oracle data source on Windows**

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

The ODBC Data Source Administrator

3. Select 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 Data Source on Windows

You can configure Oracle RAC 9.2.0.6 and 10.1.0.4 instances with the Policy Server as a single data source name similar to that of a single instance Oracle database. However, the data source name for Oracle RAC is different than a regular ODBC data source.

In an Oracle RAC system, in addition to the SID or ServiceName for each Oracle instance, there is also a ServiceName for the entire Oracle RAC system. When configuring a data source, configure the data source name to use this ServiceName when connecting to an Oracle RAC.

To configure an Oracle RAC data source

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

3. Select 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_se
rvicename[,...])
```

10. Select LoadBalancing.

11. Click OK

The Oracle RAC data source is configured for the wire protocol driver.

Create an Oracle Data Source on UNIX Systems

The SiteMinder ODBC data sources are configured using a `system_odbc.ini` file, which you create by renaming `oraclewire.ini`, located in *policy_server_installation/db*, to `system_odbc.ini`. This `system_odbc.ini` file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [SiteMinder Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding an Oracle Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the `system_odbc.ini` file if you create a new service name or want to use a different driver. You should have entries for the SQL Server or Oracle drivers under [SiteMinder Data Source].

Again, to configure an Oracle data source, you must first create a `system_odbc.ini` file in the *policy_server_installation/db* directory. To do this, you need to rename `oraclewire.ini`, located in *policy_server_installation/db*, to `system_odbc.ini`.

Configure the Oracle Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder should use 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 and rename `oraclewire.ini` to `system_odbc.ini`, which is located in *<policy_server_installation>/db*.

The `system_odbc.ini` file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the `system_odbc.ini` file.
2. Depending on the data source you are configuring, edit the applicable data source sections with the following information:

```
Driver=nete_ps_root/odbc/lib/NSora23.so
Description=DataDirect 5.3 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 to where the 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_servername

Specifies the machine name where the Oracle database is installed.

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 RAC Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder should use 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 and rename oraclewire.ini to system_odbc.ini, which is located in *<policy_server_installation>/db*.

The system_odbc.ini file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the system_odbc.ini file.
2. 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/NSora23.so
Description=DataDirect 5.3 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_servicename1

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 service name for the entire Oracle RAC system.

AlternateServers

Specifies the connection failover to the other Oracle nodes, if the primary server is not accepting connections.

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 SiteMinder data in the policy store.

To point the Policy Server to the data store

1. Open the Policy Server Management Console, and click the Data tab.
Database settings appear.
2. Select ODBC from the Storage list.
ODBC settings appear.
3. Select Policy Store from the Database list.
4. Enter the name of the data source in the Data Source Information field.
 - **Windows** - this entry must match the name you entered in the Data Source field of the ODBC Oracle Wire Protocol Driver Setup dialog when you created the Oracle data source or the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog when you created the SQL data source.
 - **UNIX** - this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, ensure that you enter the correct value.
5. Enter and confirm the username and password of the database account that has full access rights to the database instance in the respective fields.

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

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

7. Click Apply.

The settings are saved.

8. Select Key Store from the Database list.

Data source information appears.

9. Select the Use the policy store database check box and click Apply.

10. Select Audit Logs from the Database list.

Data source settings appear.

11. Select the Use the policy store database check box and click Apply.

12. Select Token Data from the Database list.

Data source settings appear.

13. Select the User policy store database check box and click Apply.

14. Click Test Connection.

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

15. Click OK.

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

Set the SiteMinder Super User Password

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

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

To set the super user password

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

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

```
smreg -su password
```

password

Specifies the password for the default SiteMinder administrator.

Limits:

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

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

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

The password for the default SiteMinder administrator account is set.

Note: We recommend that you do not use the default super user for day-to-day operations. Use the default super user to import the default policy store objects, and to access the FSS Administrative UI and Administrative UI for the first-time and then create an administrator with super user permissions.

More information:

[Locate the Installation Media](#) (see page 456)

Import the Default Policy Store Objects

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

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

To import the default policy store objects

1. Run the following command:

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

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

Windows example: smobjimport

```
-i"C:\Program Files\CA\site\sm\smdif\smpolicy.smdif" -d"SM Admin" -wPassword -v
```

UNIX example: smobjimport

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-v

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

Default value: stdout

-cf

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

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

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

2. Run the following command:

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

policy_server_home

Specifies the Policy Server installation path.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder super user account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder super user account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

1. Open a command window and navigate to one of the following locations:

- **Windows**—*policy_server_home*\xps\dd
- **UNIX**—*policy_server_home*/xps/dd

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

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

```
XPSDDInstall SmObjects.xdd
```

XPSDDInstall imports the required data definitions.

3. Run the following command:

```
XPSDDInstall EPMSObjects.xdd
```

XPSDDInstall imports the required data definitions.

4. Run the following command:

```
XPSDDInstall SecCat.xdd
```

XPSDDInstall imports the required data definitions.

5. Run the following command:

```
XPSDDInstall FssSmObjects.xdd
```

You have imported all required policy store data definitions.

Restart the Policy Server

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

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

To restart the Policy Server

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.
The Policy Server stops as indicated by the red stoplight.
3. Click Start.
The Policy Server starts as indicated by the green stoplight.

Prepare for the Administrative UI Registration

You use the default SiteMinder super user account (siteminder) to log into the Administrative UI for the first-time. The initial login requires that you to register the Administrative UI with a Policy Server, which creates a trusted relationship between both components. You prepare for the registration by using the XPSRegClient utility to supply the super user account name and password. The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

Note: 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.

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 log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

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

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

-adminui-setup

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

-t timeout

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

Unit of measurement: minutes

Default: 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 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 SQL Server Data Stores

SiteMinder key, audit log, token, and session information can each be stored in a separate database.

The following sections detail how to configure individual data stores.

Note: Storing keys in a separate database may be required to implement single sign-on functionality. More information on key management exists in the *Policy Server Administration Guide*.

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 SiteMinder.
4. Point the Policy Server to the Database.
5. Restart the Policy Server.

Note: If you are trying to configure or upgrade a SiteMinder store listed in the SiteMinder Platform Support Matrix and cannot find the procedures in this guide, see the *Directory Configuration Guide*.

Gather Database Information

Configuring a single SQL Server database to function as a policy store or any other type of 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 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 SiteMinder data store. You can print the applicable worksheet and 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.

- (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.

More information:

[SQL Server Information Worksheet](#) (see page 383)

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 SiteMinder key store schema is created in the database.

Configure a SQL Server Data Source for SiteMinder

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

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.

To create the data source on Windows

1. Click Start and select Programs, Administrative Tools, ODBC Data Sources.
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 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: 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 SiteMinder ODBC data sources are configured using a `system_odbc.ini` file, which you create by renaming `sqlserverwire.ini`, located in *policy_server_installation/db*, to `system_odbc.ini`. This `system_odbc.ini` file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, `[ODBC Data Sources]`, contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is `[SiteMinder Data Source]`, take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding a SQL Server Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the `system_odbc.ini` file if you create a new service name or want to use a different driver. You should have entries for the Oracle or SQL drivers under [SiteMinder Data Source].

Again, to configure a 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 SiteMinder should use 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 and rename `oraclewire.ini` to `system_odbc.ini`, which is located in `<policy_server_installation>/db`.

The `system_odbc.ini` file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

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

SiteMinder Data Source=DataDirect 5.3 SQL Server 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/NSmass23.so
Description=DataDirect 5.3 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 may cause ODBC connections to fail.

nete_ps_root

Specifies an explicit path, rather than one with an environment variable.

Example: export/smuser/siteminder

SiteMinder Data

Specifies the SQL Server database instance name.

myhost

Specifies the IP Address of the SQL Server database.

1433

Represents the default listening port for SQL Server.

4. Save the file.

The wire protocol driver is configured.

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 field of the ODBC Oracle Wire Protocol Driver Setup dialog when you created the Oracle data source or the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog when you created the SQL data source.
 - **UNIX**—this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.
5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
6. Specify the maximum number of database connections allocated to SiteMinder.
Note: We recommend retaining the default for best performance.
7. Click Apply.
The settings are saved.
8. Click Test Connection.
SiteMinder returns a confirmation that the Policy Server can access the data store.
9. Click OK.
The Policy Server is configured to use the database as a key store

Restart the Policy Server

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

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

To restart the Policy Server

1. Open the Policy Server Management Console.
2. Click the Status tab, and click Stop in the Policy Server group box.
The Policy Server stops as indicated by the red stoplight.
3. Click Start.
The Policy Server starts as indicated by the green stoplight.

How to Store Audit Logs in SQL Server

To configure a SQL Server database as a standalone audit logging database, complete the following procedures:

1. Gather Database Information.
2. Create the Audit Log Schema.
3. Configure a SQL Server Data Source for SiteMinder.
4. Point the Policy Server to the Database.
5. Restart the Policy Server.

Note: If you are trying to configure or upgrade a SiteMinder store listed in the SiteMinder Platform Support Matrix and cannot find the procedures in this guide, see the *Directory Configuration Guide*.

Gather Database Information

Configuring a single SQL Server database to function as a policy store or any other type of 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 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 SiteMinder data store. You can print the applicable worksheet and 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.
- (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.

More information:

[SQL Server Information Worksheet](#) (see page 383)

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 SiteMinder audit log store schema is created in the database.

Configure a SQL Server Data Source for SiteMinder

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

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.

To create the data source on Windows

1. Click Start and select Programs, Administrative Tools, ODBC Data Sources.
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 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: 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 SiteMinder ODBC data sources are configured using a `system_odbc.ini` file, which you create by renaming `sqlserverwire.ini`, located in `policy_server_installation/db`, to `system_odbc.ini`. This `system_odbc.ini` file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [SiteMinder Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding a SQL Server Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the `system_odbc.ini` file if you create a new service name or want to use a different driver. You should have entries for the Oracle or SQL drivers under [SiteMinder Data Source].

Again, to configure a 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 SiteMinder should use 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 and rename `oraclewire.ini` to `system_odbc.ini`, which is located in `<policy_server_installation>/db`.

The `system_odbc.ini` file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

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

SiteMinder Data Source=DataDirect 5.3 SQL Server 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/NSmass23.so
Description=DataDirect 5.3 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 may cause ODBC connections to fail.

nete_ps_root

Specifies an explicit path, rather than one with an environment variable.

Example: export/smuser/siteminder

SiteMinder Data

Specifies the SQL Server database instance name.

myhost

Specifies the IP Address of the SQL Server database.

1433

Represents the default listening port for SQL Server.

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 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 field of the ODBC Oracle Wire Protocol Driver Setup dialog when you created the Oracle data source or the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog when you created the SQL data source.

- **UNIX**—this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.

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

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

Note: We recommend retaining the default for best performance.

8. Click Apply.

The settings are saved.

9. Click Test Connection.

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

10. Click OK.

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

Restart the Policy Server

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

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

To restart the Policy Server

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

The Policy Server stops as indicated by the red stoplight.

3. Click Start.

The Policy Server starts as indicated by the green stoplight.

How to Store Token Data in SQL Server

To configure a SQL Server database as a standalone token store, complete the following procedures:

1. Gather Database Information.
2. Create the Token Store Schema.
3. Configure a SQL Server Data Source for SiteMinder.

4. Point the Policy Server to the Database.
5. Restart the Policy Server.

Note: If you are trying to configure or upgrade a SiteMinder store listed in the SiteMinder Platform Support Matrix and cannot find the procedures in this guide, see the *Directory Configuration Guide*.

Gather Database Information

Configuring a single SQL Server database to function as a policy store or any other type of 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 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 SiteMinder data store. You can print the applicable worksheet and 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.
- (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.

More information:

[SQL Server Information Worksheet](#) (see page 383)

Create the Token Store Schema

You create the logging schema so the SQL Server database can store token information.

To create the token store schema

1. Open `sm_mssql_token.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_token.sql` into the query.
5. Execute the query.

The SiteMinder token store schema is created in the database.

Configure a SQL Server Data Source for SiteMinder

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

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.

To create the data source on Windows

1. Click Start and select Programs, Administrative Tools, ODBC Data Sources.
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 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: 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 SiteMinder ODBC data sources are configured using a `system_odbc.ini` file, which you create by renaming `sqlserverwire.ini`, located in *policy_server_installation/db*, to `system_odbc.ini`. This `system_odbc.ini` file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [SiteMinder Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding a SQL Server Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the `system_odbc.ini` file if you create a new service name or want to use a different driver. You should have entries for the Oracle or SQL drivers under [SiteMinder Data Source].

Again, to configure a 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 SiteMinder should use 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 and rename `oraclewire.ini` to `system_odbc.ini`, which is located in `<policy_server_installation>/db`.

The `system_odbc.ini` file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

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

SiteMinder Data Source=DataDirect 5.3 SQL Server Wire Protocol.

- 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/NSmass23.so
Description=DataDirect 5.0 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 may cause ODBC connections to fail.

nete_ps_root

Specifies an explicit path, rather than one with an environment variable.

Example: export/smuser/siteminder

SiteMinder Data

Specifies the SQL Server database instance name.

myhost

Specifies the IP Address of the SQL Server database.

1433

Represents the default listening port for SQL Server.

- Save the file.
The wire protocol driver is configured.

Point the Policy Store 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

- Open the Policy Server Management Console, and click the Data tab.
Database settings appear.
- Select ODBC from the Storage list.
ODBC settings appear.
- Select Token Data from the Database list.
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 field of the ODBC Oracle Wire Protocol Driver Setup dialog when you created the Oracle data source or the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog when you created the SQL data source.
 - **UNIX**—this entry must match the first line of the data source entry in the system_odbrc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.
5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
6. Specify the maximum number of database connections allocated to SiteMinder.

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

The settings are saved.
8. Click Test Connection.

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

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

Restart the Policy Server

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

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

To restart the Policy Server

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

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

The Policy Server starts as indicated by the green stoplight.

How to Store Session Information in SQL Server

To configure a SQL Server database as a session store, complete the following procedures:

1. Gather Database Information.
2. Create the Session Store Schema.
3. Configure a SQL Server Data Source for SiteMinder.
4. Point the Policy Server to the Database.
5. Restart the Policy Server.

Note: If you are trying to configure or upgrade a SiteMinder store listed in the SiteMinder Platform Support Matrix and cannot find the procedures in this guide, see the *Directory Configuration Guide*.

Gather Database Information

Configuring a single SQL Server database to function as a policy store or any other type of 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 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 SiteMinder data store. You can print the applicable worksheet and 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.
- (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.

More information:

[SQL Server Information Worksheet](#) (see page 383)

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. 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 from sm_mssql_ss.sql into the query.
5. Execute the query.

The session store schema is created in the database.

Configure a SQL Server Data Source for SiteMinder

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

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.

To create the data source on Windows

1. Click Start and select Programs, Administrative Tools, ODBC Data Sources.
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 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: 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 SiteMinder ODBC data sources are configured using a `system_odbc.ini` file, which you create by renaming `sqlserverwire.ini`, located in `policy_server_installation/db`, to `system_odbc.ini`. This `system_odbc.ini` file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, `[ODBC Data Sources]`, contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is `[SiteMinder Data Source]`, take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding a SQL Server Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the system_odbc.ini file if you create a new service name or want to use a different driver. You should have entries for the Oracle or SQL drivers under [SiteMinder Data Source].

Again, to configure a 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 SiteMinder should use 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 and rename oraclewire.ini to system_odbc.ini, which is located in *<policy_server_installation>/db*.

The system_odbc.ini file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the system_odbc.ini file.
2. Enter the following under [ODBC Data Sources]:
SiteMinder Data Source=DataDirect 5.3 SQL Server 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/NSmass23.so
Description=DataDirect 5.3 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 may cause ODBC connections to fail.

nete_ps_root

Specifies an explicit path, rather than one with an environment variable.

Example: export/smuser/siteminder

SiteMinder Data

Specifies the SQL Server database instance name.

myhost

Specifies the IP Address of the SQL Server database.

1433

Represents the default listening port for SQL Server.

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 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 field of the ODBC Oracle Wire Protocol Driver Setup dialog when you created the Oracle data source or the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog when you created the SQL data source.
 - **UNIX**—this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.
4. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
5. Specify the maximum number of database connections allocated to SiteMinder.

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

The settings are saved.
7. Click Test Connection.

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

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

Restart the Policy Server

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

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

To restart the Policy Server

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

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

The Policy Server starts as indicated by the green stoplight.

Configure Oracle Data Stores

SiteMinder key, audit log, token, and session information can each be stored in a separate database.

The following sections detail how to configure individual data stores.

Note: Storing keys in a separate database may be required to implement single sign-on functionality. More information on key management exists in the *Policy Server Administration Guide*.

How to Store Key Information in Oracle

To configure an Oracle database as key store, complete the following procedures:

1. Gather Database Information.
2. Create the Key Store Schema.
3. Configure an Oracle Data Source for SiteMinder.
4. Point the Policy Server to the Database.
5. Restart the Policy Server.

Note: If you are trying to configure or upgrade a SiteMinder store listed in the SiteMinder Platform Support Matrix and cannot find the procedures in this guide, see the *Directory Configuration Guide*.

Gather Database Information

Configuring a single Oracle database to function as a policy store or any other type of 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 SiteMinder data store. You can print the applicable worksheet and use it to record required information before beginning.

More information:

[Oracle Information Worksheet](#) (see page 384)

[Oracle RAC Information Worksheet](#) (see page 384)

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 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 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 Information

Gather the following information only if you are configuring a supported Oracle RAC database as a policy store or any other 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=
(AADDRESS = PROTOCOL = TCP)(HOST = nete_servername1)(PORT=1521
(AADDRESS = PROTOCOL = TCP)(HOST = nete_servername2)(PORT=1521)
(AADDRESS = 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.

Create the Key Store Schema

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

To create the 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 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.

Configure an Oracle Data Source for SiteMinder

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

Create an Oracle Data Source on Windows

To create an Oracle data source on Windows

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

3. Select 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 Data Source on Windows

You can configure Oracle RAC 9.2.0.6 and 10.1.0.4 instances with the Policy Server as a single data source name similar to that of a single instance Oracle database. However, the data source name for Oracle RAC is different than a regular ODBC data source.

In an Oracle RAC system, in addition to the SID or ServiceName for each Oracle instance, there is also a ServiceName for the entire Oracle RAC system. When configuring a data source, configure the data source name to use this ServiceName when connecting to an Oracle RAC.

To configure an Oracle RAC data source

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

3. Select 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 Data Source on UNIX Systems

The SiteMinder ODBC data sources are configured using a system_odbc.ini file, which you create by renaming oraclewire.ini, located in *policy_server_installation/db*, to system_odbc.ini. This system_odbc.ini file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [SiteMinder Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding an Oracle Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the `system_odbc.ini` file if you create a new service name or want to use a different driver. You should have entries for the SQL Server or Oracle drivers under [SiteMinder Data Source].

Again, to configure an Oracle data source, you must first create a `system_odbc.ini` file in the `policy_server_installation/db` directory. To do this, you need to rename `oraclewire.ini`, located in `policy_server_installation/db`, to `system_odbc.ini`.

Configure the Oracle Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder should use 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 and rename `oraclewire.ini` to `system_odbc.ini`, which is located in `<policy_server_installation>/db`.

The `system_odbc.ini` file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the system_odbc.ini file.
2. Depending on the data source you are configuring, edit the applicable data source sections with the following information:

```
Driver=nete_ps_root/odbc/lib/NSora23.so
Description=DataDirect 5.3 Oracle Wire Protocol
LoginID=uid
Password=pwd
HostName=nete_servename
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 to where the 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_servername

Specifies the machine name where the Oracle database is installed.

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 RAC Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder should use 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 and rename oraclewire.ini to system_odbc.ini, which is located in *<policy_server_installation>/db*.

The system_odbc.ini file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the system_odbc.ini file.
2. 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/NSora23.so
Description=DataDirect 5.3 Oracle Wire Protocol
Logon=uid
Password=pwd
HostName=nete_servename1
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_servicename1

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 service name for the entire Oracle RAC system.

AlternateServers

Specifies the connection failover to the other Oracle nodes, if the primary server is not accepting connections.

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 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 field of the ODBC Oracle Wire Protocol Driver Setup dialog when you created the Oracle data source or the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog when you created the SQL data source.
 - **UNIX**—this entry must match the first line of the data source entry in the system_odbrc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.
5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
6. Specify the maximum number of database connections allocated to SiteMinder.

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

The settings are saved.
8. Click Test Connection.

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

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

Restart the Policy Server

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

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

To restart the Policy Server

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

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

The Policy Server starts as indicated by the green stoplight.

How to Store Audit Logs in Oracle

To configure an Oracle database as key store, complete the following procedures:

1. Gather Database Information.
2. Create the Audit Log Schema.
3. Configure an Oracle Data Source for SiteMinder.
4. Point the Policy Server to the Database.
5. Restart the Policy Server.

Note: If you are trying to configure or upgrade a SiteMinder store listed in the SiteMinder Platform Support Matrix and cannot find the procedures in this guide, see the *Directory Configuration Guide*.

Gather Database Information

Configuring a single Oracle database to function as a policy store or any other type of 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 SiteMinder data store. You can print the applicable worksheet and use it to record required information before beginning.

More information:

[Oracle Information Worksheet](#) (see page 384)

[Oracle RAC Information Worksheet](#) (see page 384)

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 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 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 Information

Gather the following information only if you are configuring a supported Oracle RAC database as a policy store or any other 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.

Create the Audit Log Schema

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

To create the 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 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.

Configure an Oracle Data Source for SiteMinder

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

Create an Oracle Data Source on Windows

To create an Oracle data source on Windows

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

3. Select 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 Data Source on Windows

You can configure Oracle RAC 9.2.0.6 and 10.1.0.4 instances with the Policy Server as a single data source name similar to that of a single instance Oracle database. However, the data source name for Oracle RAC is different than a regular ODBC data source.

In an Oracle RAC system, in addition to the SID or ServiceName for each Oracle instance, there is also a ServiceName for the entire Oracle RAC system. When configuring a data source, configure the data source name to use this ServiceName when connecting to an Oracle RAC.

To configure an Oracle RAC data source

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

3. Select 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_se
rvicename[,...])
```

10. Select LoadBalancing.

11. Click OK

The Oracle RAC data source is configured for the wire protocol driver.

Create an Oracle Data Source on UNIX Systems

The SiteMinder ODBC data sources are configured using a `system_odbc.ini` file, which you create by renaming `oraclewire.ini`, located in *policy_server_installation/db*, to `system_odbc.ini`. This `system_odbc.ini` file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [SiteMinder Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding an Oracle Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the `system_odbc.ini` file if you create a new service name or want to use a different driver. You should have entries for the SQL Server or Oracle drivers under [SiteMinder Data Source].

Again, to configure an Oracle data source, you must first create a `system_odbc.ini` file in the *policy_server_installation/db* directory. To do this, you need to rename `oraclewire.ini`, located in *policy_server_installation/db*, to `system_odbc.ini`.

Configure the Oracle Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder should use 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 and rename `oraclewire.ini` to `system_odbc.ini`, which is located in *<policy_server_installation>/db*.

The system_odbc.ini file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the system_odbc.ini file.
2. Depending on the data source you are configuring, edit the applicable data source sections with the following information:

```
Driver=nete_ps_root/odbc/lib/NSora23.so
Description=DataDirect 5.3 Oracle Wire Protocol
LoginID=uid
Password=pwd
HostName=nete_servename
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 to where the 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_servername

Specifies the machine name where the Oracle database is installed.

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 RAC Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder should use 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 and rename oraclewire.ini to system_odbc.ini, which is located in *<policy_server_installation>/db*.

The system_odbc.ini file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the system_odbc.ini file.
2. 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/NSora23.so
Description=DataDirect 5.3 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_servicename1

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 service name for the entire Oracle RAC system.

AlternateServers

Specifies the connection failover to the other Oracle nodes, if the primary server is not accepting connections.

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 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 field of the ODBC Oracle Wire Protocol Driver Setup dialog when you created the Oracle data source or the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog when you created the SQL data source.
 - **UNIX**—this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.
6. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.

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

Note: We recommend retaining the default for best performance.

8. Click Apply.

The settings are saved.

9. Click Test Connection.

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

10. Click OK.

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

Restart the Policy Server

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

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

To restart the Policy Server

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

The Policy Server stops as indicated by the red stoplight.

3. Click Start.

The Policy Server starts as indicated by the green stoplight.

How to Store Token Information in Oracle

To configure an Oracle database as a token store, complete the following procedures:

1. Gather Database Information.
2. Create the Token Store Schema.
3. Configure an Oracle Data Source for SiteMinder.

4. Point the Policy Server to the Database.
5. Restart the Policy Server.

Note: If you are trying to configure or upgrade a SiteMinder store listed in the SiteMinder Platform Support Matrix and cannot find the procedures in this guide, see the *Directory Configuration Guide*.

Gather Database Information

Configuring a single Oracle database to function as a policy store or any other type of 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 SiteMinder data store. You can print the applicable worksheet and use it to record required information before beginning.

More information:

[Oracle Information Worksheet](#) (see page 384)

[Oracle RAC Information Worksheet](#) (see page 384)

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 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 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 Information

Gather the following information only if you are configuring a supported Oracle RAC database as a policy store or any other 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 =
(AADDRESS = PROTOCOL = TCP)(HOST = nete_servername1)(PORT=1521
(AADDRESS = PROTOCOL = TCP)(HOST = nete_servername2)(PORT=1521)
(AADDRESS = 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.

Create the Token Store Schema

You create the token store schema so the Oracle database can store token information.

To create the 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 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_token.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 token store schema is created in the database.

Configure an Oracle Data Source for SiteMinder

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

Create an Oracle Data Source on Windows

To create an Oracle data source on Windows

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

3. Select 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 Data Source on Windows

You can configure Oracle RAC 9.2.0.6 and 10.1.0.4 instances with the Policy Server as a single data source name similar to that of a single instance Oracle database. However, the data source name for Oracle RAC is different than a regular ODBC data source.

In an Oracle RAC system, in addition to the SID or ServiceName for each Oracle instance, there is also a ServiceName for the entire Oracle RAC system. When configuring a data source, configure the data source name to use this ServiceName when connecting to an Oracle RAC.

To configure an Oracle RAC data source

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

3. Select 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 Data Source on UNIX Systems

The SiteMinder ODBC data sources are configured using a system_odbc.ini file, which you create by renaming oraclewire.ini, located in *policy_server_installation/db*, to system_odbc.ini. This system_odbc.ini file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [SiteMinder Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding an Oracle Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the `system_odbc.ini` file if you create a new service name or want to use a different driver. You should have entries for the SQL Server or Oracle drivers under [SiteMinder Data Source].

Again, to configure an Oracle data source, you must first create a `system_odbc.ini` file in the `policy_server_installation/db` directory. To do this, you need to rename `oraclewire.ini`, located in `policy_server_installation/db`, to `system_odbc.ini`.

Configure the Oracle Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder should use 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 and rename `oraclewire.ini` to `system_odbc.ini`, which is located in `<policy_server_installation>/db`.

The `system_odbc.ini` file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the system_odbc.ini file.
2. Depending on the data source you are configuring, edit the applicable data source sections with the following information:

```
Driver=nete_ps_root/odbc/lib/NSora23.so
Description=DataDirect 5.0 Oracle Wire Protocol
LoginID=uid
Password=pwd
HostName=nete_servename
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 to where the 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_servername

Specifies the machine name where the Oracle database is installed.

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 RAC Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder should use 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 and rename oraclewire.ini to system_odbc.ini, which is located in *<policy_server_installation>/db*.

The system_odbc.ini file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the system_odbc.ini file.
2. 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/NSora23.so
Description=DataDirect 5.0 Oracle Wire Protocol
Logon=uid
Password=pwd
HostName=nete_servename1
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_servicename1

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 service name for the entire Oracle RAC system.

AlternateServers

Specifies the connection failover to the other Oracle nodes, if the primary server is not accepting connections.

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 Store 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 Token Data from the Database list.
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 field of the ODBC Oracle Wire Protocol Driver Setup dialog when you created the Oracle data source or the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog when you created the SQL data source.
 - **UNIX**—this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.
5. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
6. Specify the maximum number of database connections allocated to SiteMinder.

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

The settings are saved.
8. Click Test Connection.

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

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

Restart the Policy Server

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

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

To restart the Policy Server

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

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

The Policy Server starts as indicated by the green stoplight.

How to Store 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 SiteMinder.
4. Point the Policy Server to the Database.
5. Restart the Policy Server.

Note: If you are trying to configure or upgrade a SiteMinder store listed in the SiteMinder Platform Support Matrix and cannot find the procedures in this guide, see the *Directory Configuration Guide*.

Gather Database Information

Configuring a single Oracle database to function as a policy store or any other type of 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 SiteMinder data store. You can print the applicable worksheet and use it to record required information before beginning.

More information:

[Oracle Information Worksheet](#) (see page 384)

[Oracle RAC Information Worksheet](#) (see page 384)

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 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 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 Information

Gather the following information only if you are configuring a supported Oracle RAC database as a policy store or any other 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.

Create the Session Store Schema

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

To create the 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 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_ss.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 session store schema is created in the database.

Configure an Oracle Data Source for SiteMinder

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

Create an Oracle Data Source on Windows

To create an Oracle data source on Windows

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

3. Select 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 Data Source on Windows

You can configure Oracle RAC 9.2.0.6 and 10.1.0.4 instances with the Policy Server as a single data source name similar to that of a single instance Oracle database. However, the data source name for Oracle RAC is different than a regular ODBC data source.

In an Oracle RAC system, in addition to the SID or ServiceName for each Oracle instance, there is also a ServiceName for the entire Oracle RAC system. When configuring a data source, configure the data source name to use this ServiceName when connecting to an Oracle RAC.

To configure an Oracle RAC data source

1. Select Start, Programs, Administrative Tools, Data Sources (ODBC).

The ODBC Data Source Administrator appears.

2. Click the System DSN tab, and then click Add.

3. Select 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 Data Source on UNIX Systems

The SiteMinder ODBC data sources are configured using a `system_odbc.ini` file, which you create by renaming `oraclewire.ini`, located in `policy_server_installation/db`, to `system_odbc.ini`. This `system_odbc.ini` file contains all of the names of the available ODBC data sources as well as the attributes that are associated with these data sources. This file must be customized to work for each site. Also, you can add additional data sources to this file, such as defining additional ODBC user directories for SiteMinder.

The first section of the `system_odbc.ini` file, [ODBC Data Sources], contains a list of all of the currently available data sources. The name before the "=" refers to a subsequent section of the file describing each individual data source. After the "=" is a comment field.

Note: If you modify of the first line of data source entry, which is [SiteMinder Data Source], take note of the change because you will need this value when configure your ODBC database as a policy store.

Each data source has a section in the `system_odbc.ini` file describing its attributes. The first attribute is the ODBC driver to be loaded when this data source is used by SiteMinder. The remaining attributes are specific to the driver.

Adding an Oracle Data source involves adding a new data source name in the [ODBC Data Sources] section of the file, and adding a section that describes the data source using the same name as the data source. You need to change the `system_odbc.ini` file if you create a new service name or want to use a different driver. You should have entries for the SQL Server or Oracle drivers under [SiteMinder Data Source].

Again, to configure an Oracle data source, you must first create a `system_odbc.ini` file in the `policy_server_installation/db` directory. To do this, you need to rename `oraclewire.ini`, located in `policy_server_installation/db`, to `system_odbc.ini`.

Configure the Oracle Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder should use 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 and rename `oraclewire.ini` to `system_odbc.ini`, which is located in `<policy_server_installation>/db`.

The system_odbc.ini file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the system_odbc.ini file.
2. Depending on the data source you are configuring, edit the applicable data source sections with the following information:

```
Driver=nete_ps_root/odbc/lib/NSora23.so
Description=DataDirect 5.3 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 to where the 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_servername

Specifies the machine name where the Oracle database is installed.

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 RAC Wire Protocol Driver

You configure the wire protocol driver to specify the settings SiteMinder should use 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 and rename oraclewire.ini to system_odbc.ini, which is located in *<policy_server_installation>/db*.

The system_odbc.ini file contains the following sections. The sections you edit are determined by the data source you are configuring:

[SiteMinder Data Source]

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

[SiteMinder Tokens Data Source]

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

[SiteMinder Logs Data Source]

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

[SiteMinder Keys Data Source]

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

[SiteMinder Session Data Source]

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

[SmSampleUsers Data Source]

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

To configure the wire protocol driver

1. Open the system_odbc.ini file.
2. 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/NSora23.so
Description=DataDirect 5.3 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_servicename1

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 service name for the entire Oracle RAC system.

AlternateServers

Specifies the connection failover to the other Oracle nodes, if the primary server is not accepting connections.

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 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 field of the ODBC Oracle Wire Protocol Driver Setup dialog when you created the Oracle data source or the name you entered in the Data Source field of the ODBC SQL Server Wire Protocol Driver Setup dialog when you created the SQL data source.
 - **UNIX**—this entry must match the first line of the data source entry in the system_odbc.ini file. By default, the first line in the file is [SiteMinder Data Sources]. If you modified the first entry, be sure that you enter the correct value.
4. Enter and confirm the user name and password of the database account that has full access rights to the database instance in the respective fields.
5. Specify the maximum number of database connections allocated to SiteMinder.

Note: We recommend retaining the default for best performance.

6. Click Apply.

The settings are saved.

7. Click Test Connection.

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

8. Click OK.

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

Restart the Policy Server

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

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

To restart the Policy Server

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

The Policy Server stops as indicated by the red stoplight.

3. Click Start.

The Policy Server starts as indicated by the green stoplight.

Sample User Directories

SiteMinder provides schema files that populate a user directory with sample users.

The following schema files are provided in the `<siteminder_home>\db\SQL` directory:

smsampleusers_sqlserver.sql

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

smsampleusers_oracle.sql

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

Note: Creating a sample user directory is optional. More information on configuring user directory connections to the Policy Server exists in 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 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 9: Installing the Administrative UI

This section contains the following topics:

[Installation Road Map](#) (see page 261)
[Administrative UI Installation Options](#) (see page 262)
[Trusted Relationship with a Policy Server](#) (see page 263)
[Administrative UI Installation Checklist](#) (see page 264)
[How to Install the Administrative UI](#) (see page 264)
[How to Register the Administrative UI](#) (see page 272)
[Stop the Application Server](#) (see page 275)
[Administrator Credentials](#) (see page 275)
[Administrative UI High Availability](#) (see page 276)
[How to Configure Additional Policy Server Connections](#) (see page 276)
[Modify the Default Policy Server Connection](#) (see page 281)
[Delete a Policy Server Connection](#) (see page 281)
[Unattended Administrative UI Installation](#) (see page 282)
[Uninstall the Administrative UI on Windows](#) (see page 282)
[Uninstall the Administrative UI on UNIX](#) (see page 283)
[Prepare for Web Agent Installation](#) (see page 284)

Installation Road Map

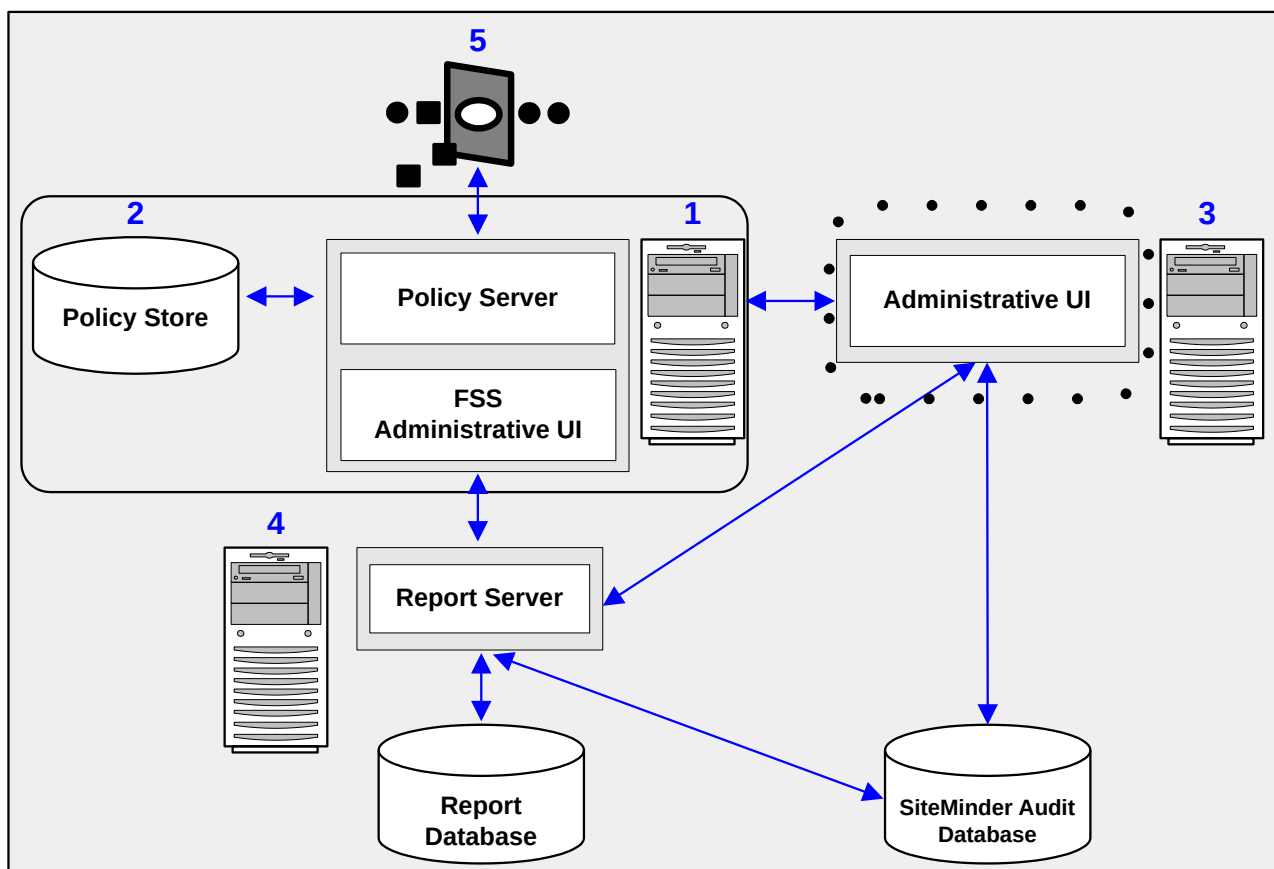
The following diagram illustrates a sample SiteMinder installation and lists the order in which you install and configure each component.

- 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, do not continue with the installation process.

- The component surrounded by the dotted line is the Administrative UI, which you install now.

Note: Once you have installed and registered the Administrative UI, you can prepare for a Web Agent installation, as illustrated by step five.



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 357)

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 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.
- ☐ 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 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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[System Requirements](#) (see page 27)

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

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. Gather information for the installer.
3. (Optional) Reset the registration window.
4. Install the Administrative UI.
5. Register the Administrative UI.

Consider the following:

- After a successful Windows installation, the 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.

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

Note: Worksheets are provided to help you gather and record required information before installing the Administrative UI.

More information:

[Prerequisite Installer Worksheet](#) (see page 385)

Reset the Administrative UI Registration Window

If you used the XPSRegClient utility more than 24 hours ago to submit the SiteMinder super user credentials to the Policy Server, this step is required. The time from which you submit the credentials and attempt to create a trusted relationship with a Policy Server cannot exceed 24 hours.

To reset the registration window

1. Log into 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 SiteMinder administrator. If you are installing the Administrative UI as part of:

- A new r12.0 SP2 environment, specify the default SiteMinder administrator account (siteminder).
- An upgrade, specify any 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 in the policy store, use the smreg utility to create the default SiteMinder account.

passphrase

Specifies the password for the SiteMinder administrator account.

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

-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: 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 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.

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.

Before You Install

Consider the following 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 based on operating system, see the installation and upgrade considerations in 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*.
- **Important!** The installation zip contains the prerequisite installer and the Administrative UI installer.
 - If you are installing to Windows or are installing to UNIX and running the prerequisite installer in GUI-mode, 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 installing to UNIX and running the installation media in console-mode, 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.
- **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
- **Important!** (UNIX) Depending on your permissions, you may need to add executable permissions to the directory that contains the installation media by running the following:

```
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.
- If you are installing the Administrative UI to the same system as the Report Server, port conflicts can occur. By default, both components use port 8080.

More information:

[Locate the Installation Media](#) (see page 456)

[Install the Administrative UI](#) (see page 366)

Windows**To install the Administrative UI on Windows**

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 based on operating system, see the installation and upgrade considerations in 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 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.

UNIX GUI

To install the Administrative UI using a UNIX GUI

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 gui
```

prerequisite_installation_media

Specifies the Administrative UI prerequisite installer executable.

The installer starts.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in 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.

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 272)

UNIX Console

To install the Administrative UI using a UNIX console

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 based on operating system, see the installation and upgrade considerations in 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 272)

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 SiteMinder objects. Registering the Administrative UI creates a trusted connection between the Administrative UI and a Policy Server. Consider the following:

- (UNIX) You are required to start the application server manually and log into the Administrative UI to complete the registration.
- (Windows) The 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. Start the application server.
2. Register the Administrative UI.

More information:

[How to Register the Administrative UI](#) (see page 369)

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 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 357)
[Start the Application Server](#) (see page 372)

Register the Administrative UI

You register the Administrative UI with a Policy Server to begin managing your environment.

To register the Administrative UI

1. Do one of the following:

- **Windows**—Use the Administrative UI shortcut to open the Administrative UI.
- **UNIX**—Open a web browser and go to `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 SiteMinder Administrative UI login screen appears.

2. Type siteminder in the User Name field.
3. Type the siteminder account password in the Password field.
4. 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.

More information:

[Registration Not on File Error Appears](#) (see page 398)

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 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 357)
[Stop the Application Server](#) (see page 374)

Administrator Credentials

By default, the Administrative UI uses the policy store as its source for 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 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 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 SiteMinder administrators are available to all GUIs.

Note: For more information about configuring an external administrator store, see the *Policy Server Configuration Guide*.

More information:

[How to Install the Administrative UI](#) (see page 264)

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.

More information:

[Policy Server Registration Worksheet](#) (see page 387)

Configure the Connection to the Policy Server

You configure the connection so the Administrative UI can be used to manage 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.

Unattended Administrative UI Installation

After the Administrative UI is installed on one system, you can reinstall it or install it on a separate system using an unattended installation. An unattended installation lets you install or uninstall the Administrative UI without any user interaction.

To configure an unattended installation, the installer provides properties files that let you define installation variables. The default parameters, passwords, and paths in these files reflect the information you entered during the initial Administrative UI installation.

More information:

[How to Silently Install the Administrative UI](#) (see page 422)

Uninstall the Administrative UI on Windows

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*.

To uninstall the Administrative UI

1. Stop the application server.
2. Open the Windows Control Panel and double-click Add/Remove Programs.
A list of installed programs appears.
3. Select CA SiteMinder Administrative UI and click Change/Remove.

Note: If you upgraded the Administrative UI from r12.0 SP1, CA SiteMinder Web Access Manager Administrative UI is listed in addition to CA SiteMinder Administrative UI. Select CA SiteMinder Administrative UI to uninstall the Administrative UI after an upgrade.

The process to remove the Administrative UI starts.

4. Follow the instructions and prompts in the wizard.
Note: If the system displays a message prompting you to remove shared file, click No to All.
5. If requested, reboot the system.
6. Open the Windows Control Panel and double-click Add/Remove Programs.
A list of installed programs appears.

7. Select Prerequisite Installer and click Change/Remove.
8. The process to remove the Administrative UI prerequisite components starts.
Note: If the system displays a message prompting you to remove shared file, click No to All.
9. 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 357)

Uninstall the Administrative UI on UNIX

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](#).

To uninstall the Administrative UI on UNIX

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 357)

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 SiteMinder Administrator that has the right to register trusted hosts**—A trusted host is a client computer where one or more SiteMinder Web Agents are installed. The term trusted host refers to the physical system. There must be an administrator with the permission to register trusted hosts. The default 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 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 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 SiteMinder. When users need to access resources on an IIS web server protected by SiteMinder, they may not have the necessary server access privileges. The Web Agent must use the Windows account, which is previously assigned by an administrator, to act as a proxy user account for users granted access by 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 10: Registering the Federation Security Services Administrative UI

This section contains the following topics:

[Registering the FSS Administrative UI](#) (see page 287)

[Installation Road Map](#) (see page 288)

[Pre-registration Checklist](#) (see page 289)

[Before You Register the FSS Administrative UI](#) (see page 289)

[How to Register the FSS Administrative UI](#) (see page 290)

Registering the FSS Administrative UI

The FSS Administrative UI is an applet-based application that is installed with the Policy Server and is used to manage Federation Security Services. Federation Security Services components consist of the affiliates (consumers, service providers, resource partners) and SAML authentication schemes that you configure to support federated communication between two partners.

The intent of the FSS Administrative UI is to let you manage SiteMinder Federation Security Services. If you are familiar with previous versions of the SiteMinder Policy Server User Interface, you will notice that all SiteMinder objects appear in the FSS Administrative UI. The only objects that do not appear are objects related to Enterprise Policy Management (EPM) and reports. You can use the FSS Administrative UI to manage the SiteMinder objects. If you need information while using the FSS Administrative UI, consult the FSS Administrative UI online help system.

You register the FSS Administrative UI with the Policy Server to ensure that the communication between both components is FIPS-encrypted (AES encryption).

Note: If your organization is not federating with a partner, you may safely leave the FSS Administrative UI on the Policy Server machine without registering it with the Policy Server.

Installation Road Map

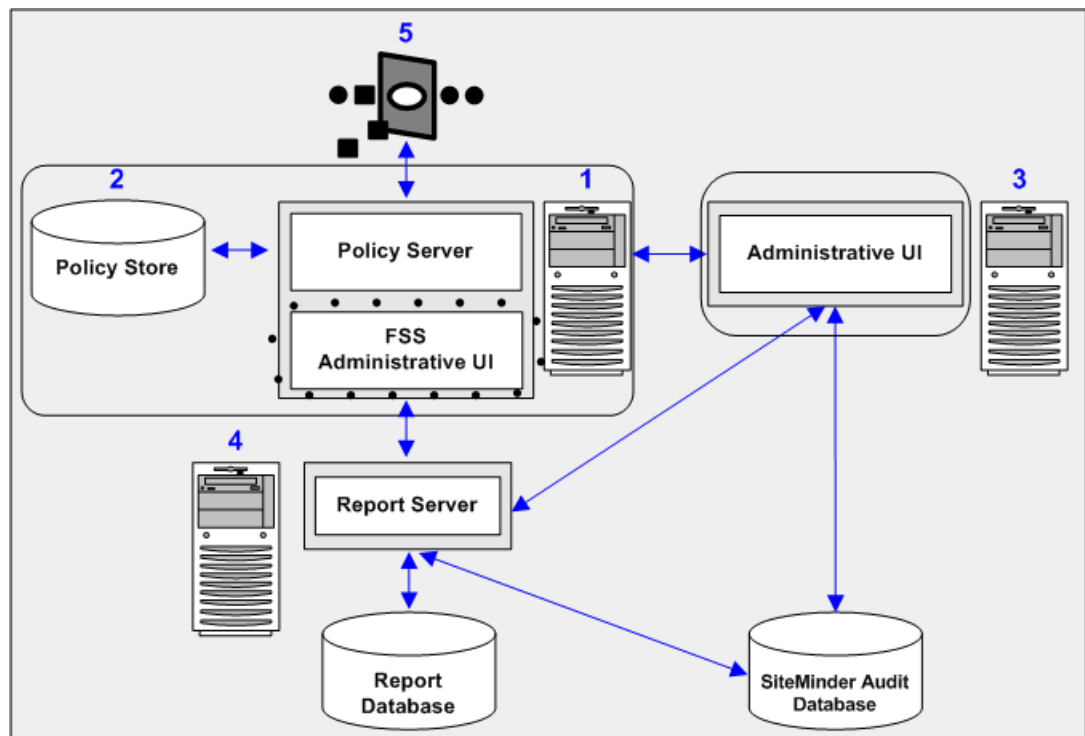
The following diagram illustrates a sample SiteMinder installation and lists the order in which you install and configure each component.

- Solid lines surround the components that are required before registering the FSS Administrative UI. They include:
 - A Policy Server
 - A policy store
 - An installed and registered Administrative UI
 - A non-registered FSS Administrative UI

Note: The FSS Administrative UI is installed with the Policy Server.

- The component surrounded by the dotted line is the FSS Administrative UI, which you register with the Policy Server now.

Note: A registered FSS Administrative UI is only required to manage Federation Security Services. If your organization is not federating with a partner, you can safely leave the Federation Security Services on the Policy Server system without registering it with the Policy Server.



Pre-registration Checklist

You may want to print the following to use as a checklist to help ensure that you have the required SiteMinder components and information to register the FSS Administrative UI with the Policy Server:

- ☐ Ensure that the Administrative UI is installed and configured. You register the FSS Administrative UI using the Administrative UI.
- ☐ Ensure that the Administrative user account you will use to access the Administrative UI has the necessary privileges to create an agent. You create a 4.x Agent during the FSS Administrative UI registration process.
- ☐ Ensure that you have the default SiteMinder Super User account password. You log in to the FSS Administrative UI to confirm the registration process.

Note: The default SiteMinder Super User account is SiteMinder. The default SiteMinder Super User account password was created when the policy store was configured. If you do not have the password, you may change it using the smreg utility. More information on using the smreg utility exists in the *Policy Server Administration Guide*.

- ☐ If you are registering the FSS Administrative UI as part of an upgrade to r12.0 SP2, ensure that you have upgraded the policy store to r12.0 SP2. You should not begin using the FSS Administrative UI to manage Federation Security Services until the policy store is upgraded to r12.0 SP2.

Before You Register the FSS Administrative UI

Do the following before you register the FSS Administrative UI:

- (Internet Explorer) If you are using a supported version of Internet Explorer, add your domain as a trusted site before accessing the FSS Administrative UI.

Consider the following when adding your domain as a trusted site:

- Enter the full name of the server, including the domain.

Example: http://servername.domain-name

Example: http://security.myorg.org

- If you are connecting to the FSS Administrative UI using a secured connection (https), you must include https when specifying the domain.

Example: https://security.myorg.org

- If you are not accessing the Policy Server using a secured connection (https), you may disable the Require server verification (https) for all sites in this zone setting.

Note: For more information about adding a domain as a trusted site, see the Internet Explorer documentation.

- (Netscape Communicator) If you are using a supported version Netscape Communicator, you can reduce the time the FSS Administrative UI takes to load by copying FSS Administrative UI `sm_admin_noswing.jar` file to the directory where the Netscape Java classes are located. The `sm_admin_noswing.jar` file is located in *policy_server_home*\admin.

policy_server_home

Specifies the Policy Server installation location.

Note: For more information about where Netscape Java classes are located, see your Netscape documentation.

- (Windows) When launching the FSS Administrative UI, the URL assumes that you are running the Web server at the default port 80. If the Web server is not running on the default port, or if you change the Web server port, modify the FSS Administrative UI shortcut in the Start menu before accessing the FSS Administrative UI.
- Accessing the FSS Administrative UI locally reduces the time it takes to load. If you access the FSS Administrative UI from Internet Explorer, the FSS Administrative UI files, which are stored in `sm_admin.cab`, are automatically stored in Internet Explorer's cache.

Note: For a list of supported CA and third-party components, refer to the SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

How to Register the FSS Administrative UI

Complete the following steps to register the FSS Administrative UI with the Policy Server:

1. Review pre-requisite considerations in Before you Register the FSS Administrative UI.
2. Create the registration credentials for the FSS Administrative UI.
3. Log into the FSS Administrative UI.

Create the Registration Credentials for the FSS Administrative UI

In addition to the SiteMinder Super User administrator account credentials, which were established when you installed the Policy Server and configured the policy store, the FSS Administrative UI login screen also requires the name and shared secret of a 4.x Agent. You establish these credentials to ensure that the communication between the FSS Administrative UI and the Policy Server is FIPS-encrypted (AES encryption).

Note: Creating a 4.x Agent identity to log into the FSS Administrative UI does not require that you to install a SiteMinder Web Agent, configure a Host Configuration Object and Agent Configuration object, or register a trusted host. The FSS Administrative UI only requires the 4.x Agent identity.

To create the 4x agent

1. Log into the Administrative UI.
2. Click Infrastructure, Agents.
3. Click Agent, Create Agent.

The Create Agent screen appears. The create new object radio button is selected.

4. Click OK.

Agent-related properties appear.

5. Enter an Agent name in the Agent Name field.

Example: FSS UI Agent

Note: Record the Agent name as it is required to log into the FSS Administrative UI.

6. Select the Supports 4.x agents check box in the Agent Type Settings group box.

The Trust Settings group box appears.

7. Enter the IP Address of the machine hosting the Policy Server in the IP Address field.
8. Enter and confirm the Agent shared secret in the Shared Secret and Confirm Shared Secret fields.

Note: Record the Agent shared secret as it is required to log into the FSS Administrative UI.

You have created the required 4.x Agent credentials and may log into the FSS Administrative UI.

Log into the FSS Administrative UI

You log into the FSS Administrative UI to complete the registration process.

To log into the FSS Administrative UI

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

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

2. Complete one of the following
 - Enter `http://hostname:port/siteminder` in a supported browser.

hostname:port

Specifies the name of the machine on which the Policy Server is installed. The port is the port number of the Web server. You do not need to enter a port number if you are using the default port (80) for HTTP requests.

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

- From the Start menu, select Start, Programs, siteminder, SiteMinder FSS Administrative UI

The FSS Administrative UI login screen appears.

Note: If the login screen does not appear, refer to Federation Security Services Administrative UI Troubleshooting.

3. Click Login.

Note: If you are prompted to trust or grant permissions to the signed applet delivered by CA, click Yes.

The SiteMinder FSS Administrative UI login screen appears.

4. Enter the following information:
 - SiteMinder in the Username field
 - The password for the SiteMinder Super User account in the Password field.
 - The name of the 4.x Agent identity you created in the Host Name field.
 - The shared secret of the 4.x Agent identity you created in the Passphrase field.

5. Click Login.

The FSS Administrative UI opens.

Note: We recommend that the default SiteMinder Super User account not be used in day-to-day operations. Instead, create an administrator with system configuration privileges. More information on creating a FSS Administrative UI administrator exists in the *FSS Administrative UI Help* system.

Chapter 11: Installing Reports

This section contains the following topics:

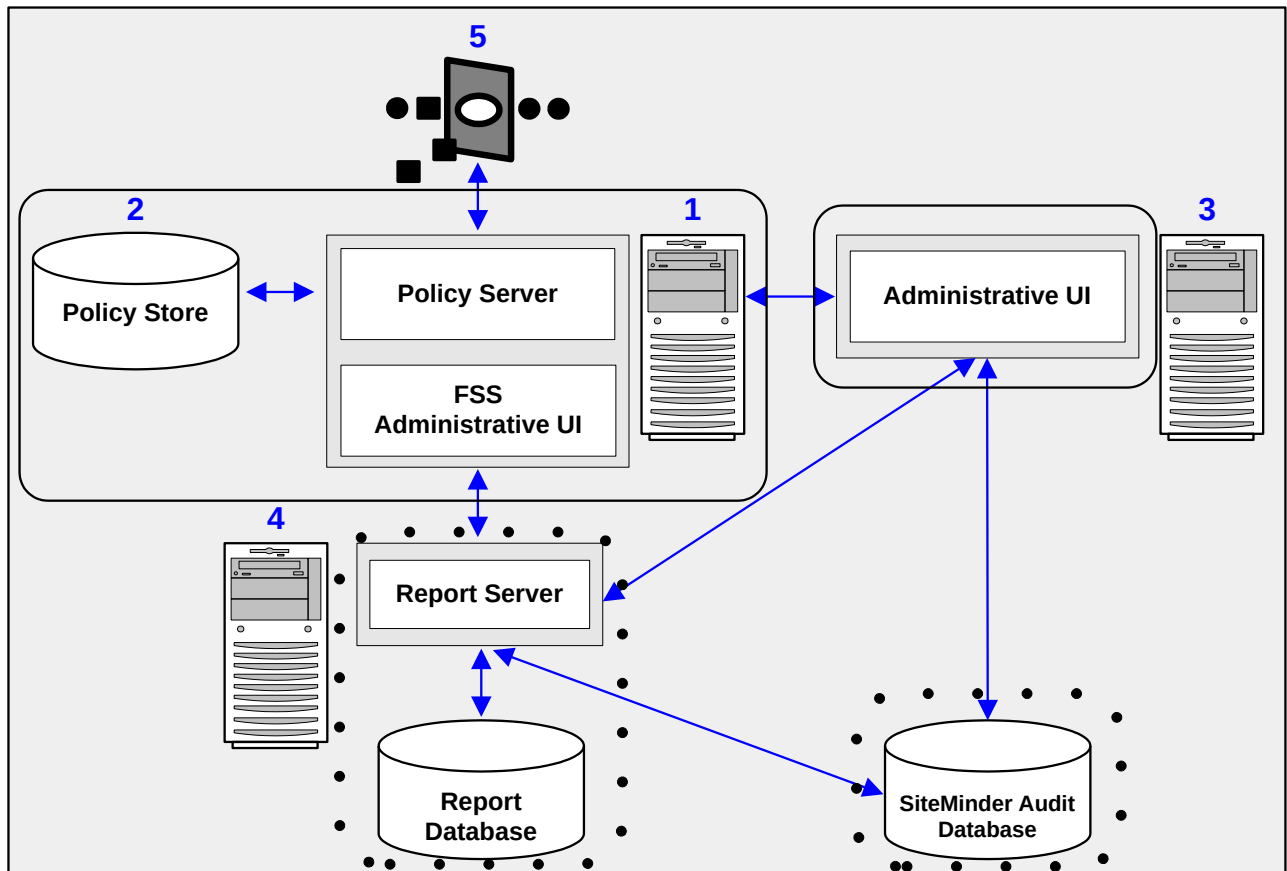
- [Installation Road Map](#) (see page 295)
- [Report Server Installation Options](#) (see page 297)
- [Reporting Installation Checklists](#) (see page 297)
- [Reporting Considerations](#) (see page 300)
- [How the Reports Installation Works](#) (see page 301)
- [How to Install the Report Server](#) (see page 302)
- [How to Install the Report Templates](#) (see page 317)
- [How to Register the Report Server](#) (see page 324)
- [How to Configure an Audit Database](#) (see page 331)
- [Stop the Report Server](#) (see page 334)
- [How to Uninstall Reporting](#) (see page 335)
- [Delete a Report Server Connection to the Administrative UI](#) (see page 338)
- [Reinstall the Report Server](#) (see page 339)

Installation Road Map

The following diagram illustrates a sample 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:
 - 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:
 - The Report Server
 - A report database

- A SiteMinder audit database.



More information:

[Policy Server](#) (see page 16)

[Policy Store](#) (see page 17)

[Administrative User Interfaces Overview](#) (see page 20)

[CA Business Intelligence](#) (see page 18)

[SiteMinder Audit Database](#) (see page 19)

Report Server Installation Options

Two installation options are available:

- **Typical**—The typical installation lets you install the Report Server using an embedded version of MySQL and Apache Tomcat to function as a report database and web server, respectively.
- **Custom**—The custom installation lets you configure a supported version of SQL Server or Oracle to function as the report database.

Important! Although a custom installation lets you configure an existing instance of MySQL and additional application server types, SiteMinder only supports the embedded version of MySQL and Apache Tomcat. If you install using the custom installation option, be sure to configure only SQL Server or Oracle as a report database and only install the embedded version of Apache Tomcat.

Note: For a list of supported CA and third-party components, refer to the SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

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 29)
 - [UNIX](#) (see page 30)
- ☐ (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 31).

- ❑ 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 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
 - 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 you are using a supported database to function as the [report database](#) (see page 30).

- ❑ If you are not using the embedded version of MySQL, be sure that the database client and server are configured to use UTF8 character encoding.

Note: 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, do the following on the Report Server host system:
 - Be sure that a 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 on the Report Server host system:
 - Be sure that a supported Oracle Net client is installed on the Report Server host system.
 - 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.

- ❑ (Oracle) If you are using Oracle Net client to connect to the report database or an audit database, do the following on the Report Server host system:

- 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

Reporting Considerations

Consider the following before installing the Report Server:

- Installing the Report Server can take up to three hours.
- 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:

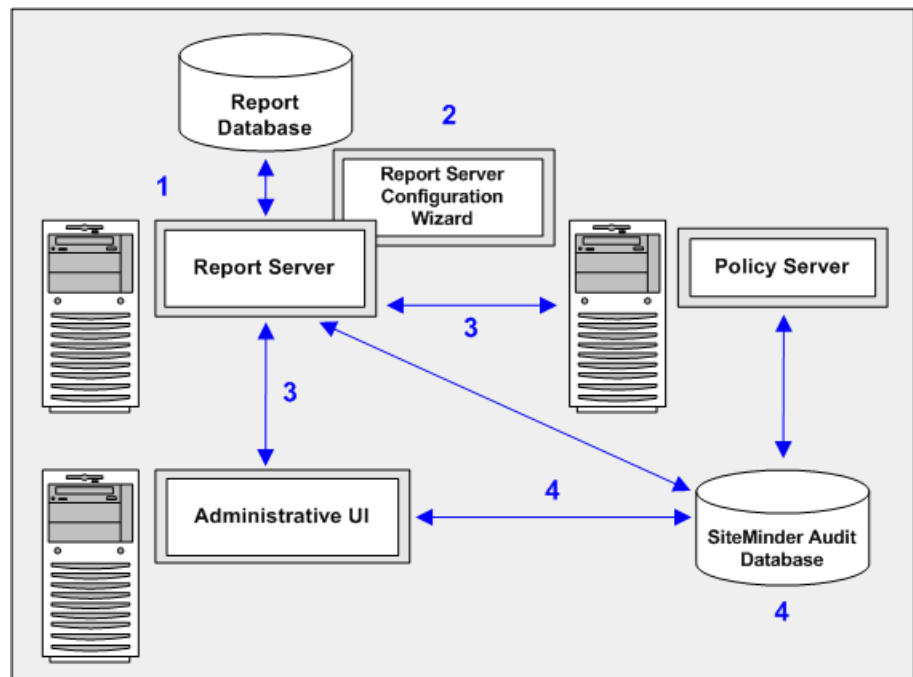
[Administrative UI Installation Options](#) (see page 262)

[Start the Application Server](#) (see page 273)

[Stop the Application Server](#) (see page 275)

How the Reports Installation Works

The SiteMinder reporting feature requires that you install and configure a Report Server, a report database, and a SiteMinder audit database to manage SiteMinder policy analysis and audit-based reports. The following diagram details a sample 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 Server is the first step in the process. You configure a report database during the installation.
2. **Install the SiteMinder report templates**—Installing the SiteMinder report templates is the second step in the process. The SiteMinder Report Server Configuration Wizard configures the Report Server to use a set of 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 SiteMinder audit database**—Configuring a SiteMinder audit database is the fourth step in the process. A separate 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.

Note: Worksheets are provided to help you gather and record required information before installing and registering the Report Server.

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 BusinessObjects administrator account (administrator). This administrator account is used to import SiteMinder report templates and to access Business Objects Java InfoView. Business Objects Java InfoView is the Report Server user interface. Determine the password for this account.

Consider the following password 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

More information:

[Installation Credentials Worksheet](#) (see page 387)

MySQL Report Database

If you are using the embedded version of MySQL to function as the report database, the installer requires the following information:

- **MySQL root password**—Identify the password for the MySQL root user.
- **User name**—Identify the user ID of the database user account that is to manage the report database.
- **Password**—Identify the user account password.
- **Database name**—Identify the name of the report database instance.

More information:

[MySQL Report Database Worksheet](#) (see page 388)

SQL Server Report Database

If you are using a supported version of Microsoft SQL Server to function as the report database, the installer requires the following information:

- **Database Name**—Identify the name of the database instance that is to function as the report database.
- **Data Source Name (DSN)**—Identify the name of the DSN that Report Server is to use to communicate with the report database.

- **User Name**—Identify the name of the database user account that has the necessary privileges to read and write to the report database.
- **Password**—Identify the password for the database user account that has the necessary privileges to read and write to the report database.

More information:

[SQL Server Report Database Worksheet](#) (see page 388)

Oracle Report Database

If you are using a supported version of Oracle to function as a report databases, the installer requires the following information:

- **Oracle Net Client Service Name**—Identify the service name that the Report Server is to use to communicate with the report database.
Note: The installer refers to the Oracle Net Client Service Name as the Transparent Network Substrate (TNS) Service Name.
- **User Name**—Identify the name of the database user account that has the necessary privileges to read and write to the report database.
- **Password**—Identify the password for the database user account that has the necessary privileges to read and write to the report database.

More information:

[Oracle Report Database Worksheet](#) (see page 388)

Apache Tomcat Installation

The installer installs an embedded version of Apache Tomcat. Gather the following installation settings:

- **Connection port**—Identify the port to which Apache Tomcat must connect.
Default: 8080
- **Redirect port**—Identify the port to which Apache Tomcat must redirect requests.
Default: 8443
- **Shutdown port**—Identify the port to which the Apache Tomcat SHUTDOWN command must be issued.
Default: 8005

More information:

[Apache Tomcat Worksheet](#) (see page 389)

Install the Report Server

The following sections detail how to install the Report Server on Windows and UNIX.

Before You Install

Consider the following before you install 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 based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.
- You install the Report Server using the typical or custom installation option. The type of report database you need to configure determines the installation option to use.
- **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) Depending on your permissions, you may need to add executable permissions to the directory that contains the installation media by running the following:

```
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.

More information:

[Locate the Installation Media](#) (see page 456)

[Report Server Installation Options](#) (see page 297)

Windows Typical Installation

To install the Report Server on Windows

1. Be sure that you have reviewed the [installation checklists](#) (see page 297).
2. Be sure that you have gathered the [required information for the installer](#) (see page 302).
3. Exit all applications that are running.

4. Navigate to Disk1\InstData\VM and double-click *installation_media*.

installation_media

Specifies the Report Server installation executable.

The installer starts and prompts you for a locale.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

5. Select English from the drop-down list and click OK.

The installer introduction appears.

6. Click Next.

The license agreement appears.

7. Accept the license agreement and click Next.

The installer prompts you for an installation type.

8. Click Typical and click Next.

The installer prompts you for an installation location.

9. Specify the installation location and click Next.

The installer prompts you for a BusinessObjects Administrator password.

10. Use your completed installation credentials worksheet to enter the required value and click Next.

The installer prompts you for Apache Tomcat information.

11. Use your completed Apache Tomcat worksheet to enter the required values and click Next.

The installer prompts you for MySQL information.

12. Use your completed MySQL report database worksheet to enter the required values and click Next.

The installer prompts you to enable auditing.

13. Select No and click Next.

Note: The Report Server audit database is used to audit activities specific to the Report Server and is not used for SiteMinder audit-based reports. A SiteMinder audit database is required to run audit-based reports.

The installation summary appears.

14. (Optional) Click Create Response File to save a silent installation properties file with the current installation settings.

15. Review the installation settings and click Install.

The Report Server is installed.

UNIX GUI Typical Installation

To install the Report Server on Windows

1. Be sure that you have reviewed the [installation checklists](#) (see page 297).
2. Be sure that you have gathered the [required information for the installer](#) (see page 302).
3. Exit all applications that are running.
4. Open a Bourne shell and navigate to the CABI folder.
5. Enter the following command:

```
.installation_media gui
```

installation_media

Specifies the Report Server installation executable.

The installer starts and prompts you for a locale.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

6. Select English from the drop-down list and click OK.

The installer introduction appears.

7. Click Next.

The license agreement appears.

8. Accept the license agreement and click Next.

The installer prompts you for an installation type.

9. Click Typical and click Next.

The installer prompts you for non-root user credentials.

10. Use your completed installation credentials worksheet to enter the required value and click Next.

The installer prompts you to specify the common reporting installation path.

11. Type a value and click Next.

Note: By default, the shared components directory and the common reporting directory values are the same. These values do not have to be the same.

The installer prompts you for a BusinessObjects Administrator password.

12. Use your completed installation credentials worksheet to enter the required value and click Next.

The installer prompts you for Apache Tomcat information.

13. Use your completed Apache Tomcat worksheet to enter the required values and click Next.

The installer prompts you for MySQL information.

14. Use your completed MySQL report database worksheet to enter the required values and click Next.

The installer prompts you to enable auditing.

15. Select No and click Next.

Note: The Report Server audit database is used to audit activities specific to the Report Server and is not used for SiteMinder audit-based reports. A SiteMinder audit database is required to run audit-based reports.

The installation summary appears.

16. (Optional) Click Create Response File to save a silent installation properties file with the current installation settings.

17. Review the installation settings and click Install.

The Report Server is installed.

UNIX Console Typical Installation

To install the Report Server on Windows

1. Be sure that you have reviewed the [installation checklists](#) (see page 297).
2. Be sure that you have gathered the [required information for the installer](#) (see page 302).
3. Exit all applications that are running.
4. Open a Bourne shell and navigate to the CABI folder.
5. Enter the following command:

```
.installation_media -i console
```

installation_media

Specifies the Report Server installation executable.

The installer starts and prompts you for a locale.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

6. Type the value for English and press Enter.

The installer introduction appears.

7. Press Enter.

The license agreement appears.

8. Do the following:

- a. Press Enter to advance the license agreement.
- b. Type y to accept the license agreement.
- c. Press Enter.

The installer prompts you for an installation type.

9. Type the value for Typical and press Enter.

The installer prompts you for non-root user credentials.

10. Use your completed installation credentials worksheet to enter the required value and press Enter.

The installer prompts you to specify the common reporting installation path.

11. Type a value and press Enter.

Note: By default, the shared components directory and the common reporting directory values are the same. These values do not have to be the same.

The installer prompts you for a BusinessObjects Administrator password.

12. Use your completed installation credentials worksheet to enter the required value and press Enter.

The installer prompts you for Apache Tomcat information.

13. Use your completed Apache Tomcat worksheet to enter the required values and press Enter.

The installer prompts you for MySQL information.

14. Use your completed MySQL report database worksheet to enter the required values and press Enter.

The installer prompts you to enable auditing.

15. Type n and press Enter.

Note: The Report Server audit database is used to audit activities specific to the Report Server and is not used for SiteMinder audit-based reports. A SiteMinder audit database is required to run audit-based reports.

The installation summary appears.

16. (Optional) Save a silent installation properties file with the current installation settings.

17. Review the installation settings and press Enter.

The Report Server is installed.

Windows Custom Installation

To install the Report Server on Windows

1. Be sure that you have reviewed the [installation checklists](#) (see page 297).
2. Be sure that you have gathered the [required information for the installer](#) (see page 302).
3. Exit all applications that are running.
4. Navigate to Disk1\InstData\VM and double-click *installation_media*.

installation_media

Specifies the Report Server installation executable.

The installer starts and prompts you for a locale.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

5. Select English from the drop-down list and click OK.

The installer introduction appears.

6. Click Next.

The license agreement appears.

7. Accept the license agreement and click Next.

The installer prompts you for an installation type.

8. Click Custom and click Next.

The installer prompts you for an installation location.

9. Specify the installation location and click Next.

The installer prompts you for a BusinessObjects Administrator password.

10. Use your completed installation credentials worksheet to enter the required value and click Next.

The installer prompts you for a report database type.

11. Select Use Existing DBMS and select a supported database type.

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 SiteMinder does not. For a list of supported database types and versions, see the SiteMinder r12.0 SP2 Platform Support Matrix.

The installer prompts you for database-specific values.

12. Use your completed report database worksheet to enter the required values and click Next.

The installer prompts you to enable auditing.

13. Select No and click Next.

Note: The Report Server audit database is used to audit activities specific to the Report Server and is not used for SiteMinder audit-based reports. A SiteMinder audit database is required to run audit-based reports.

The installer prompts you for a web server configuration

14. Select Yes and click Next.

Note: This installs an embedded version of Tomcat. SiteMinder only supports this web server type and version.

The installer prompts you for web server configuration settings.

15. Use your completed Apache Tomcat worksheet to enter the required values and click Next.

The installer prompts you to configure sample databases and templates.

16. Select No and click Next.

Note: The SiteMinder Report Server Configuration wizard installs the required reporting templates. You run the wizard after installing the Report Server.

The installation summary appears.

17. (Optional) Click Create Response File to save a silent installation properties file with the current installation settings.

18. Review the installation settings and click Install.

The Report Server is installed.

More information:

[Locate the Installation Media](#) (see page 456)

[Reporting Worksheets](#) (see page 387)

UNIX GUI Custom Installation

To install the Report Server using a UNIX GUI

1. Be sure that you have reviewed the [installation checklists](#) (see page 297).
2. Be sure that you have gathered the [required information for the installer](#) (see page 302).
3. Be sure that you are using a root-user account.
4. Exit all applications that are running.

5. Open a Bourne shell and navigate to the CABI folder.

6. Enter the following command:

```
.installation_media gui
```

installation_media

Specifies the Report Server installation executable.

The installer starts and prompts you for a locale.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

7. Select English and click OK.

The installer introduction appears.

8. Click Next.

The license agreement appears.

9. Accept the license agreement and click Next.

The installer prompts you for an installation type.

10. Click Custom and then click Next.

The installer prompts you for non-root user credentials.

11. Use your completed installation credentials worksheet to enter the required values and click Next.

The installer prompts you to specify the common reporting installation path.

12. Type a value and click Next.

Note: By default, the shared components directory and the common reporting directory values are the same. These values do not have to be the same.

The installer prompts you for the Central Management Service (CMS) port.

13. Leave the default value and click Next.

The installer prompts you for a BusinessObjects Administrator password.

14. Use your completed installation credentials worksheet to enter the required value and click Next.

The installer prompts you for a report database type.

15. Do the following:

- a. Select Use Existing DBMS.
- b. Select a supported database type.
- c. Click Next.

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 SiteMinder does not. For a list of supported database types and versions, see the SiteMinder r12.0 SP2 Platform Support Matrix.

The installer prompts you for database-specific values.

16. Use your completed report database worksheet to enter the required values and click Next.

The installer prompts you to enable auditing.

17. Select No and click Next.

Note: The Report Server audit database is used to audit activities specific to the Report Server and is not used for SiteMinder audit-based reports. A SiteMinder audit database is required to run audit-based reports.

The installer prompts you for a web server configuration.

18. Select Yes and click Next.

Note: This installs an embedded version of Tomcat. SiteMinder only supports this web server type and version.

The installer prompts for web server configuration settings.

19. Use your completed Apache Tomcat worksheet to enter the required values and click Next.

The installer prompts you to configure sample databases and templates.

20. Select No and click Next.

Note: The SiteMinder Report Server Configuration wizard installs the required reporting templates. You run the wizard after installing the Report Server.

The installation summary appears.

21. (Optional) Click Create Response File to save a silent installation properties file with the current installation settings.

22. Review the installation summary and click Install.

The Report Server is installed.

More information:

[Locate the Installation Media](#) (see page 456)

[Reporting Worksheets](#) (see page 387)

UNIX Console Custom Installation

To install the Report Server with a UNIX console

1. Be sure that you have reviewed the [installation checklists](#) (see page 297).
2. Be sure that you have gathered the [required information for the installer](#) (see page 302).
3. Be sure that you are using an account with root-user privileges.
4. Exit all applications that are running.
5. Open a Bourne shell and navigate to the CABI folder.
6. Enter the following command:

```
.installation_media -i console
```

installation_media

Specifies the Report Server installation executable.

The installer starts and prompts you for a locale.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

7. Type the value for English and press Enter.
The installer introduction appears.
8. Press Enter.
The license agreement appears.
9. Do the following:
 - a. Press Enter to advance the license agreement.
 - b. Type y to accept the license agreement.
 - c. Press Enter.The installer prompts you for an installation type.
10. Type the value for Custom and press Enter.
The installer prompts you for non-root user credentials.
11. Use your completed installation credentials worksheet to enter the required values and press Enter.
The installer prompts you to specify the common reporting installation path.

12. Type a value and press Enter.

Note: By default, the shared components directory and the common reporting directory values are the same. These values do not have to be the same.

The installer prompts you for the Central Management Service (CMS) port.

13. Leave the default value and press Enter.

The installer prompts you for a BusinessObjects Administrator password.

14. Use your completed installation credentials worksheet to enter the required value and press Enter.

The installer prompts you for a report database type.

15. Do the following:

- a. Type the value for Use Existing DBMS.
- b. Type the value for a supported database type.
- c. 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 SiteMinder does not. For a list of supported database types and versions, see the SiteMinder r12.0 SP2 Platform Support Matrix.

The installer prompts you for database-specific values.

16. Use your completed report database worksheet to enter the required values and press Enter.

The installer prompts you to enable auditing.

17. Type n and press Enter.

Note: The Report Server audit database is used to audit activities specific to the Report Server and is not used for SiteMinder audit-based reports. A SiteMinder audit database is required to run audit-based reports.

The installer prompts you for a web server configuration.

18. Type y and press Enter.

Note: This installs an embedded version of Tomcat. SiteMinder only supports this web server type and version.

The installer prompts you for web server configuration settings.

19. Use your completed Apache Tomcat worksheet to enter the required values and press Enter.

The installer prompts you to install sample databases and templates.

20. Type n and press Enter.

Note: The SiteMinder Report Server Configuration wizard installs the required reporting templates. You run the wizard after installing the Report Server.

The installation summary appears.

21. (Optional) Save a silent installation properties file with the current installation settings.

22. Review the installation settings and press Enter.

The Report Server is installed.

More information:

[Locate the Installation Media](#) (see page 456)

[Reporting Worksheets](#) (see page 387)

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. Start the Report Server.
3. Install the report templates.
4. Restart the Report Server.
5. 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.
- **SiteMinder audit database type**—Identify the type of database that is to function as a SiteMinder audit database. A separate 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 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.

More information:

[Report Server Configuration Worksheet](#) (see page 389)

Start the Report Server

To start the Report Server on Windows

1. Click Start, Programs, BusinessObjects XI Release 2, BusinessObjects Enterprise, Central Configuration Manager.

The Central Configuration Manager console appears.

2. Start all services, except World Wide Web Publishing Services.

The Report Server is started.

To start the Report Server on UNIX

1. Log into 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_home*/CommonReporting/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*/CommonReporting.

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 *report_server_home*/CommonReporting.

report_server_home

Specifies the Report Server installation path.

5. Navigate to `report_server_home/CommonReporting/bobje`

`report_server_home`

Specifies the Report Server installation path.

6. Run the following command:

```
./startServers
```

The Report Server is started.

Install the Report Templates

You install the 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 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 based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

- **Important!** (UNIX) Depending on your permissions, you may need to add executable permissions to the installation media by running the following command:

```
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.

More information:

[Locate the Installation Media](#) (see page 456)

Windows

To install the report templates on Windows

1. Be sure that you have gathered the [required information for the installer](#) (see page 317).
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 based on operating system, see the installation and upgrade considerations in 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 SiteMinder report templates.

More information:

[Locate the Installation Media](#) (see page 456)

[Report Server Configuration Worksheet](#) (see page 389)

[Restart the Report Server](#) (see page 329)

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 317).
2. Exit all applications that are running.
3. Open a shell and navigate the installation media.

4. Enter the following command:

```
.installation_media gui
```

installation_media

Specifies the name of the Report Server Configuration Wizard installation executable.

The installer starts.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in 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 SiteMinder report templates.

More information:

[Locate the Installation Media](#) (see page 456)

[Report Server Configuration Worksheet](#) (see page 389)

[Restart the Report Server](#) (see page 329)

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 317).
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 based on operating system, see the installation and upgrade considerations in 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 SiteMinder report templates.

More information:

[Locate the Installation Media](#) (see page 456)

[Report Server Configuration Worksheet](#) (see page 389)

[Restart the Report Server](#) (see page 329)

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

To increase the default timeout value of the Crystal Reports Job Server service

1. Click Start, Programs, BusinessObjects XI Release 2, 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 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

To increase the default timeout value of the Crystal Reports Job Server service

1. Navigate to *report_server_home*/CommonReporting/bobje.

report_server_home

Specifies the Report Server installation path.

2. Open the ccm.config file, and append the following 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.

More information:

[Report Server Registration Worksheet](#) (see page 389)

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.

To configure the connection to the Policy Server

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\CommonReporting

Default: (UNIX) /opt/CA/SharedComponents/CommonReporting

2. Run one of the following commands:

- (Windows)

```
regreportserver.bat -pshost host_name -client client_name -passphrase passphrase -psport portnum  
-fipsmode 0|1
```

- (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 SiteMinder when using the XPSRegClient utility, enter 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

To restart the Report Server on Windows

1. Click Start, Programs, BusinessObjects XI Release 2, BusinessObjects Enterprise, Central Configuration Manager.

The Central Configuration Manager console appears.

2. Stop all services, except World Wide Web Publishing Services.

The Report Server stops.

3. Start all services, except World Wide Web Publishing Services.

The Report Server is restarted.

To restart the Report Server on UNIX

1. Log into 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_home/CommonReporting/bobje` and run the following command:

```
./stopServers
```

report_server_home

Specifies the Report Server installation path.

The Report Server stops.

4. 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

5. Navigate to `report_server_home/CommonReporting/external/scripts` and run the following command:

```
./setupenv.sh
```

report_server_home

Specifies the Report Server installation path.

6. Be sure that:

- The IAM_RPTSRV_HOME variable is set to:

report_server_home/CommonReporting.

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 *report_server_home/CommonReporting.*

report_server_home

Specifies the Report Server installation path.

7. Navigate to *report_server_home/CommonReporting/bobje* and run the following command:

./startServers

report_server_home

Specifies the Report Server installation path.

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 SiteMinder audit database is required to run 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 SiteMinder r12.0 SP2 Platform Support Matrix.

Complete the following steps to configure an audit database:

1. (Optional) If you have not already done so, configure a 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.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

[How to Store Audit Logs in Oracle](#) (see page 224)

[How to Store Audit Logs in SQL Server](#) (see page 193)

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 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 into 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.
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.
 - **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.
8. Enter the port on which the audit database server is listening in the Database Server Port field.
9. Complete one of the following:
 - **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 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 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 r12.0 SP2 SiteMinder Platform Support Matrix.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Stop the Report Server

To stop the Report Server on Windows

1. Click Start, Programs, BusinessObjects XI Release 2, BusinessObjects Enterprise, Central Configuration Manager.

The Central Configuration Manager console appears.

2. Stop all services, except World Wide Web Publishing Services.

The Report Server is stopped.

To stop the Report Server on UNIX

1. Log into 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_home*/CommonReporting/bobje.

report_server_home

Specifies the Report Server installation path.

4. Run the following command:

```
./stopServers
```

The Report Server is stopped.

How to Uninstall Reporting

Complete the following procedures to uninstall SiteMinder reports:

1. Uninstall the Report Server.
Note: Uninstalling the Report Server can take up to three hours.
2. Uninstall the SiteMinder Report Server Configuration Wizard.
3. Remove leftover items

Uninstall the Report Server from Windows

To uninstall the Report Server

1. Exit all applications that are running.
2. Navigate to *report_server_home*\CommonReporting\Uninstall CA Business Intelligence.

report_server_home

Specifies the Report Server installation path.

3. Double-click Uninstall CA Business Intelligence.exe

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.
- b. Navigate to *report_server_home*\CommonReporting.
- c. Enter the following command:

```
Uninstall CA Business Intelligence.exe -i swing
```

4. Follow the prompts.

Note: If message prompts you to remove shared files, click No to All.

5. If requested, reboot the system.

The Report Server is uninstalled.

Uninstall the Report Server from UNIX

To uninstall the Report Server

1. Open a Bourne shell and navigate to `"report_server_home/CommonReporting/Uninstall CA Business Intelligence"`.

report_server_home

Specifies the Report Server installation path.

2. Run the following command:

```
./Uninstall_CA_Business_Intelligence
```

The uninstaller starts.

3. Follow the prompts.

The Report Server is uninstalled.

Uninstall the Report Server Configuration Wizard from Windows

To uninstall the Report Server Configuration Wizard

1. Exit all applications that are running.
2. Navigate to `report_server_home\CommonReporting\Uninstall CA SiteMinder Configuration Wizard`.

report_server_home

Specifies the Report Server installation path.

3. Double-click Uninstall CA SiteMinder Report Server Configuration Wizard.exe.

The uninstaller starts.

4. Follow the prompts.

Note: If message prompts you to remove shared files, click No to All.

5. If requested, reboot the system.

The Report Server Configuration Wizard is uninstalled.

Uninstall the Report Server Configuration Wizard from UNIX

To uninstall the Report Server Configuration Wizard

1. Exit all applications that are running.
2. Navigate to
report_server_home/CommonReporting/Uninstall_CA_SiteMinder_Configuration Wizard.

report_server_home

Specifies the Report Server installation path.

3. Run the following command:

```
./Uninstall_CA_SiteMinder_Report_Server_Configuration_Wizard
```

The uninstaller starts.

4. Follow the prompts.

The Report Server Configuration Wizard is uninstalled.

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.

To remove leftover items after uninstalling the Report Server

1. Navigate to *report_server_home*.

report_server_home

Specifies the Report Server installation path.

2. Delete the following folder:

CommonReporting

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.

To remove leftover items after uninstalling the Report Server

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.

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 335)

Chapter 12: Configuring the OneView Monitor

This section contains the following topics:

[OneView Monitor Overview](#) (see page 341)

[System Requirements for OneView Monitor](#) (see page 342)

[Configure the OneView Monitor](#) (see page 342)

[Limitation of OneView Monitor GUI/IIS Web Agent on Same Machine](#) (see page 342)

[How to Configure the OneView Monitor GUI on Windows/IIS](#) (see page 343)

[How to Configure the OneView Monitor GUI on UNIX/Sun Java System](#) (see page 344)

[Start the OneView Monitor Service](#) (see page 347)

[Access the OneView Monitor GUI](#) (see page 347)

[Monitor a Policy Server Cluster](#) (see page 347)

OneView Monitor Overview

The OneView Monitoring infrastructure consists of a number of modules that enable the monitoring of SiteMinder components. Included is the Monitor process that runs in the context of a Java Runtime Environment (JRE). The Monitor GUI's HTML pages are generated by Java Server Pages (JSPs) and servlets hosted on a ServletExec servlet engine running on the same machine as the Policy Server.

The OneView Monitor utility monitors the following SiteMinder components:

- Policy Server
- Web Agents

Note: More information on 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 ServletExec/ISAPI for Windows or ServletExec/AS for UNIX is installed on the system.
- **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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

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`
- `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

CA recommends that you read the ServletExec documentation before installing ServletExec. If ServletExec is not running properly, then the OneView Monitor GUI does not work since it relies on ServletExec's servlet engine.

Note: You can access the ServletExec documentation on the [New Atlanta Web site](#).

Install ServletExec/ISAPI on Windows 2003/IIS

To install ServletExec/ISAPI on Windows 2003/IIS

1. If you have an earlier version of ServletExec:
 - a. Back up the ServletExec Data and Servlets sub-directories, if desired.
 - b. Remove the earlier version.
2. Run the ServletExec ISAPI installer.

Note: For more information on running the ServletExec ISAPI installer, refer to New Atlanta Communication's ServletExec documentation.

3. Stop and restart the IIS Admin Web service and IIS Web server.

Set Permissions for IIS Users After Installing ServletExec

Since ServletExec/ISAPI runs as part of the IIS process, it runs as different users at different times. As a result, you must set the following permissions for the ServletExec installation directory and subdirectories.

To set permissions for IIS users after installing ServletExec, 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 347)

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 Policy 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 on using the OneView Monitor exists in the *Policy Server Administration Guide*.

Chapter 13: SNMP Support

This section contains the following topics:

[SNMP Support Overview](#) (see page 349)

[Prerequisites for Windows and UNIX Systems](#) (see page 351)

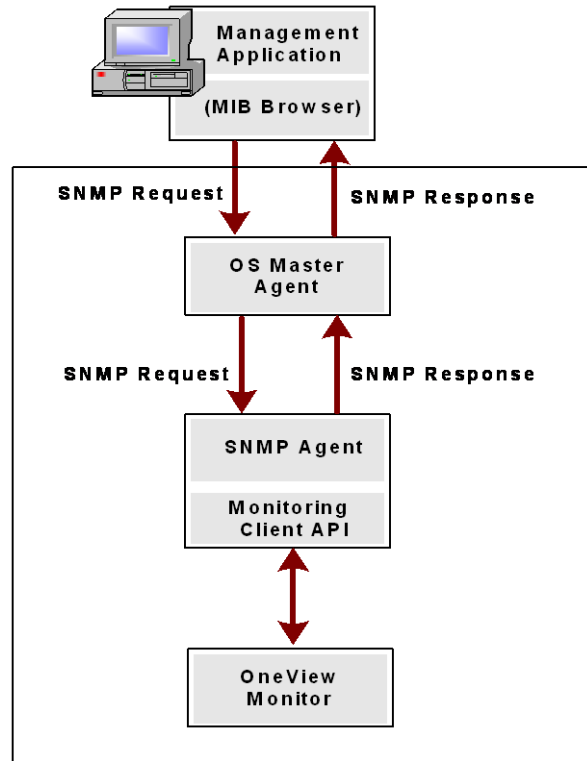
[Configure the SNMP Agent on Windows](#) (see page 352)

[Configure the SNMP Agent on UNIX Systems](#) (see page 354)

SNMP Support Overview

SNMP support includes a Management Information Base (MIB), an SNMP Agent, and the Event SNMP Trap library. You can configure the SNMP Agent and Event SNMP Trap library independently and enable one or disable the other or vice versa. The SNMP Agent enables monitoring applications to retrieve operational data from the OneView Monitor. The SNMP Agent sends data to the SNMP manager and supports SNMP request handling.

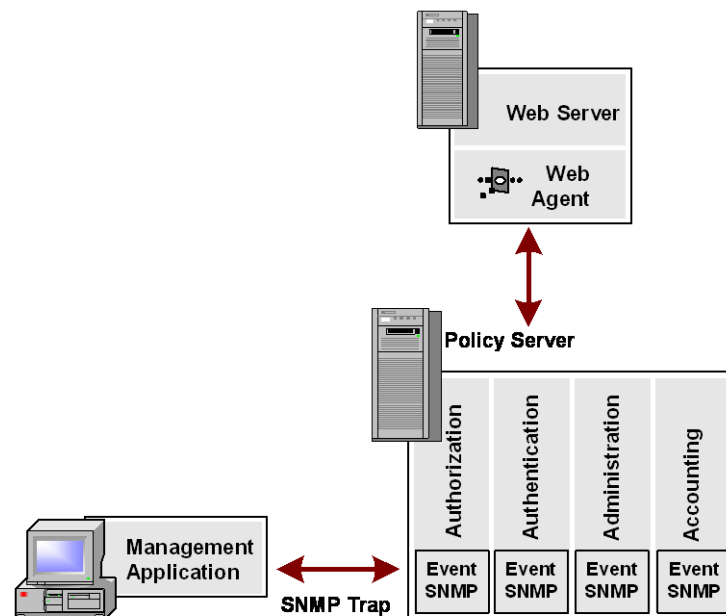
The following figure shows the architecture between the management application, OS Master Agent, SNMP Agent, and the OneView Monitor.



The OS Master Agent, such as the native Solaris SunSolstice Master Agent, invokes the SNMP Agent once you restart the Master Agent. Upon receiving an SNMP request from the management application the OS Master Agent forwards the SNMP request to the SNMP Agent. The SNMP Agent contacts the OneView Monitor, retrieves the required information using Monitor Client API, and then sends the response to the Master Agent. The Master Agent, in turn, forwards the response to the management application.

If you do not configure the SNMP Agent during the Policy Server installation, all the SNMP files are still installed in case you want to use the Agent later. However, to get the Agent running, you need to manually get the Agent started by configuring the SNMP Agent on a Windows or UNIX system.

The Event SNMP Trap library converts some SiteMinder events into SNMP traps before sending them to the management application as noted in the following figure. The trap library captures events sent by the Policy Server, decides if SNMP traps are to be generated on a given event, and generates a trap.



Note: 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

For instructions on how to install the SNMP service on a Windows operating system, see Windows Help.

UNIX Systems Prerequisites

The following section details UNIX prerequisites for SNMP support:

Solaris

You need the native Solaris SunSolstice Master Agent, which comes with the operating system.

Linux

For the supported Master Agent on Red Hat Advanced Server 3.0, upgrade the net-snmp package to net-snmp-5.1-2.1 or greater.

To upgrade the net-snmp package to net-snmp-5.1-2.1 or greater, use the following setting in net-snmpd instead of -c public -v 1 -p 8001 localhost .1.3.6.1.4.1.2552:

```
proxy -c public -v 1 localhost:8001 .1.3.6.1.4.1.2552
```

HP-UX

You need the HP-UX Master Agent, which comes with the operating system.

Configure the SNMP Agent on Windows

To configure the SNMP agent on Windows

1. Be sure that the NETE_PS_ROOT environment variable is set to the SiteMinder installation directory. The Policy Server installation program should have already done this.
2. Open *siteminder_home*\config\snmp.conf file and edit the last row to contain the full path to *siteminder_home*\log\snmp.log.

Note: You only need to do this if you did not specify the Policy Server installation program to automatically configure SNMP.

Correct example: LOG_FILE=C:\Program Files\Netegrity\siteminder\log\snmp.LOG

Incorrect example: LOG_FILE=\$NETE_PS_ROOT\log\snmp.log

3. Edit the *windows_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! If you are running a SiteMinder utility or executable on Windows Server 2008, be sure to open the command-line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

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 354).

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 356)

Configure the SNMP Agent on UNIX Systems

To configure the SNMP Agent on UNIX systems

1. Ensure the NETE_PS_ROOT environment variable is set to the SiteMinder installation directory. The Policy Server installation program should have already done this.

Example: /home/smuser/siteminder

2. Edit the file /etc/snmp/conf/RunSubagent.sh:

- a. Set the correct JRE path:
JAVA_HOME=\$INSTALL_HOME/bin/jdk/<required_version>/jre
- b. Set the correct SiteMinder path:

Example: INSTALL_HOME=/home/smuser/siteminder

Note: The INSTALL_HOME variable should contain the full path for the SiteMinder installation directory.

3. Restart the SNMP daemon on Solaris
 - a. Become root.
 - b. Goto `/etc/rc3.d`.
 - c. Execute the `S76snmpdx` script twice, as follows:
`sh S76snmpdx stop` to stop the running Solaris master agent.
`sh S76snmpdx start` to start the Solaris master agent and Netegrity subagent.

How to Configure SNMP Event Trapping on UNIX Systems

Configuring SNMP event trapping on UNIX systems requires you to:

1. Enable SNMP event trapping.
2. [Configure `snmptrap.config`](#) (see page 355).

Enable SNMP event trapping

To enable SNMP event trapping, use the `XPSCfg` utility to set the event handler library (`libeventsnmp.so`) to the `XPSCfg` 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 `XPSCfg` 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 356)

Stop and Restart the Policy Server

In order for the SNMP configurations changes to take effect, you need to stop and restart the Policy Server using the Status tab of the Policy Server Management Console.

Test SNMP Gets for Red Hat Enterprise Linux Advanced Server

You should test SNMP Gets after configuring SNMP.

To test SNMP Gets

1. Start the native SNMP master agent. On Red Hat AS, the master agent is not started automatically on start up as is the case on Solaris and HP-UX. To start the master agent, go to the `/etc/rc1.d` directory and run the following command (run as root):

```
K50snmpd start
```

2. Start the Netegrity subagent using the following command (run as root):

```
sh /etc/init.d/NetegrityAgent
```

3. To stop the Netegrity subagent on Red Hat AS, run the following command as root:

```
sh $NETE_PS_ROOT/etc/snmp/conf/StopSubagent.sh
```

Test SNMP Gets for HP-UX

You should test SNMP Gets after configuring SNMP.

To test SNMP Gets

1. Start the Native Agent Adaptor with the script `"/sbin/init.d/SnmpNaa"` using the following command as root:

```
nohup sh /sbin/init.d/SnmpNaa start
```

2. Start the Netegrity subagent with the script `"/sbin/init.d/SnmpNetegrity"` using the following command (run as root):

```
nohup sh /sbin/init.d/SnmpNetegrity start
```

3. To stop the Netegrity subagent on HP-UX, run the following command as root:

```
sh /sbin/init.d/SnmpNetegrity stop
```

Appendix A: Installing the Administrative UI to an Existing Application Server

This section contains the following topics:

[Administrative UI Installation Options](#) (see page 357)
[Administrative UI Installation Requirements](#) (see page 358)
[Trusted Relationship with a Policy Server](#) (see page 362)
[Administrative UI Installation Checklist](#) (see page 362)
[How to Install the Administrative UI](#) (see page 363)
[How to Register the Administrative UI](#) (see page 369)
[Stop the Application Server](#) (see page 374)
[Administrator Credentials](#) (see page 375)
[Administrative UI High Availability](#) (see page 376)
[Uninstall the Administrative UI on Windows](#) (see page 376)
[Uninstall the Administrative UI on UNIX](#) (see page 377)

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 261)

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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Windows

The Windows system to which you are installing the Administrative UI must meet the following minimum system requirements.

- **CPU**—Single or dual-processor, Intel Pentium III (or compatible), 700-900 MHz.
- **Memory**—512 MB system RAM. We recommend 1 GB.
Note: If you are running WebSphere, 2 GB 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**—450 MB.
- **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.

UNIX

The UNIX system to which you are installing the Administrative UI must meet the following minimum system requirements.

- **CPU**

- Solaris—Sparc Workstation 440 MHz.
- Red Hat Linux—Single or dual-processor, Intel Pentium III (or compatible), 700-900 MHz.

- **Memory**—512 MB system RAM. We recommend 1 GB.

Note: If you are running WebSphere, 2 GB 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**—450 MB.

- **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.

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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

JBoss as an Application Server

A supported application server is required on the Administrative UI host system. Follow the installation instructions as described on the [JBoss web site](#) to install JBoss.

Important! Be sure to install JBoss in a directory pathname that contains no spaces.

WebLogic as an Application Server

The following sections provide basic instructions for using WebLogic as a SiteMinder application server.

Install WebLogic

Install a version of a WebLogic server that is supported by 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 SiteMinder application server.

Install WebSphere

Follow the WebSphere installation instructions as described in the IBM documentation.

When installing WebSphere, consider that WebSphere 6.x uses default messaging (embedded messaging for WebSphere 5.1), which is installed with the WebSphere server.

- (Solaris) Configure the groups `mqm` and `mqbrkr`; and the users `mqm` and `root`, as described in the IBM installation documentation before you install the Embedded Messaging service.
- For all WebSphere versions, be sure to select the Server and Client option when installing WebSphere.

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 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.
- ☐ 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 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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Administrative UI System Requirements](#) (see page 358)

[Application Server Requirements](#) (see page 359)

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

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. Gather application server information for the Administrative UI installer.
3. Install the Administrative UI.
4. Start the application server.

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.

More information:

[Administrative UI Installation Worksheets](#) (see page 385)

JBoss Information

If you are using a JBoss application server, gather the following information before installing and registering the Administrative UI:

- **JBoss installation folder**—The path to the folder where JBoss is installed.
Note: The path cannot contain spaces.
- **JBoss URL**—The fully qualified URL of the JBoss host system.
- **JDK**—The installation location of the required JDK.
- **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.
Note: For more information about starting the Policy Server Management Console, see the *Policy Server Administration Guide*.

More information:

[JBoss Worksheet](#) (see page 385)

WebLogic Information

If you are using a WebLogic application server, gather the following information before installing and registering the Administrative UI:

- **WebLogic binary folder**—The path to the WebLogic installation directory.
Example: C:\bea\weblogic
- **WebLogic domain folder**—The path to the WebLogic domain you created for the Administrative UI.
Example: C:\bea\user_projects\domains\mydomain
- **WebLogic server name**—The name of the WebLogic server on which the WebLogic domain is configured.
Default: AdminServer
- **Application server URL and port**—The fully qualified URL of WebLogic host system.
Example: http://mymachine.mycompany.com:7001

- **JDK**—The installation location of the required JDK.
- **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.

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

More information:

[WebLogic Worksheet](#) (see page 386)

WebSphere Information

If you are using a WebSphere application server, gather the following information 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.
- **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.

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

More information:

[WebSphere Worksheet](#) (see page 386)

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 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 based on operating system, see the installation and upgrade considerations in 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.
- **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

- **Important!** (UNIX) Depending on your permissions, you may need to add executable permissions to the directory that contains the installation media by running the following:

```
chmod -R+x directory
```

directory

Specifies the directory that contains the installation media.

- **Important!** (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.
- If you are installing the Administrative UI to the same system as the Report Server, port conflicts can occur. By default, both components use port 8080.

More information:

[Installing the Administrative UI](#) (see page 261)

[Install the Administrative UI](#) (see page 267)

[Locate the Installation Media](#) (see page 456)

Windows

To install the Administrative UI on Windows

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 based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

4. Use your completed installation worksheet to enter the required values.

Note: If you enter IPv6 addresses, surround the entry with brackets.

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

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 369)

UNIX GUI

To install the Administrative UI with a UNIX GUI

1. Exit all applications that are running.
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 based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

4. Use your completed installation worksheet to enter the required values.

Note: If you enter IPv6 addresses, surround the entry with brackets.

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

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.

More information:

[How to Register the Administrative UI](#) (see page 369)

UNIX Console

To install the Administrative UI with a UNIX console

1. Exit all applications that are running.
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 based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

4. Use your completed installation worksheet to enter the required values.

Note: If you enter IPv6 addresses, surround the entry with brackets.

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

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 369)

How to Register the Administrative UI

You must register the Administrative UI before you can 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.
2. Start the application server.
3. Register the Administrative UI.

More information:

[Installing the Administrative UI](#) (see page 261)

[How to Register the Administrative UI](#) (see page 272)

Reset the Administrative UI Registration Window

If you used the XPSRegClient utility more than 24 hours ago to submit the SiteMinder super user credentials to the Policy Server, this step is required. The time from which you submit the credentials and attempt to create a trusted relationship with a Policy Server cannot exceed 24 hours.

To reset the registration window

1. Log into 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 SiteMinder administrator. If you are installing the Administrative UI as part of:

- A new r12.0 SP2 environment, specify the default SiteMinder administrator account (siteminder).
- An upgrade, specify any 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 in the policy store, use the smreg utility to create the default SiteMinder account.

passphrase

Specifies the password for the SiteMinder administrator account.

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

-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: 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 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.

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.

To start the application server

1. Do one of the following:

- **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. Do one of the following:

■ **JBoss**

- Windows: Type `run_idm.bat` and press Enter.
- UNIX: Type `run_idm.sh` and press Enter.

■ **WebLogic**

- Windows: Type `startWebLogic.cmd` and press Enter.
- UNIX: Type `startWebLogic.sh` and press Enter.

■ **WebSphere**

- Windows: Type `startServer.bat identifier` and press Enter.
- UNIX: Type `startServer.sh identifier` and press Enter.

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 261)

[Start the Application Server](#) (see page 273)

Register the Administrative UI

You register the Administrative UI with a Policy Server to begin managing your environment.

To register the Administrative UI

1. Do one of the following:

- **Windows**—Use the Administrative UI shortcut to open the Administrative UI.

- **UNIX**—Open a web browser and go to `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 SiteMinder Administrative UI login screen appears.

2. Type siteminder in the User Name field.
3. Type the siteminder account password in the Password field.
4. 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.

More information:

[Registration Not on File Error Appears](#) (see page 398)

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.

- 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 261)

[Stop the Application Server](#) (see page 275)

Administrator Credentials

By default, the Administrative UI uses the policy store as its source for 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 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 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 SiteMinder administrators are available to all GUIs.

Note: For more information about configuring an external administrator store, see the *Policy Server Configuration Guide*.

More information:

[How to Install the Administrative UI](#) (see page 363)

Uninstall the Administrative UI on Windows

You uninstall the Administrative UI when it is no longer required on the system.

Note: 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 uninstall the Administrative UI

1. Stop the application server.
2. Open the Windows Control Panel and double-click Add/Remove Programs.
A list of installed programs appears.

3. Select CA SiteMinder Administrative UI, and click Change/Remove.

Note: If you upgraded the Administrative UI from r12.0 SP1, CA SiteMinder Web Access Manager Administrative UI is listed in addition to CA SiteMinder Administrative UI. Select CA SiteMinder Administrative UI to uninstall the Administrative UI after an upgrade.

The process to uninstall the Administrative UI starts.

4. Follow the prompts to uninstall the Administrative UI.

Note: If a message prompts you to remove shared files, click No to All.

5. If requested, reboot the system.

The Administrative UI is uninstalled.

More information:

[Installing the Administrative UI](#) (see page 261)

[Uninstall the Administrative UI on Windows](#) (see page 282)

Uninstall the Administrative UI on UNIX

You uninstall the Administrative UI when it is no longer required on the system.

Note: 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 uninstall the Administrative UI on UNIX

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 261)

[Uninstall the Administrative UI on UNIX](#) (see page 283)

Appendix B: Installation Worksheets

Use the worksheets in this section to help you record information that is required to install or upgrade SiteMinder.

Policy Server Worksheets

Use the following worksheets to record the necessary information to install the Policy Server and configure Policy Server components.

Required Information Worksheet

Use this worksheet to gather the required information before running the Policy Server installer.

Information Needed	Your Value
JRE location	
Policy Server installation location	
Encryption key value	

OneView Monitor Information Worksheet

If you plan on configuring the OneView Monitor, use this worksheet to gather information.

Information Needed	Your Value
JDK path	
ServletExec installation directory	
ServletExec port number	
Sun Java System administrator directory	
Multiple ServletExec instances	

Microsoft ADAM/AD LDS Server Information Worksheet

Use this worksheet to gather the required information to configure an ADAM/AD LDS policy store.

Information Needed	Your Value
System IP address	
Server instance port number	
Root DN of the application partition	
Administrator domain name	
Administrator password	
Alternate LDAP administrator	
SiteMinder super user password	

Sun Java System Directory Server Information Worksheet

Use this worksheet to gather the required information to configure a Sun Java System Directory Server policy store.

Information Needed	Your Value
System IP address	
Directory instance port number	
Root DN	
Administrator account	
Administrator password	
Alternate LDAP administrator	
SiteMinder super user password	

SM Key Database Information Worksheet

If you plan on configuring the smkeydatabase, use this worksheet to gather the required information.

Information Needed	Your Value
smkeydatabase password	

Policy and Data Store Worksheets

You can use the following worksheets to record the necessary information to configure:

- An LDAP database as a policy store
- A relational database as a policy store
- An individual relational database as an audit logging database, key store, token store or session store

CA Directory Information Worksheet

You can use this worksheet to gather the required information for configuring a CA Directory database as a policy store.

Information Needed	Your Value
Host information	
CADSA port number	
Base DN	
Administrative DN	
Administrative password	

More information:

[Gather Directory Server Information](#) (see page 97)

Sun Java System Directory Server Information Worksheet

You can use this worksheet to gather the required information for configuring a Sun Java System Directory Server as a policy store or upgrading an existing policy store.

Information Needed	Your Value
Host information	
Directory server port information	
Administrative DN	
Administrative password	
Policy store root DN	
(Optional) SSL client certificate	

More information:

[Gather Directory Server Information](#) (see page 110)

Active Directory Information Worksheet

You can use this worksheet to gather the required information for configuring an Active Directory directory server as a policy store or upgrading an existing policy store.

Information Needed	Your Value
Host information	
Directory server port information	
Administrative DN	
Administrative password	
Policy store root DN	
(Optional) SSL client certificate	

More information:

[Gather Directory Server Information](#) (see page 110)

Microsoft ADAM/AD LDS Information Worksheet

Use this worksheet to gather the required information to configure an ADAM/AD LDS policy store.

Information Needed	Your Value
Host information	
Directory server port information	
Administrative DN	
Administrative password	
Policy store root DN	
(Optional) SSL client certificate	

SQL Server Information Worksheet

Use this worksheet to gather the required information for configuring a SQL Server database to function as a policy store or any other type of SiteMinder data store.

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.

Information Need	Your Value
Database instance name	
Database administrative account	
Database administrative password	
(W) Data source name	
(W) SQL Server name	
(U) Policy Server root	
(U) IP address	

Oracle Information Worksheet

Use this worksheet to gather the required information for configuring an Oracle database to function as a policy store or any other type of SiteMinder data store.

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 the Oracle data source for UNIX.

Information Needed	Your Value
(U) Policy Server installation path	
Data source	
Database administrative account	
Database administrative password	
Oracle machine name	
Oracle instance service name	
Oracle port number	

Oracle RAC Information Worksheet

Use this worksheet to gather the required information for configuring an Oracle RAC database to function as a policy store or any other type of SiteMinder data store.

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 the Oracle data source for UNIX.

Information Needed	Your Value
(U) Policy Server installation path	
Data source name	
Database administrative account	
Database administrative password	
Oracle RAC system service name	
Oracle RAC node service names	
Oracle RAC node IP addresses	
Oracle RAC node port number	

Administrative UI Installation Worksheets

You can use the following worksheets to record the necessary information to:

- Install the Administrative UI.
- Configure the connection between the Administrative UI and a Policy Server.

Prerequisite Installer Worksheet

Use this worksheet to gather the required information for installing and registering the Administrative UI using the prerequisite installer.

Required Information	Your Value
Installation location	
Administrative UI system name	
Server port	
SiteMinder super user account password	
Policy Server host name	
Policy Server authentication port	

More information:

[Gather Information for the Installer](#) (see page 265)

JBoss Worksheet

Use this worksheet to gather the required JBoss information for installing and registering the Administrative UI:

Required Information	Your Value
JBoss installation folder	
JBoss URL	
JDK installation location	
SiteMinder super user account password	
Policy Server host name	
Policy Server authentication port	

More information:

[JBoss Information](#) (see page 364)

WebLogic Worksheet

Use this worksheet to gather the required WebLogic information for installing and registering the Administrative UI.

Required Information	Your Value
WebLogic binary folder	
WebLogic domain folder	
WebLogic server name	
Application server URL and port	
JDK installation location	
SiteMinder super user account password	
Policy Server host name	
Policy Server authentication port	

More information:

[WebLogic Information](#) (see page 364)

WebSphere Worksheet

Use this worksheet to gather the required WebSphere information for installing and registering the Administrative UI.

Required Information	Your Value
WebSphere installation folder	
WebSphere URL	
Server name	
Profile name	
Node name	
Cell name	
JDK installation location	

Required Information	Your Value
SiteMinder super user password	
Policy Server host name	
Policy Server authentication port	

More information:

[WebSphere Information](#) (see page 365)

Policy Server Registration Worksheet

Use this worksheet to gather the required information for registering the Administrative UI with additional Policy Servers.

Required Information	Your Value
Client name	
Passphrase	
Policy Server host name	
Policy Server authentication port	

More information:

[Gather Registration Information](#) (see page 279)

Reporting Worksheets

You can use the following worksheets to record the necessary information to install SiteMinder reports.

Installation Credentials Worksheet

Use this worksheet to gather the required installation credentials:

Required Value	Your Value
(Windows and UNIX) BusinessObjects administrator password	
(UNIX) Non-root user account name	

Required Value	Your Value
(UNIX) Non-root user group name	

MySQL Report Database Worksheet

Use this worksheet to gather the required MySQL database information:

Required Value	Your Value
MySQL root password	
User name	
Password	
Database name	

SQL Server Report Database Worksheet

Use this worksheet to gather the required Microsoft SQL Server database information:

Required Value	Your Value
Data source name	
Database name	
User name	
Password	

Oracle Report Database Worksheet

Use this worksheet to gather the required Oracle database information:

Required Value	Your Value
Oracle Net Services Name	
User name	
Password	

Apache Tomcat Worksheet

Use this worksheet to gather the required Apache Tomcat information:

Required Value	Your Value
Connection port	
Redirect port	
Shutdown port	

Report Server Configuration Worksheet

Use this worksheet to gather the required information for installing the report templates:

Required Value	Your Value
BusinessObjects default administrator password	
SiteMinder audit database type	

Report Server Registration Worksheet

You can use this worksheet to gather the required registration information for the Report Server installation:

Required Value	Your Value
Client name	
Passphrase	
Policy Server host	

Appendix C: Troubleshooting

This section contains the following topics:

[Policy Server Troubleshooting](#) (see page 391)

[Policy Store Troubleshooting](#) (see page 393)

[OneView Monitor Troubleshooting](#) (see page 395)

[Administrative UI Troubleshooting](#) (see page 397)

[FSS Administrative UI Troubleshooting](#) (see page 403)

[Report Server Troubleshooting](#) (see page 406)

[Java Error Messages When Uninstalling](#) (see page 407)

[Adobe Acrobat Reader Won't Install](#) (see page 408)

[Problem With Using Active Directory as a User Store](#) (see page 408)

[AE failed to load library 'smjavaapi'. System error](#) (see page 408)

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 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 SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

Winsock error 10054 message

Valid on Windows

Symptom:

When I try to log into the Policy Server, I receive the "Unable to proceed, winsock error 10054" message.

Solution:

One of the following could be the cause of the problem:

- The policy store does not contain the proper SiteMinder schema. Make sure you imported the correct SiteMinder schema.
- The Policy Server is not running. To start this server, use the Status tab on the Policy Server Management Console.

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

- The Policy Server is not connected to the policy store properly. Using the Data tab on the Policy Server Management Console, click Test Connection to make sure the policy store connects successfully. If it does not, reenter the data source information values on the Data tab by pointing the Policy Server at the policy store.

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.IndexOutOfBoundsException` to the FSS Administrative UI.

Solution:

Policy Stores with large numbers of objects may return the exception `java.lang.IndexOutOfBoundsException` to the Administrative UI.

Define the registry key
`\HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\ObjectStore\MaxObjects` to a value lower than 100 (such as 50).

SSL initialization failed: error -8174 (security library: bad database.)

Valid on Windows and UNIX Systems

Symptom:

When I run `smldapsetup ldmod -fpstore -ssl1 -c/app/siteminder/ssl/cert7.db` for policy stores that are using an SSL-encrypted connection to Sun Java System Directory Server, I receive the following error message:

"SSL initialization failed: error -8174 (security library: bad database.)"

Solution:

1. Make sure the `key3.db` file exists in the same directory as `cert7.db` for the Netscape Web browser.
2. Rerun this `smldapsetup` command, and, for the `-c` option, specify the path of the directory where the SSL client certificate database file, `cert7.db`, exists.

Example: if `cert7.db` exists in `/app/siteminder/ssl`, specify
`-c/app/siteminder/ssl/cert7.db`

ODBC Policy Store Import Fails with UserDirectory Error

Symptom:

I receive an error message stating that the policy store failed operation "save" for object type "UserDirectory" when importing policy store data into an ODBC policy store.

Solution:

It is possible that the server name in the ODBC store's userDirectory object is longer than 512 characters, which by default, exceeds the limit allowed by the MS SQL Server and Oracle policy store schema scripts that are shipped with SiteMinder.

Do one of the following:

If you are trying to import policy data into a supported version of a MS SQL Server policy store:

1. Open `sm_mssql_ps.sql`.

Note: This schema script is located in *policy_server_home*\db\SQL.

2. Search for the following text:

```
CREATE TABLE smuserdirectory5
```

3. Modify "server smstringreq512N," to one of the following depending on your needs:

- server smstringreq1024,N
- server smstringreq4000,N

4. Re-import the policy store schema into the policy store.

5. Import the policy store data.

If you are trying to import policy data into a supported version of an Oracle policy store:

1. Open `sm_oracle_ps.sql`.

Note: This schema script is located in *policy_server_home*\db\SQL.

2. Search for the following text:

```
CREATE TABLE smuserdirectory5
```

3. Modify "server VARCHAR2(512) NOT NULL," to one of the following depending on your needs:

- server VARCHAR2(1024) NOT NULL,
- server VARCHAR2(4000) NOT NULL,

4. Re-import the policy store schema into the policy store.

5. Import the policy store data.

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

As mentioned in the procedure for installing the ServletExec/AS on a UNIX/Sun Java System, we advise not allowing ServletExec to modify the Sun Java System Web server's configuration files (obj.conf and magnus.conf). However, if ServletExec did modify these files during installation, the Web server instance fails after you configure the FSS Administrative UI and OneView Monitor GUI using the Policy Server installer/wizard. The ServletExec installer puts entries in these files that conflict with those from the Policy Server.

To keep the Web server instance from failing, remove the conflicting entries from the Sun Java System Web Server instance's obj.conf and magnus.conf files.

1. Open
`/<sunjavasystem_home>/servers/https-<web_server_instance_name>.do`
`main.com/config/magnus.conf`, and remove the first line:

```
Init fn="ServletExecInit" <ServExec_instance_name>.instances="<IP_address>:<portnumber> "
```

ServExec_instance_name

Specifies the name of your ServletExec instance.

IP_address

Specifies the IP Address of the machine where ServletExec is installed.

portnumber

Specifies the port number for the ServletExec instance.

Note: The Policy Server Configuration Wizard added the correct entry at the end of the file.

2. Open
`/<sunjavasystem_home>/servers/https-<web_server_instance_name>.do`
`main.com/config/obj.conf`, and remove lines four and five from the top of the file:

```
NameTrans fn="assign-name" from="/servlet/*" name="<ServExec_instance_name>"
```

```
NameTrans fn="assign-name" from="*.jsp*" name="<ServExec_instance_name>"
```

Important! Do not remove the `name="se-<ServExec_instance_name>"` entries in lines two and three since these were added by the Policy Server Configuration Wizard.

3. In the same `obj.conf` file, remove the second to the last `<Object name="<ServExec_instance_name>">` section from the end of the file:

```
<Object name="<ServExec_instance_name>">  
Service fr="ServletExecService" group="<ServExec_instance_name>"  
</Object>
```

Important! Do not remove the `<Object name="se-<ServExec_instance_name>">` entry since this one was added by the Policy Server Configuration Wizard.

4. After saving these files, you should be able to start the Web server instance from the Sun Java System Web Server Administration Server page.

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 Allow Execute Access permission.
9. Click Finish.

Administrative UI Troubleshooting

The following sections detail common problems you may experience with registering the Administrative UI and the proposed solutions.

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 SiteMinder administrator. If you are installing the Administrative UI as part of:

- A new r12.0 SP2 environment, specify the default SiteMinder administrator account (siteminder).
- An upgrade, specify any 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 SiteMinder administrator (siteminder). For more information about using the smreg utility, see the *Policy Server Administration Guide*.

passphrase

Specifies the password for the 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 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 (smpls.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 searching on a large number of policy objects via the Administrative UI, the connection between the Administrative UI and the Policy Server may time out and/or the Policy Server tunnel buffer may become corrupt. This 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 this 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\Netegrity\SiteMinder\CurrentVersion\PolicyServer\
Max AdmComm Buffer Size
2. Set this registry key to a large value, such as 5,910,496 bytes (0x5a2fe0).
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 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 r12.0 SP2, the properties file is located at *deploy*/IdentityMinder.ear/user_console.war/META-INF.

FSS Administrative UI Troubleshooting

The following sections detail common problems you may experience with using the FSS Administrative UI and the proposed solutions.

FSS Administrative UI Fails to Start in IE

Symptom:

When I attempt to start the FSS Administrative UI in Internet Explorer it fails.

Solution:

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

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

FSS Administrative UI does not appear on Windows

Valid on Windows

Symptom:

I have installed the FSS Administrative UI, but it does not appear.

Solution:

If you installed an Internet Information Server (IIS) Web Server on a port other than 80, the FSS Administrative UI may not appear. Editing the FSS Administrative UI shortcut URL should fix the problem.

To edit the shortcut URL.

1. Right-click Start and select Open All Users.
2. Double-click Programs.
3. Double-click SiteMinder.
4. Highlight the FSS Administrative UI icon, right click, and select Properties.
5. Select the Web Document tab.

6. In the URL field on the Web Document tab, change the port number to the one you configured for the IIS Web Server.

Example: if your IIS Web Server is located on port 81, change:

`http://<fully qualified domain name>:80/siteminder/index.htm`

to `http://<fully qualified domain name>:81/siteminder/index.htm`

7. Click Apply and OK.

If you are still have difficulty getting the FSS Administrative UI to display, run the FSS Administrative UI Browser Compatibility Test at the following URL:

`http://www.netegrity.com/uitest`

If the panel is a solid box, click Details for more troubleshooting information.

FSS Administrative UI Fails to Start on a Sun Java Web Server

Symptom:

When I attempt to start the FSS Administrative UI that is configured for a Sun Java System Web server, it fails to start.

Solution:

Disable the Java Enabled Globally option by doing the following:

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

yourserver.com

Specifies the domain name of the Enterprise Administration Server.

webserverport

Specifies the port number.

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

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.

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.

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, even if you are logged into the system as an Administrator. For more information, see the release notes for your 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.

Appendix D: Unattended Installation

This section contains the following topics:

[Silent Installation](#) (see page 411)

[Silent Installation Guidelines](#) (see page 411)

[Default Properties Files](#) (see page 412)

[How to Silently Install a Policy Server](#) (see page 413)

[How to Silently Install the Administrative UI](#) (see page 422)

[How to Silently Install Reports](#) (see page 429)

Silent Installation

After you have installed a SiteMinder component once, you can silently install the component again. A silent installation lets you install a component without user interaction. The following details how to install the following silently:

- A Policy Server
- An Administrative UI
- A Report Server

Silent Installation Guidelines

Each SiteMinder component is associated with its own properties file or files. The following guidelines apply to all properties files. Review them before starting a silent 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`

`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`

`admin_ui_home`

Specifies the Administrative UI installation path.

More information:

[Administrative UI Installation Options](#) (see page 262)

Reporting Properties File

Silently installing SiteMinder reports requires a properties file for the Report Server and a properties file for the SiteMinder Report Server Configuration Wizard. These properties files have the following default names and locations:

- response.properties

Use this file to install the Report Server.

Location

This file has no default location. The user who installed the Report Server specified where to save the file.

- reportserver_config_installer.properties

Location

report_server_home\CommonReporting\install_config_info

report_server_home

Specifies the Report Server installation path.

How to Silently Install a Policy Server

Complete the following steps to install a Policy Server silently:

1. Review the silent installation guidelines.
2. From a Policy Server host system, copy the Policy Server properties file.
3. Do one of the following. If you are:
 - Reinstalling the Policy Server, copy the file to a temporary location.
 - 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:

[Silent Installation Guidelines](#) (see page 411)

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 SiteMinder program icon.

Example: `C:\\Documents and Settings\\All Users\\Start or /SiteMinder`

Note: The icon feature only works on Windows.

DEFAULT_JRE_ROOT

Specifies the JRE installation location.

DEFAULT_BROWSER

(UNIX only) Specifies the installation location of the browser.

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 section allows you to set the following:

DEFAULT_OVMGUI_CHOICE

If you want the installation to auto-configure the OneView Monitor GUI on the Web server, then set this value to **true**. Otherwise, enter **false**.

DEFAULT_WEBSERVERS_CHOICE

If you want the installation to auto-configure the FSS Administrative UI, documentation, SiteMinder CGI scripts, and OneView Monitor on the Web server, then set this value to **true**. Otherwise, enter **false**.

DEFAULT_SNMP_CHOICE

If you want the installation to auto-configure the SNMP support with the Policy Server, then set this value to **true**. Otherwise, enter **false**.

DEFAULT_POLICYSTORE_CHOICE

If you want the installation to auto-configure the policy store, then set this value to **true**. Otherwise, enter **false**.

OneView Monitor GUI

If you set the `DEFAULT_OVMGUI_CHOICE` parameter to **true** when configuring the Policy Server features to have the installation configure the OneView Monitor, 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 Password

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`.

LDAP Policy Store

You set the `DEFAULT_POLICYSTORE_CHOICE` parameter to **true** when configuring Policy Server features to have the installation configure the LDAP policy store, then set the following:

DEFAULT_POLICYSTORE_TYPE

Specifies the type of LDAP Directory Server for the policy store.

DEFAULT_POLICYSTORE_IP

Specifies the IP Address (or host name) of the machine where the LDAP Directory Server resides.

Example: 172.26.4.238.

DEFAULT_POLICYSTORE_PORT

Specifies the port number for the LDAP instance that you are configuring as a policy store.

Example: 1356.

DEFAULT_POLICYSTORE_ADMINDN

Specify the LDAP Directory Server's administrator user name.

Example: cn=Directory Manager.

DEFAULT_POLICYSTORE_ADMINPW

Allows you to enter a cleartext password for the LDAP Directory Server's administrator. If you comment out the `ENCRYPTED_LDAP_ADMINPW` parameter and uncomment `DEFAULT_LDAP_ADMINPW`, then the unattended installer uses the cleartext password from `DEFAULT_LDAP_ADMINPW`.

Default: The `DEFAULT_LDAP_ADMINPW` parameter is commented out after the initial Policy Server installation.

ENCRYPTED_POLICYSTORE_ADMINPW

Shows the encrypted password for the LDAP Directory Server's administrator. You entered this password during the initial Policy Server installation and cannot change it.

Important! Do not modify this password since it is encrypted. If you comment out the `DEFAULT_LDAP_ADMINPW` parameter and uncomment `ENCRYPTED_LDAP_ADMINPW`, then the unattended installer uses the encrypted password from `ENCRYPTED_LDAP_ADMINPW`.

DEFAULT_POLICYSTORE_ROOTDN

Specifies the root DN.

Example: o=test.com.

DEFAULT_POLICYSTORE_USER_CHOICE

If you want to specify a different LDAP user account to update SiteMinder data, then set this value to **true**. Otherwise, enter **false**.

DEFAULT_POLICYSTORE_USERDN

Specifies the DN for the different LDAP user.

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

DEFAULT_POLICYSTORE_USERPW

Allows you to enter a cleartext password for the different LDAP user. If you comment out the ENCRYPTED_LDAP_USERPW parameter and uncomment DEFAULT_LDAP_USERPW, then the unattended installer uses the cleartext password from DEFAULT_LDAP_USERPW.

Default: The DEFAULT_LDAP_USERPW parameter is commented out after the initial Policy Server installation.

ENCRYPTED_POLICYSTORE_USERPW

Shows the encrypted password for the different LDAP user. You entered this password during the initial Policy Server installation and cannot change it.

Important! Do not modify this password since it is encrypted.

If you comment out the DEFAULT_LDAP_USERPW parameter and uncomment ENCRYPTED_LDAP_USERPW, then the unattended installer uses the encrypted password from ENCRYPTED_LDAP_USERPW.

DEFAULT_INIT_POLICYSTORE_CHOICE

If you are initializing a new LDAP instance, then set this value to **true**. Otherwise, enter **false**.

DEFAULT_SM_ADMINPW

Allows you to enter a cleartext password for the SiteMinder Super User. If you comment out the ENCRYPTED_SM_ADMINPW parameter and uncomment DEFAULT_SM_ADMINPW, then the unattended installer uses the cleartext password from DEFAULT_SM_ADMINPW.

Default: The DEFAULT_SM_ADMINPW parameter is commented out after the initial Policy Server installation.

ENCRYPTED_SM_ADMINPW

Shows the encrypted password for the SiteMinder Super User. You entered this password during the initial Policy Server installation and cannot change it.

Important! Do not modify this password since it is encrypted.

If you comment out the DEFAULT_SM_ADMINPW parameter and uncomment ENCRYPTED_SM_ADMINPW, then the unattended installer uses the encrypted password from ENCRYPTED_SM_ADMINPW.

DEFAULT_SMKEYDB_CHOICE

Specifies if an smkeydatabase is created during installation or is created manually after installation.

true

Specifies that the smkeydatabase be created during installation.

Limit: The value must be entered in lower-case text.

false

Specifies that the smkeydatabase is to be manually created after installation.

Limit: The value must be entered in lower-case text.

DEFAULT_SMKEYDB_PW

Allows you to enter a clear text password for the smkeydatabase.

Default: This parameter is commented out after the initial Policy Server installation. The password cannot be encrypted.

ENCRYPTED_SMKEYDB_PW

Represents the encrypted smkeydatabase password entered during the initial Policy Server installation.

Important! Do not modify this password since it is encrypted.

DEFAULT_SMKEYBD_IMPORT_CHOICE

Specifies if the certificate authority (CA) default certificates are imported into the smkeydatabase during installation or if they will be manually imported after installation.

true

Specifies that the CA default certificates be imported into the smkeydatabase during the installation.

Limit: The value must be entered in lower-case text.

false

Specifies that the CA default certificates are to be manually imported into the smkeydatabase after the installation.

Limit: The value must be entered in lower-case text.

Run the Policy Server Installer

You run the Policy Server installer silently 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 based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

More information:

[Locate the Installation Media](#) (see page 456)

Windows

To install the Policy Server silently on Windows, 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
```

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 silent installation begins. The installer uses the parameters you specified in the properties file to install the Policy Server.

UNIX

To install the Policy Server silently on UNIX, open a shell and 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 silent installation begins. The installer uses the parameters 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

- **smpls.log**

The smpls.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 `ca-ps-12.0-sp2-win32.exe` and `ps_install.exe` processes.
- **UNIX**—Press Ctrl+C

How to Silently Install the Administrative UI

Complete the following steps to silently install the Administrative UI:

1. Do one of the following. If you are:
 - Using the prerequisite installer, review the [installation checklist](#) (see page 264).
 - Installing to an existing application server infrastructure, review the [installation checklist](#) (see page 362).
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, do the following:
 - 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:

[Silent Installation Guidelines](#) (see page 411)

[Administrative UI Properties Files](#) (see page 412)

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 412)

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 412)

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.

Silently Install the Administrative UI

You run the Administrative UI installer silently to install the Administrative UI without user interaction.

Before You Install

Consider the following 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 based on operating system, see the installation and upgrade considerations in 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, be sure that both executables are in the same location. The prerequisite installer automatically calls the Administrative UI installer to complete the installation.

More information:

[Locate the Installation Media](#) (see page 456)

Windows

To install the Administrative UI silently on Windows, 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.

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 272).
- If you installed the Administrative UI to an existing application server infrastructure, see [How to Register the Administrative UI](#) (see page 369).

UNIX

To install the Policy Server silently on UNIX, open a shell 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.

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 272).
- If you installed the Administrative UI to an existing application server infrastructure, see [How to Register the Administrative UI](#) (see page 369).

How to Silently Install Reports

Complete the following steps to install SiteMinder reports silently:

1. Review the [installation checklists](#) (see page 297).
2. Gather the [required information for the installer](#) (see page 302).
3. Review the guidelines for silent installation.
4. Locate the Report Server and SiteMinder Report Server Configuration Wizard properties files.
5. Copy the properties files to a temporary location on the host system.
6. Copy the Report Server and the SiteMinder Report Server Configuration Wizard installation media to a temporary location on the host system.

Note: You can download the installation media from the Technical Support site.

7. Modify the Report Server properties file.
8. Modify the SiteMinder Report Server Configuration Wizard properties file.
9. Run the Report Server installer.
10. Run the SiteMinder Report Server Configuration Wizard.
11. Register the Report Server.

Modify the Report Server Properties File

You modify the installer properties file to define installation variables. The default values reflect the information entered when a Report Server was installed and a response file was saved.

Installation Options

This section lets you specify the installation type and the root folder for the installation. This section contains the following parameters:

IS_CA_BOXI_INSTALLED

Specifies if the Report Server is installed on the system.

SiteMinder setting: false

CHOSEN_INSTALL_SET

Specifies the type of installation.

TYPICAL

Installs the Report Server using an embedded version of MySQL and Apache Tomcat to function as a report database and web server, respectively.

CUSTOM

Installs the Report Server using a supported version of SQL Server or Oracle to function as the report database.

Important! Although a custom installation lets you configure an existing instance of MySQL and additional application server types, SiteMinder only supports the embedded version of MySQL and Apache Tomcat. If you install using the custom installation option, be sure to configure only SQL Server or Oracle as a report database and only install the embedded version of Apache Tomcat.

USER_INSTALL_DIR

(Windows) Specifies the location to which the Report Server must be installed.

Note: Be sure that you escape the back slashes in the path with a back slash character.

Example: C:\\Program Files\\CA\\SC\\CommonReporting

BIEK_INSTALL_DIR

(UNIX) Specifies the location to which the Report Server must be installed.

BIEK_SOURCE_DIR

Specifies the location of the cabi folder that is delivered as part of the installation media.

Limit: The path you enter must be relative to the installer executable.

BIEK_PATH_DIR

Specifies the location of the biek folder that is delivered as part of the installation media.

Limit: The path you enter must be relative to the installer executable.

BusinessObjects XI Administrator User

This section lets you specify the password for the default BusinessObjects administrator account. This section contains the following parameter:

BIEK_BO_ADMIN_PASSWORD

Specifies the password for the default BusinessObjects administrator account.

Consider the following password 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

Parameters for non-Windows Operating Systems

This section lets you specify the non-root user account credentials required to install the Report Server on UNIX. This section contains the following parameters:

CABI_NONROOT_USER

Specifies the non-root user the installer must use.

CABI_NONROOT_GROUP

Specifies the group to which the user account belongs.

BIEK_CASHCOMP_USER_DEFINED

Specifies the path to which the CA Shared Components environment variable (CASHComp) must be set.

Central Management Server Port

This section lets you specify the port on which the Central Management Server must listen. This section contains the following parameters:

BIEK_PARAM_CMSPORT

Specifies the port on which the Central Management Server must listen.

Default: 6400

Locale Code

This section lets you specify the installer locale. This section contains the following parameter:

INSTALLER_LOCALE

Specifies the installer locale.

SiteMinder setting: en

Report Database Parameters

This section lets you specify the database type that is to function as the report database and the required credentials to connect to it.

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 SiteMinder does not. For a list of supported database types and versions, see the SiteMinder r12.0 SP2 Platform Support Matrix.

This section contains the following parameters:

BIEK_INSTALL_MYSQL

Specifies if the embedded version of MySQL can be used as the report database.

true

Installs the embedded version of MySQL.

false

Does not install the embedded version of MySQL.

BIEK_CMS_DB_TYPE

Specifies the database type that is to function as the report database.

MYSQL

Specifies that MySQL is to function as the report database.

Important! SiteMinder only supports the embedded version of MySQL.

MSSQL

Specifies that SQL Server is to function as the report database.

ORACLE

Specifies that Oracle is to function as the report database.

BIEK_MYSQL_ROOT

Specifies the password for the MySQL root user.

BIEK_CMS_USER

Specifies the name of the database account that has the necessary privileges to read and write to the report database.

BIEK_CMS_PASSWORD

Specifies the password for the database account.

BIEK_CMS_DB

(MySQL and SQL Server) Specifies the name of the database instance that is to function as the report database.

BIEK_CMS_SRV

(Oracle) Specifies the Oracle Net Service Name that must be used to connect to the report database.

Note: If you are using the embedded version of MySQL, a value for this parameter is not required.

BIEK_CMS_DSN

(SQL Server) Specifies the name of the DSN that must be used to connect to the report database.

BIEK_CMS_PORT

Specifies the port on which the MySQL report database instance must listen.

Note: If you are using the embedded version of MySQL, a value for this parameter is not required.

Audit Database Parameters

This section lets you specify the database type that is to function as the Report Server audit database. The report database can function as the audit database.

Note: The Report Server audit database is used to audit activities specific to the Report Server and is not used for SiteMinder audit-based reports. A SiteMinder audit database is required to run audit-based reports.

This section contains the following parameters:

BIEK_ENABLE_AUDITING

Specifies if Report Server auditing must be enabled.

SiteMinder setting: false

BIEK_AUDIT_USER

Specifies the name of the database account that has the necessary privileges to read and write to the audit database.

Note: A value for this parameter is not required because Report Server auditing is not enabled.

BIEK_AUDIT_PASSWORD

Specifies the password for the database account that has the necessary privileges to read and write to the audit database.

Note: A value for this parameter is not required because Report Server auditing is not enabled.

BIEK_AUDIT_DB

(MySQL and SQL Server) Specifies the name of the database instance that is to function as the audit database.

Note: A value for this parameter is not required because Report Server auditing is not enabled.

BIEK_AUDIT_SRV

(Oracle) Specifies the Oracle Net Service Name that must be used to connect to the audit database.

Note: A value for this parameter is not required because Report Server auditing is not enabled.

BIEK_AUDIT_DSN

(SQL Server) Specifies the name of the DSN that must be used to connect to the audit database.

Note: A value for this parameter is not required because Report Server auditing is not enabled.

BIEK_AUDIT_PORT

Specifies the port on which the MySQL audit database instance must listen.

Note: A value for this parameter is not required because Report Server auditing is not enabled.

Web Server Properties

This section lets you specify the Web Server type to install. This section has the following parameters:

BIEK_INSTALL_TOMCAT

Specifies if an embedded version of Apache Tomcat must be installed.

SiteMinder setting: true

Note: This installs an embedded version of Tomcat. SiteMinder only supports this web server type and version.

BIEK_INSTALL_DOTNET

Specifies if .NET for IIS must be installed.

SiteMinder setting: false

BIEK_INSTALL_SAMPLES

Specifies if sample databases and templates must be installed.

SiteMinder setting: false

Note: The SiteMinder Report Server Configuration wizard installs the required reporting templates. You run the wizard after installing the Report Server.

CABI_WEB_SERVER_TYPE

Specifies the type of web server the Report Server must use.

SiteMinder setting: TOMCAT

Post Install Functions

This section lets you specify additional Apache Tomcat and logging parameters. This section has the following parameters:

BIEK_TOMCAT_DIR

Specifies the installation location for the embedded version of Apache Tomcat.

Default: *report_server_home*\CommonReporting\TomCat

report_server_home

Specifies the Report Server installation path.

BIEK_TOMCAT_CONNECTION_PORT

Specifies the port on which Apache Tomcat must connect and wait for requests.

Default: 8080

BIEK_TOMCAT_REDIRECT_PORT

Specifies the port on which Apache Tomcat must redirect requests.

Default: 8443

BIEK_TOMCAT_SHUTDOWN_PORT

Specifies the port on which the Apache Tomcat SHUTDOWN command must be issued.

Default: 8005

BIEK_DEPLOY_WEBSPHERE_DIR

Specifies the WebSphere target directory.

SiteMinder setting: Do not provide a value for this parameter.

BIEK_DEPLOY_WEBSPHERE_SRV

Specifies the WebSphere server name.

SiteMinder setting: Do not provide a value for this parameter.

BIEK_DEPLOY_WEBLOGIC_DIR

Specifies the WebLogic target directory.

SiteMinder setting: Do not provide a value for this parameter.

BIEK_DEPLOY_WEBLOGIC_PORT

Specifies the port on which the WebLogic server is listening.

SiteMinder setting: Do not provide a value for this parameter.

BIEK_DEPLOY_WEBLOGIC_USER

Specifies the name of the WebLogic server administrator account.

SiteMinder setting: Do not provide a value for this parameter.

BIEK_DEPLOY_WEBLOGIC_PWD

Specifies the password for the WebLogic server administrator account.

SiteMinder setting: Do not provide a value for this parameter.

BIEK_DEPLOY_WEBLOGIC_SRV

Specifies the WebLogic server name.

SiteMinder setting: Do not provide a value for this parameter.

BIEK_DEPLOY_WEBLOGIC_VERSION

Specifies the WebLogic Server version

SiteMinder setting: Do not provide a value for this parameter.

BIEK_LOG_FILE

Specifies the location of the installation log file (ca-install.log).

Note: Be sure that you escape the back slashes in the path with a back slash character.

BIEK_DEBUG_ON

Specifies if debug-level logging must be enabled.

true

Enables debug-level logging.

false

Disables debug-level logging.

USER_REQUESTED_RESTART

(Windows) Specifies that the Windows system automatically restart upon a successful installation.

Yes

Enables the installer to restart the system automatically after a successful installation.

No

Prevents the installer from automatically restarting the system after a successful installation. Manually restart the system to complete the installation.

Modify the 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 SiteMinder audit store.

Note: You do not have to configure a SiteMinder audit database before running the Report Server Configuration Wizard.

Values: 1 or 2

1

Specifies Microsoft SQL Server.

2

Specifies Oracle.

Silently Install the Report Server

You run the Report Server installer silently to install the Report Server without user interaction.

Before You Install

Consider the following 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 based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

- **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.

More information:

[Locate the Installation Media](#) (see page 456)

Windows

To install the Report Server silently

1. Exit all applications that are running.
2. Open a command prompt.

3. Change the directory to *temporary_location*\Disk1\InstData\VM.

temporary_location

Specifies the location to which you copied the installation media.

4. Enter the following command:

```
installation_media -f properties_file -i silent
```

installation_media

Specifies the name of the Report Server installation executable.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in 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 silent installation begins.

UNIX

To install the Report Server silently

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 the CABI folder.
4. Enter the following command:

```
.installation_media -f properties_file -i silent
```

installation_media

Specifies the name of the Report Server executable.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

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 silent installation begins.

Note: If the installation launches into the GUI or console mode, the properties file path may be invalid. Cancel the installation and correct the properties file path.

Silently Install Report Templates

You run a silent installation to install report templates without user input.

Before You Install

You install the SiteMinder report templates using the installation media on the Technical Support site.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in the *Policy Server Release Notes*.

More information:

[Locate the Installation Media](#) (see page 456)

Windows

To install report templates silently

1. Exit all applications that are running.
2. Be sure that the Report Server is [started](#) (see page 318).
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
```

installation_media

Specifies the name of the SiteMinder Report Server Configuration Wizard installation executable.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in 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: To begin creating reports, the Report Server must be registered.

More information:

[How to Register the Report Server](#) (see page 324)

UNIX

You install the SiteMinder report templates using the installation media on the Technical Support site.

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

To install report templates silently

1. Exit all applications that are running.
2. Be sure that the Report Server is [started](#) (see page 318).
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 SiteMinder Report Server Configuration Wizard installation media.

Note: For a list of installation media names based on operating system, see the installation and upgrade considerations in 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: To begin creating reports, the Report Server must be registered.

More information:

[How to Register the Report Server](#) (see page 324)

Appendix E: Configuring the Policy Server for an International Environment

This section contains the following topics:

[Policy Servers in an International Environment](#) (see page 443)

[Planning Considerations Before Installing the Policy Server](#) (see page 443)

[Configure SiteMinder Data Stores Supporting International Characters](#) (see page 449)

Policy Servers in an International Environment

The Policy Server supports SiteMinder data stores residing in an Oracle or SQL Server database, and LDAP servers for an international environment.

Planning Considerations Before Installing the Policy Server

Consider the following before installing the Policy Server:

- Use supported operating system and third-party software
- Create supported databases
 - Before creating databases for storing policy or session data, make sure they are formatted with UTF-8 encoding.
 - User store databases are not limited to UTF-8 encoding. User databases may be created in the local character set encoding.

Example: to store Japanese characters in Oracle 9i, the database can be created in JA16EUC encoding or JA16SJIS encoding.

Note: The Active Directory namespace does not support multi-byte characters. Regardless of the code page you are using, SiteMinder treats characters as they are defined in Unicode. Although your code page may reference a special character as single-byte, SiteMinder treats it as a multi-byte character if Unicode defines it as such.

- All Administrative UI fields support multi-byte characters.
- Some of the FSS Administrative UI fields support multi-byte characters.

- Some Policy Server components support multi-byte and ASCII characters in an internationalized environment.
- SiteMinder supports multi-byte character (MBCS) URLs.

Note: For a list of supported CA and third-party components, refer to the SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support site.

More information:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

User Interface Fields Supporting Multi-byte Characters

The Administrative UI and FSS Administrative UI contain fields that support multi-byte characters. The following sections detail the specific fields.

Administrative UI

All of the fields in the Administrative UI support multi-byte characters.

Federation Security Services Administrative UI

The following FSS Administrative UI dialog box fields support multi-byte characters:

Field Name	Dialog Where Field is Located	Access Dialog By Selecting:
All Description fields	All dialogs	Any dialog that has a Description field
All Name fields except dialogs listed in next column	All dialogs except Name fields in: ■ SiteMinder Agent Dialog ■ SiteMinder Agent Group Dialog ■ SiteMinder Agent Configuration Object Dialog ■ SiteMinder Host Configuration Object Dialog ■ SiteMinder Agent Type Dialog	Access Dialog by selecting: ■ Edit, Create Agent ■ Edit, System Configuration, Create Agent Group ■ Edit, System Configuration, Create Agent Conf Object ■ Edit, System Configuration, Create Host Conf Object ■ Edit, System Configuration, Create Type
DN field under the User Session Caches group	SiteMinder Cache Management Dialog	Tools, Manage Cache
Value and Enter Single Value	SiteMinder Host Configuration	Edit, System Configuration, Create

fields	Object's Edit Parameter Dialog	Host Conf Object, click Add
Root, Start, and End fields for the LDAP and AD namespaces	SiteMinder User Directory Dialog	Edit, System Configuration, Create User Directory
Username field	SiteMinder User Directory Dialog's Credentials and Collection tab	Edit, System Configuration, Create User Directory
Filter (binoculars) fields	SiteMinder Policy Domain Dialog	Edit, System Configuration, Create Domain
Manual Entry field in the Condition group Value field in the Infix Notation group	SiteMinder Password Policy Dialog's SiteMinder User Lookup screen	Edit, System Configuration, Create Password Policy
Function Parameter field of the SiteMinder Active Rule editor dialog	SiteMinder Rule and SiteMinder Global Rule dialogs	Click a realm and select Create Rule Under Realm
- Variable Value field in the Static option. - DN Spec field in the DN Attribute option. - Parameters field in Active Response option.	SiteMinder Response and Global Response dialogs	Click a response and select Create Response
- On the Users tab, the Manual Entry field in Condition group and the Value field in Infix Notation group. - On the Rules tab, the Filter fields (binoculars) of the Set Response and Set Global Response dialogs. - On the Advanced tab, the Function Parameter field in Active Policy group.	SiteMinder Policies and Global Policies dialogs	Click Policies and select Policy
- Value field in Attribute-Value option. - Search Expression field in the LDAP Query option.	SiteMinder User Lookup screen	In multiple dialogs

Policy Server Components Supporting Multi-byte Characters

The following Policy Server components support multi-byte and ASCII characters in an internationalized environment:

- 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
- SiteMinder Test Tool
- Audit logging to text files
- Audit logging to ODBC databases
- smobjexport and smobjimport
- XPSEExport and XPSImport
- Java Agent API

Support for Multi-Byte Character URLs

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:

- 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 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 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 Punny code is used. More information on configuring authentication schemes exists in the *Policy Server Configuration Guide*.

Configure SiteMinder Data Stores Supporting International Characters

You can configure SiteMinder data stores in SQL Server or Oracle databases. When configuring these data stores, be aware that the Policy Server only supports UTF-8 encoding and, as a result, you must use databases that support this encoding type.

Note: This section applies to configuring SiteMinder data stores in relational databases. More information on configuring these stores in LDAP servers exists in LDAP Directory Servers as a Policy Store or Key Store.

Configure an International SiteMinder Data Store in SQL Server

To create policy, keys, session, or key stores, configure a SiteMinder data store in the SQL Server database.

Note: By default, SQL Server supports UTF-8 character encoding.

Configure an International SiteMinder Data Store in Oracle

To configure an international SiteMinder data store in Oracle

1. On the machine where Oracle is installed, create a custom Oracle database that supports UTF-8 character encoding.

Note: For more information and instructions, see Oracle's documentation.

To verify if an existing Oracle database supports UTF-8 character encoding, run the following query:

```
Select * from nls_database_parameters where parameter =  
'NLS_CHARACTERSET'
```

2. Create policy, keys, session, or key stores for the Policy Server, by configuring a SiteMinder data store in the Oracle database.

Solaris/LINUX Red Hat Policy Server Logging UTF-8 Characters to an Oracle Database

A Solaris/LINUX Red Hat Policy Server can log UTF-8 characters to an Oracle audit log database. To enable this configuration, you need to set the following environment variables:

For a simplified Chinese operating system

- LANG=zh_CN.utf8

For a Japanese operating system

- LANG=jp_JP.UTF-8

You set the LANG variable system-wide or just for the Policy server process.

Note: To avoid impacting any other applications, make sure that you set this variable for the Policy Server process only.

Database Driver Variable

- IANAAppCodePage=utf-8

You set this variable in the appropriate data source definition section of the system_odbc.ini file, installed in *<policy_server_installation>/db*.

Oracle Client Settings

Since the Policy Server uses the Oracle wire protocol driver, an Oracle client is not necessary. However, if you need an Oracle SQLPLUS client in your environment to read data from the audit log database, you may have to set one or both of the following environment variables to correctly display the multi-bytes characters:

For a simplified Chinese operating system

- LANG=zh_CN.utf8

For a Japanese operating system

- LANG=jp_JP.UTF-8

For the Oracle SQLPlus Client

- NLS_LANG (For example, NLS_LANG=Japanese_Japan.UTF8)

Note: For more information, see the operating system and database client configuration manual.

Configure a Japanese User Store in SQL Server

Using the smsampleusers_sqlserver.sql file installed with the Policy Server, you can configure a user store in a SQL Server database. This file is installed in the *<siteminder_installation>\db\SQL* directory.

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 SQL Server

1. Edit the smsampleusers_sqlserver.sql file, by doing the following:
 - a. Replace every varchar instance with **nvarchar**.
 - b. Place an **N** before any insert statement with international strings.

Japanese example:

```
insert into SmUser ( UserID , Name, Password,
  LastName, FirstName, ...)
```

```
values (12, N' やまもと ',
'siteminder','guest','guest','guest@mycompany.com...')
```

2. Import the smsampleusers_sqlserver.sql file.

Note: More information on importing the smsampleusers_sqlserver.sql file exists in Sample User Directories.

3. Open the Policy Server User Interface's SiteMinder ODBC Query Scheme dialog and modify the policy store's SQL query scheme by placing an **N** before every %s reference in any = %s statement.

Example: the following sample query scheme statements:

```
select Name, 'User' from SmUser where Name = '%s' Union select Name,  
'Group' from SmGroup where Name = '%s'
```

should become:

```
select Name, 'User' from SmUser where Name = N'%s' Union select Name,  
'Group' from SmGroup where Name = N'%s'
```

4. Stop and restart the Policy Server.

The user store configuration is complete and now supports multi-byte characters.

Configure a Japanese User Store in Oracle

Using the smsampleusers_oracle.sql file installed with the Policy Server, you can configure a user store in an Oracle database. This file is installed in the *<siteminder_installation>\db\SQL* directory.

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 F: Modified Environment Variables

This section contains the following topics:

[Modified Windows Environment Variables](#) (see page 453)

[Modified UNIX Environment Variables](#) (see page 454)

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$$/$lib`
- `NETEGRITY_LICENSE_FILE = %NETE_PS_ROOT%$/license$/license.dat`
- `NETE_JVM_OPTION_FILE =
%NETE_PS_ROOT%$/config$/JVMOptions.txt`
- `NETE_DOC_ROOT=$INSTALL_PATH$$/$netegrity_documents`
- `NETE_PS_OPACK="INSTALLED"`
- `NETE_JRE_ROOT = HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java
Runtime Environment\1.5 in JAVAHOME value`
- `NETE_JAVA_PATH=%NETE_JRE_ROOT%$/bin;%NETE_JRE_ROOT%$/bin
n$/server`
- `NETE_JDK_ROOT = HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java
Development Kit\1.5 in JAVAHOME value`
- `NETE_SHORTCUTS = C:\Documents and Settings\All Users\Start
Menu\Programs\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"`

Appendix G: Platform Support and Installation Media

This section contains the following topics:

[Locate the SiteMinder Platform Support Matrix](#) (see page 455)

[Locate the Bookshelf](#) (see page 456)

[Locate the Installation Media](#) (see page 456)

Locate the SiteMinder Platform Support Matrix

You can find a comprehensive list of the CA and third-party components supported by SiteMinder on the [Technical Support site](#).

To locate the support matrix from the Support site

1. From the Technical Support site, click Enterprise/Small and Medium Business.

The Support for Business and Partners screen appears.

2. Log in to CA Support Online.

The CA Support Online Basic and Enterprise User screen appears.

3. Enter your login credentials, again.

The CA Support Online screen appears.

4. Under Support, click Support By Product.

5. Select CA SiteMinder from the Select a Product Page list.

The CA SiteMinder screen appears.

6. Scroll to the Product Status section and click CA SiteMinder Platform Support Matrices.

Note: You can download the latest JDK and JRE versions at the [Sun Developer Network](#).

Locate the Bookshelf

The SiteMinder bookshelf is available on the

To locate the support matrix from the Support site

1. Go to the CA [Technical Support site](#).
2. If the Get Support tab is not pulled to the front, click Get Support.
3. Under Find Product News and Support, click Product Pages.
The Support by Product page appears.
4. Locate CA SiteMinder in the product list and click the link.
The CA SiteMinder product page appears.
5. Click Bookshelves.
6. Click the link for the release that you require.
The SiteMinder bookshelf main page appears.

Locate the Installation Media

You can find a comprehensive list of the SiteMinder installation media on the [Technical Support site](#).

To locate the support matrix from the Support site

1. From the Technical Support site, click Enterprise/Small and Medium Business.
The Support for Business and Partners screen appears.
2. Log in to CA Support Online.
The CA Support Online Basic and Enterprise User screen appears.
3. Enter your login credentials, again.
The CA Support Online screen appears.
4. Under Support, click Download Center, Products.
The Download Center screen appears.
5. Type CA SiteMinder in the Select a Product field.
6. Select a release from the Select a Release list.

7. Select a service pack from the Select a Gen Level list.
8. Click Go.

The Product Downloads screen appears. All SiteMinder installation executables are listed.

Index

A

Access the OneView Monitor GUI • 347
Active Directory as a Policy Store • 121
Active Directory Information Worksheet • 382
ADAM and AD LDS Server Information • 42, 51, 72, 84
ADAM/AD LDS Prerequisites • 133
Administrative UI • 444
Administrative UI High Availability • 276, 376
Administrative UI Installation Checklist • 264, 362
Administrative UI Installation Options • 262, 357
Administrative UI Installation Requirements • 27, 358
Administrative UI Installation Worksheets • 385
Administrative UI Properties Files • 412
Administrative UI System Requirements • 358
Administrative UI Troubleshooting • 397
Administrative User Interfaces Overview • 20
Administrator Credentials • 275, 375
Adobe Acrobat Reader Won't Install • 408
AE failed to load library 'smjavaapi'. System error • 408
Agents • 19
Allow User Creation in the Configuration Partition • 133
Apache Tomcat Installation • 304
Apache Tomcat Worksheet • 389
API Error Appears • 397
Application Server Information • 425
Application Server Requirements • 359
Audit Database and Report Server Connectivity • 333
Audit Database Parameters • 433
Audit-based Reports Return No Results • 406
Authentication Schemes Supporting MBCS URLs • 449

B

Backup Versions of Obj.conf and Magnus.conf Files • 88
Before You Install • 268, 305, 319, 366, 420, 427, 438, 440
Before You Install the Policy Server • 35, 65

Before You Register the FSS Administrative UI • 289
BusinessObjects XI Administrator User • 431

C

CA Business Intelligence • 18
CA Directory as a Policy Store • 97
CA Directory Information Worksheet • 381
CA Product References • iii
Cannot Find the Administrative UI Registration Log • 401
Cannot Find the Default Logging File • 402
Cannot Register a Policy Server Connection • 397
Central Management Server Port • 431
Configuration Wizard Requirements • 81
Configure a Japanese User Store in Oracle • 452
Configure a Japanese User Store in SQL Server • 451
Configure a Key Store in an Existing Policy Store • 144
Configure a Policy Store • 47, 79
Configure a Separate Key Store • 144
Configure a SQL Server Data Source for SiteMinder • 155, 188, 195, 201, 207
Configure a SQL Server Policy Store • 151
Configure a SQL Server Sample User Directory • 259
Configure an International SiteMinder Data Store in Oracle • 450
Configure an International SiteMinder Data Store in SQL Server • 449
Configure an Oracle Data Source for SiteMinder • 171, 215, 226, 238, 249
Configure an Oracle Policy Store • 165
Configure an Oracle Sample User Directory • 259
Configure Auto Startup • 79
Configure Oracle Data Stores • 212
Configure SiteMinder Data Stores Supporting International Characters • 449
Configure snmptrap.conf • 354
Configure snmptrap.config • 355
Configure SQL Server Data Stores • 186
Configure the Connection to the Administrative UI • 330

- Configure the Connection to the Policy Server • 280
- Configure the OneView Monitor • 342
- Configure the Oracle RAC Wire Protocol Driver • 176, 220, 231, 243, 254
- Configure the Oracle Wire Protocol Driver • 174, 218, 229, 241, 252
- Configure the SNMP Agent on UNIX Systems • 354
- Configure the SNMP Agent on Windows • 352
- Configure the SQL Server Wire Protocol Driver • 156, 190, 196, 203, 209
- Configuring LDAP Directory Servers as a Policy or Key Store • 95
- Configuring SiteMinder Data in a Relational Database • 147
- Configuring the OneView Monitor • 341
- Configuring the Policy Server for an International Environment • 443
- Connectivity Requirements • 31
- Contact CA • iii
- Create a Client Name and Passphrase • 324
- Create a DSA for the Policy Store • 98
- Create a New UNIX Account • 63
- Create a SQL Server Data Source on Windows • 155, 188, 195, 201, 207
- Create a SQL Server Data Sources on UNIX Systems • 156, 189, 196, 202, 208
- Create a Super User Administrator for the DSA • 102
- Create a WebLogic Application Server Instance • 360
- Create an Oracle 10g Table Space for the Policy Store • 166
- Create an Oracle 10g User to Manage the Policy Store's Table Space • 167
- Create an Oracle Data Source on UNIX Systems • 174, 217, 229, 240, 252
- Create an Oracle Data Source on Windows • 171, 215, 226, 238, 249
- Create an Oracle RAC Data Source on Windows • 172, 216, 227, 239, 250
- Create the Audit Log Schema • 194, 226
- Create the Base Tree Structure for Policy Store Data • 102
- Create the Key Store Schema • 188, 215
- Create the Policy Store Schema • 99, 115, 125, 137

- Create the Registration Credentials for the FSS Administrative UI • 291
- Create the Session Store Schema • 207, 249
- Create the SiteMinder Schema • 154, 170
- Create the Token Store Schema • 201, 238

D

- Default Log File does not Provide Enough Information • 403
- Default Properties Files • 412
- Delete a Policy Server Connection • 281
- Delete a Report Server Connection to the Administrative UI • 338
- Disable Servlets in Sun Java System 6.0 • 344

E

- Enable Multi-byte Character Support • 448
- Enable or Disable ObjectCategory Attribute Support • 132
- Enable SNMP event trapping • 355
- Enable SNMP Event Trapping • 46, 353
- End User Licensing Agreement • 424

F

- Federation Security Services Administrative UI • 17, 444
- FIPS Considerations • 38, 68
- Fix Modified UNIX/Sun Java System Web Server Configuration Files • 395
- FSS Administrative UI does not appear on Windows • 404
- FSS Administrative UI Fails to Start in IE • 404
- FSS Administrative UI Fails to Start on a Sun Java Web Server • 405
- FSS Administrative UI Troubleshooting • 403

G

- Gather Application Server Information • 363
- Gather Database Information • 152, 168, 187, 193, 200, 206, 212, 224, 236, 247
- Gather Directory Server Information • 97, 110, 122, 134
- Gather Information for the Configuration Wizard • 49, 82
- Gather Information for the Installer • 40, 70, 265, 302, 317
- Gather Registration Information • 279, 327
- General Information • 423, 424
- General Policy Server Information • 414

Global Zone Support • 61

H

How the Reports Installation Works • 301
How to Configure Additional Policy Server Connections • 276
How to Configure an Audit Database • 331
How to Configure SNMP Event Trapping on UNIX Systems • 355
How to Configure SNMP Event Trapping on Windows • 353
How to Configure the OneView Monitor GUI on UNIX/Sun Java System • 344
How to Configure the OneView Monitor GUI on Windows/IIS • 343
How to Configure the Policy Store • 98, 111, 123, 135, 153, 169
How to Enable MBCS URL Support • 447
How to Install the Administrative UI • 264, 363
How to Install the Policy Server • 35, 66
How to Install the Report Server • 302
How to Install the Report Templates • 317
How to Prepare for the Policy Server Installation • 63
How to Register the Administrative UI • 272, 369
How to Register the FSS Administrative UI • 290
How to Register the Report Server • 324
How to Silently Install a Policy Server • 413
How to Silently Install Reports • 429
How to Silently Install the Administrative UI • 422
How to Store Audit Logs in Oracle • 224
How to Store Audit Logs in SQL Server • 193
How to Store Key Information in Oracle • 212
How to Store Key Information in SQL Server • 187
How to Store Session Information in Oracle • 247
How to Store Session Information in SQL Server • 206
How to Store Token Data in SQL Server • 199
How to Store Token Information in Oracle • 235
How to Uninstall Reporting • 335
How to Uninstall the Documentation • 92
How to Uninstall the Policy Server • 54, 88
How to use the Configuration Wizard • 81
How to Use the Configuration Wizard • 48
HPUX • 352

I

Import the Default Policy Store Objects • 106, 117, 127, 139, 161, 182
Import the Policy Store Data Definitions • 107, 118, 128, 140, 162, 183
Important Considerations • 97, 149
Increase the Job Server Service Timeout Value • 322
Increase the Timeout Value on UNIX • 323
Increase the Timeout Value on Windows • 322
Install ServletExec/AS on UNIX/Sun Java System • 345
Install ServletExec/ISAPI on Windows 2003/IIS • 343
Install the Administrative UI • 267, 366
Install the Bookshelf on UNIX • 22
Install the Bookshelf on Windows • 21
Install the Policy Server in Console Mode • 76
Install the Policy Server in GUI Mode • 74
Install the Report Server • 305
Install the Report Templates • 319
Install WebLogic • 360
Install WebSphere • 361
Installation Credentials • 302
Installation Credentials Worksheet • 387
Installation Options • 430
Installation Overview • 15
Installation Road Map • 34, 60, 96, 148, 261, 288, 295
Installation Worksheets • 379
Installing Reports • 295
Installing the Administrative UI • 261
Installing the Administrative UI to an Existing Application Server • 357
Installing the Policy Server on UNIX Systems • 59
Installing the Policy Server on Windows Systems • 33
Intended Audience • 15
Invalid Registration File Error Appears • 399

J

Java Error Messages When Uninstalling • 407
JBoss as an Application Server • 360
JBoss Information • 364, 425
JBoss Worksheet • 385

L

- LDAP Directory Servers as a Policy or Key Store • 95
- LDAP Policy Store • 417
- Limitation of OneView Monitor GUI/IIS Web Agent on Same Machine • 342
- Linux • 352
- Locale Code • 432
- Locate the Bookshelf • 456
- Locate the Installation Media • 456
- Locate the SiteMinder Platform Support Matrix • 455
- Log into the FSS Administrative UI • 292

M

- Microsoft ADAM/AD LDS as a Policy Store • 132
- Microsoft ADAM/AD LDS Information Worksheet • 383
- Microsoft ADAM/AD LDS Server Information Worksheet • 380
- Modified Environment Variables • 453
- Modified UNIX Environment Variables • 454
- Modified Windows Environment Variables • 453
- Modify the Administrative UI Installer Properties File • 424
- Modify the Default Policy Server Connection • 281
- Modify the Policy Server Installer Properties Files • 414
- Modify the Prerequisite Installer Properties File • 423
- Modify the Report Server Properties File • 429
- Modify the SiteMinder Report Server Configuration Wizard Properties File • 437
- Modify the UNIX System Parameters • 63
- Monitor a Policy Server Cluster • 347
- MySQL Report Database • 303
- MySQL Report Database Worksheet • 388

N

- NETE_PS_ALT_CONF_FILE Environment Variable on Solaris • 391

O

- ODBC Policy Store Import Fails with UserDirectory Error • 394
- OneView Monitor GUI • 416
- OneView Monitor Information • 41, 50, 71, 83

- OneView Monitor Information Worksheet • 379
- OneView Monitor Overview • 341
- OneView Monitor Troubleshooting • 395
- Open the DSA • 101
- Oracle Database Information • 169, 213, 225, 237, 248
- Oracle Information Worksheet • 384
- Oracle RAC Database Information • 169, 214, 225, 237, 248
- Oracle RAC Information Worksheet • 384
- Oracle Report Database • 304
- Oracle Report Database Worksheet • 388
- Oracle Schema Files • 151

P

- Parameters for non-Windows Operating Systems • 431
- Patch the ADAM Server • 133
- Planning Considerations Before Installing the Policy Server • 443
- Platform Support and Installation Media • 455
- Point the Policy Server to Database • 191, 222
- Point the Policy Server to the Database • 158, 179, 198, 210, 234, 257
- Point the Policy Server to the Directory Server • 114, 123, 135
- Point the Policy Server to the Policy Store • 103
- Point the Policy Store to the Database • 204, 245
- Policy and Data Store Worksheets • 381
- Policy Server • 16
- Policy Server Component Considerations • 36, 66
- Policy Server Components Supporting Multi-byte Characters • 445
- Policy Server Configuration Wizard • 47, 80
- Policy Server Fails to Start After Installation • 392
- Policy Server Features • 415
- Policy Server Installation Requirements • 25
- Policy Server Properties File • 412
- Policy Server Registration Worksheet • 387
- Policy Server System Requirements • 25
- Policy Server Troubleshooting • 391
- Policy Server Worksheets • 379
- Policy Servers in an International Environment • 443
- Policy Store • 17
- Policy Store Considerations • 38, 49, 68, 82

- Policy Store Troubleshooting • 393
- Policy Stores with Large Numbers of Objects • 393
- Post Install Functions • 435
- Pre-Installation Checklist • 23
- Prepare for the Administrative UI Registration • 108, 119, 129, 141, 163, 184
- Prepare for Web Agent Installation • 284
- Pre-registration Checklist • 289
- Prerequisite Installer Worksheet • 385
- Prerequisites for an Oracle 10g Database • 166
- Prerequisites for Windows and UNIX Systems • 351
- Prerequisites to Installing ServletExec • 344
- Prerequisites to Installing ServletExec on Windows • 343
- Problem With Using Active Directory as a User Store • 408
- Protect a Resource with MBCS URLs • 448

R

- Register the Administrative UI • 274, 373
- Register the Audit Database with the Administrative UI • 332
- Register the Report Server with the Policy Server • 327
- Registering the Federation Security Services Administrative UI • 287
- Registering the FSS Administrative UI • 287
- Registration Fails without Timeout • 400
- Registration Not on File Error Appears • 398
- Reinstall the Policy Server • 53
- Reinstall the Report Server • 339
- Relational Databases as a Policy or Key Store • 147
- Remove Leftover Items • 56
- Remove Leftover Services • 56
- Remove Policy Server References from Agent Host Files • 55, 89
- Remove SiteMinder References from IWS • 91
- Remove SiteMinder References from StartServletExec • 92
- Remove UNIX Items • 338
- Remove Windows Items • 337
- Replicate the Policy Store on Sun Java System Directory Server Enterprise Edition • 113
- Report Database and Audit Database • 299
- Report Database Parameters • 432
- Report Database Requirements • 30

- Report Server • 297
- Report Server Configuration Worksheet • 389
- Report Server Installation Fails with Error Regarding Characters • 406
- Report Server Installation Options • 297
- Report Server Installation Requirements • 29
- Report Server Registration Worksheet • 389
- Report Server Troubleshooting • 406
- Reporting Considerations • 300
- Reporting Installation Checklists • 297
- Reporting Properties File • 413
- Reporting Worksheets • 387
- Required Information • 40, 70, 82, 168, 213, 224, 236, 247
- Required Information Worksheet • 379
- Reset the Administrative UI Registration Window • 265, 370
- Restart the Policy Server • 119, 129, 141, 163, 184, 192, 199, 205, 211, 223, 235, 246, 258
- Restart the Report Server • 329
- Restart the SNMP Daemon • 79
- Run the Configuration Wizard • 53
- Run the Configuration Wizard in Console Mode • 87
- Run the Configuration Wizard in GUI Mode • 86
- Run the Policy Server Installer • 44, 419
- Run the Registration Tool • 277

S

- Sample SiteMinder Installation • 15
- Sample User Directories • 258
- Schema Files for Relational Databases • 149
- Scripting Interface • 57, 93
- Search Fails with Timeout Error • 401
- Server Information • 423
- Set Permissions for IIS Users After Installing ServletExec • 344
- Set the JRE in the Path Variable • 54
- Set the JRE in the PATH Variable • 89, 92
- Set the JRE in the PATH Variable on Solaris • 407
- Set the JRE in the PATH Variable on Windows • 407
- Set the SiteMinder Super User Password • 103, 116, 126, 138, 159, 180
- Silent Installation • 411
- Silent Installation Guidelines • 411
- Silently Install Report Templates • 440
- Silently Install the Administrative UI • 426
- Silently Install the Report Server • 438

- SiteMinder Administrative UI • 17
- SiteMinder Audit Database • 19
- SiteMinder Documentation • 20
- SiteMinder Key Database Information • 40, 49, 70, 83
- SiteMinder Key Store Overview • 144
- SM Key Database Information Worksheet • 381
- smlldapsetup and Sun Java System Directory Server Enterprise Edition • 112
- SNMP Password • 416
- SNMP Support • 349
- SNMP Support Overview • 349
- Solaris • 352
- Solaris 10 Zone Support • 61
- Solaris and HP-UX Patches • 62
- Solaris Required Patch Clusters • 30
- Solaris/LINUX Red Hat Policy Server Logging UTF-8 Characters to an Oracle Database • 450
- Sparse-root Zone Support • 61
- SQL Server Information Worksheet • 383
- SQL Server Report Database • 303
- SQL Server Report Database Worksheet • 388
- SQL Server Schema Files • 150
- SSL initialization failed
 - error -8174 (security library bad database.) • 393
- Start the Application Server • 273, 372
- Start the OneView Monitor Service • 347
- Start the Report Server • 318
- Stop all SiteMinder Processes • 90
- Stop an Unattended Policy Server Installation • 422
- Stop and Restart the Policy Server • 356
- Stop the Application Server • 275, 374
- Stop the Report Server • 334
- Sun Java System Directory Server as a Policy Store • 110
- Sun Java System Directory Server Information • 43, 52, 73, 85
- Sun Java System Directory Server Information Worksheet • 380, 382
- Sun ONE LDAP Directory Server Considerations • 112
- Support for Active Directory ObjectCategory Indexing Attribute • 131
- Support for Multi-Byte Character URLs • 446
- System Requirements • 27, 29
- System Requirements for OneView Monitor • 342

T

- Test SNMP Gets for HP-UX • 356
- Test SNMP Gets for Red Hat Enterprise Linux Advanced Server • 356
- Troubleshoot the Administrative UI Installation • 272
- Troubleshoot the Policy Server Installation • 46, 78, 421
- Troubleshoot the Report Server Installation • 316
- Troubleshooting • 391
- Trusted Relationship with a Policy Server • 263, 362

U

- Unattended Administrative UI Installation • 282
- Unattended Installation • 411
- Unattended Policy Server Installation • 47, 80
- Uninstall the Administrative UI on UNIX • 283, 377
- Uninstall the Administrative UI on Windows • 282, 376
- Uninstall the Documentation • 57, 93
- Uninstall the Policy Server • 55, 90
- Uninstall the Policy Server and Documentation • 54, 88
- Uninstall the Report Server Configuration Wizard from UNIX • 337
- Uninstall the Report Server Configuration Wizard from Windows • 336
- Uninstall the Report Server from UNIX • 336
- Uninstall the Report Server from Windows • 335
- UNIX • 26, 28, 30, 359, 421, 428, 439, 441
- UNIX Console • 271, 321, 369
- UNIX Console Custom Installation • 314
- UNIX Console Typical Installation • 308
- UNIX GUI • 270, 320, 368
- UNIX GUI Custom Installation • 311
- UNIX GUI Typical Installation • 307
- UNIX Systems Prerequisites • 351
- Unset Localization Variables • 64
- Unset the LANG Environment Variable • 64
- Use the SiteMinder Bookshelf • 23
- User Interface Fields Supporting Multi-byte Characters • 444

V

- Verify the CA Directory Cache Configuration • 105
- Verify the WebLogic Domain • 361
- Verify WebSphere is Working • 361

W

- Web Browser Requirements for MBCS URLs • 447
- Web Server Properties • 434
- Web Server Requirements for MBCS URLs • 447
- WebLogic as an Application Server • 360
- WebLogic Information • 364, 426
- WebLogic Worksheet • 386
- WebSphere as an Application Server • 361
- WebSphere Information • 365, 426
- WebSphere Worksheet • 386
- Whole-root Zone Support • 62
- Windows • 25, 27, 29, 269, 320, 358, 367, 420, 427, 438, 440
- Windows Custom Installation • 310
- Windows Prerequisites • 351
- Windows Typical Installation • 305
- Windows/IIS Virtual Path to /sitemindermonitor Does Not Exist • 396
- Winsock error 10054 message • 392