CA SiteMinder®

Upgrade Guide

r12.0 SP2

CA Product References

This document references the following CA products:

- CA SiteMinder®
- CA SOA Security Manager
- CA Security Command Center
- eTrust® Audit iRecorder for 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: Planning an Upgrade

This section contains the following topics:

SiteMinder Documentation

SiteMinder documentation is now available through a 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.

You continue to install SiteMinder product documentation separately. This guide references other SiteMinder guides. We recommend that you install the documentation before beginning an upgrade.

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 136)

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 136)

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.html

The bookshelf opens.

5. Add the bookshelf to your Internet Explorer favorites or create a Mozilla Firefox bookmark to return to the bookshelf.

Component Versions in this Guide

This guide details the paths for upgrading a SiteMinder environment to r12.0 SP2. An upgrade to r12.0 SP2 is supported from the following versions:

- r6.0 base and higher
- r12.0 base and higher

The component versions in this guide include the following:

- CA SiteMinder Administrative UI upgrades from r12.x. In this guide:
  - r12.x is r12.0 SP1.
- Policy Server and policy store upgrades from r6.x and r12.x. In this guide:
  - r6.x is r6.0, r6.0 SP1, r6.0 SP2, r6.0 SP3, r6.0 SP4, and r6.0 SP5.
  - r12.x is r12.0 and r12.0 SP1.
- CA Business Intelligence Common Reporting component (Report Server) upgrades from r12.x. In this guide:
  - r12.x is r12.0 and r12.0 SP1.
- Web Agent upgrades from r6.x and r12.x. In this guide:
  - r6.x is r6.0, r6.x QMR 1, r6.x QMR 2, r6.x QMR 3, r6.x QMR 4, and r6.x QMR 5.
  - r12.x is r12.0 and r12.0 SP1.

Upgrade Paths

An upgrade consists of deploying r12.0 SP2 components to an existing SiteMinder environment. Upgrading to r12.0 SP2 can be accomplished in two ways:

- Completing a migration.
- Configuring a parallel r12.0 SP2 environment beside an existing environment. Both environments use one or more key stores to maintain single sign-on.

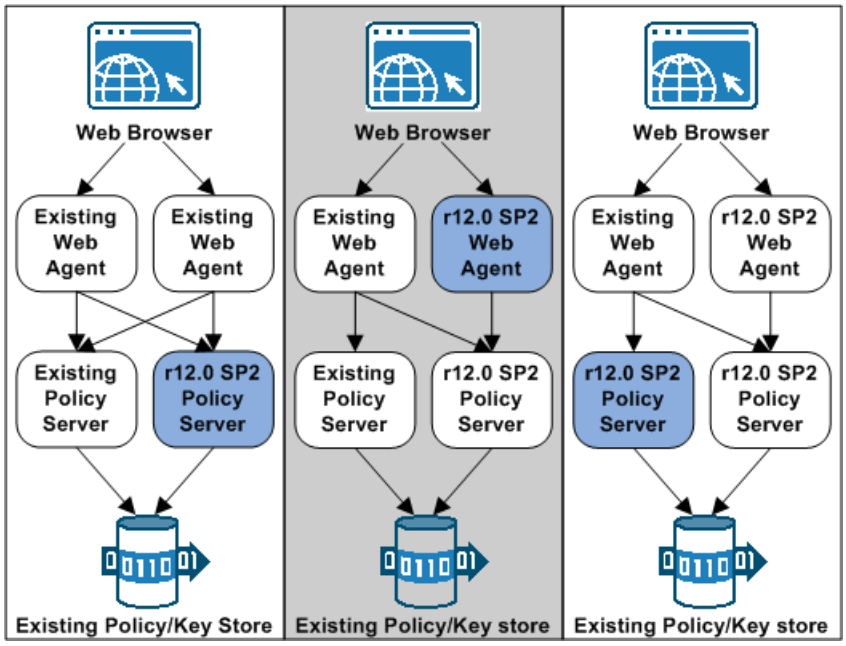
Migration

A migration is the process of upgrading individual SiteMinder components until your environment is operating at r12.0 SP2. Upgrading individual components consists of one or more steps during which you:

- Take a component offline.
- Upgrade the component.
- Bring the component online.

You upgrade individual components over an extended period to maintain system availability. A key to maintaining system availability is the order in which you upgrade components. During a migration, specific components that have been upgraded can continue to communicate with prior versions. This type of communication is known as mixed-mode support.

The following illustrates the concept of a migration. For more information about migrating from r6.x or r12.0 SP1, see the respective chapter:

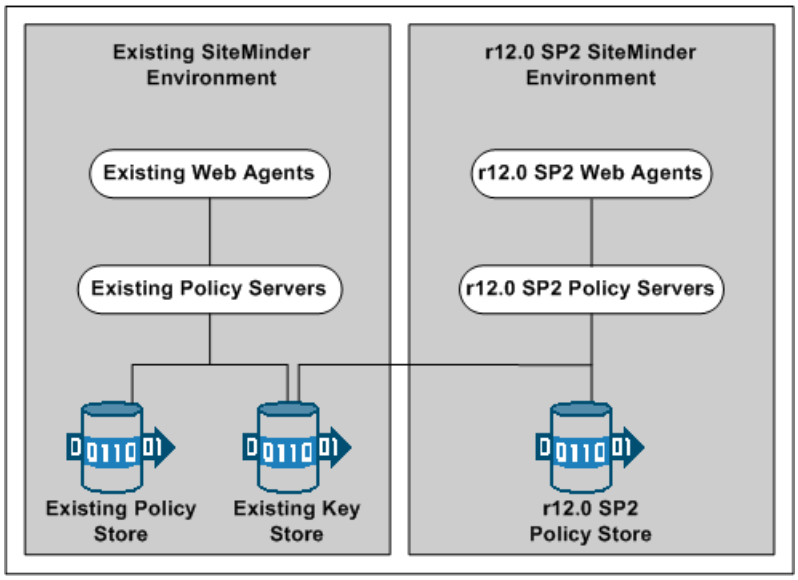


Parallel Upgrade

A parallel upgrade is the process of configuring an r12.0 SP2 environment beside an existing environment. Configuring a parallel upgrade consists of multiple steps during which you:

- Leave the existing environment unchanged
- Configure an r12.0 SP2 environment
- Use a common key store or multiple key stores to enable single sign–on between both environments

The following illustrates the concept of a parallel upgrade. For more information about completing a parallel upgrade from r6.x or r12.x, see the respective chapter.



How to Plan a Migration

Migrating a complex SiteMinder environment involves many component upgrades before the environment is upgraded. A migration strategy is critical so that the migration is completed efficiently and without exposing sensitive resources to security risks or downtime.

A migration strategy can consist of the following:

- A test environment

  Perform a test migration to become familiar with the process. A test migration can help you identify, troubleshoot, and avoid issues that can bring down mission-critical resources when you migrate a production environment.

- Current third-party products and hardware

  Determine if r12.0 SP2 supports your current third-party products and hardware.

  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.

- A site analysis

  Determine the current state of your SiteMinder environment and when it is the best time to update each component.

- SiteMinder Components

  List the individual SiteMinder components that you plan on upgrading and identify where each component is being hosted.

- A recovery plan

  Back up your existing components in the case you experience problems during the migration.

- Upgrade paths

  Determine the individual component upgrade paths supported by a migration.

- Mixed–mode support

  Develop an understanding of mixed mode support.

- Performance testing

  Develop a strategy to performance test the environment when the migration is complete.

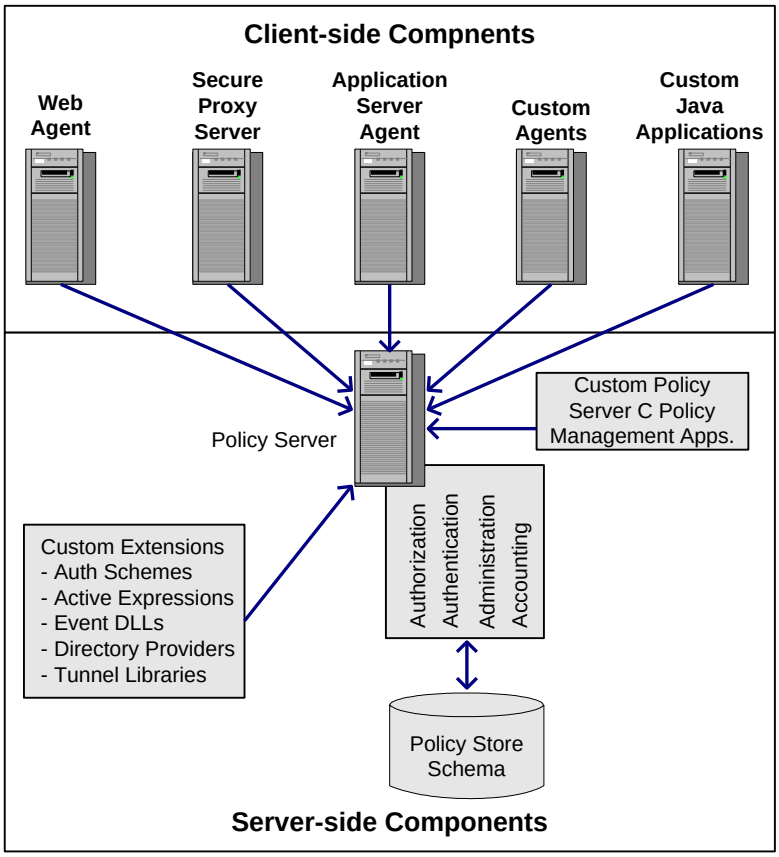
Analyze Your SiteMinder Environment

Analyze your SiteMinder environment to determine the complexity of your migration. Consider the following questions:

Question	Recommendation
How many Policy Server and Agents running in your environment?	Use the Policy Server audit logs to determine the number.

Question	Recommendation
What are the versions of the Policy Server and Agents?	Use the Policy Server audit logs to determine the versions.
Which Policy Servers are communicating with which Web Agents?	Use the Policy Server audit logs to determine this information.
What time of day do you encounter the least traffic at each site?	Review your web server logs and the Policy Server audit logs.
Are your Web Agents working in failover or round robin mode?	To maintain failover and round robin, refer to Mixed SiteMinder Environments.
Are you using single sign–on across the SiteMinder environment?	See this guide for more information about maintaining single sign–on.
Are you using credential collectors for authentication schemes?	See the *Web Agent Configuration Guide* for more information about using credential collectors in a mixed environment.
Does r12.0 SP2 support your third–party hardware and software?	See the SiteMinder r12.0 SP2 Platform Support Matrix on the Technical Support Site.
Do you have SiteMinder software that Professional Services customized?	Contact Customer Support for instructions.
Do you have access to previous versions of SiteMinder documentation? This guide refers to the previous SiteMinder documentation.	Locate the SiteMinder documentation on the Technical Support Site.
Do you have any customized files that can be overwritten by the upgrade?	Back up customized files before beginning the migration.

The following figure shows SiteMinder components to consider before upgrading:



More information

Locate the SiteMinder Platform Support Matrix (see page 135)
Locate the Bookshelf (see page 136)

Plan a Recovery Strategy

Implement a recovery plan that lets you return to your original configuration. You cannot revert from a component upgrade or a migration.

Important! The most complete recovery plan is to back up entire image of each Policy Server and Web Agent host. We recommend this method.

If you do not want to back up the entire image of each system, do the following:

- Back up all Web Agent and Policy Server binaries. Most of these files are in the bin subdirectory where you installed the Policy Server and Web Agent.
- Back up the Web Agent configuration file (WebAgent.conf).

  If you intend to manage Agents centrally from an r12.0 SP2 Policy Server, give the Agent configuration file to the Policy Server administrator. The Administrator needs this file to create an Agent Configuration Object.

  Note: For more information about centrally managing Web Agents, see the *Policy Server Configuration Guide*.
- If you are migrating from r6.x, export the policy store in clear–text to a file using the smobjexport utility.

  Exporting the policy store in clear-text provides you with a record of encrypted information, such as shared secrets. You can use this information to troubleshoot problems. If your key store resides in the policy store, use the -k option with the smobjexport utility. This option includes keys with the exported information.
- If you are migrating from r12.0 SP1, export the policy store to a file using the XPSExport utility.
- Copy the r6.x or r12.x installation scripts, hot fixes, and service packs so you can re–install if necessary. You can download copies from the Technical Support site.

More information:

Locate the Installation Media (see page 136)

Determine the Upgrade Path

A site can contain a combination of the following components during a migration:

- r6.x and r12.0 SP2 components
- r12.0 SP1 and r12.0 SP2 components

The following table lists the supported Policy Server upgrade paths for a migration to r12.0 SP2:

Policy Server Versions	Upgrade To
r6.0	r12.0 SP2
r6.0 SP1	r12.0 SP2
r6.0 SP2	r12.0 SP2

Policy Server Versions	Upgrade To
r6.0 SP3	r12.0 SP2
r6.0 SP4	r12.0 SP2
r6.0 SP5	r12.0 SP2
r12.0 SP1	r12.0 SP2

The following table lists the supported Web Agent upgrade paths for a migration to r12.0 SP2:

Web Agent Versions	Upgrade To
r6.0	r12.0 SP2
r6.x QMR 1	r12.0 SP2
r6.x QMR 2	r12.0 SP2
r6.x QMR 3	r12.0 SP2
r6.x QMR 4	r12.0 SP2
r6.x QMR 5	r12.0 SP2
r12.0 SP1	r12.0 SP2

Note: Upgrade any Web Agent acting as a forms or SSL credential collector last.

The following table lists the supported Administrative UI upgrade path for a migration to r12.0 SP2:

Administrative UI Versions	Upgrade To
r12.0 SP1	r12.0 SP2

The following table lists the supported Report Server upgrade path for a migration to r12.0 SP2:

Report Server Versions	Upgrade To
r12.0	r12.0 SP2
r12.0 SP1	r12.0 SP2

Mixed SiteMinder Environments

As you migrate to r12.0 SP2, your environment can contain a combination of SiteMinder components at different versions. In addition, you do not have to upgrade all of your components to r12.0 SP2. You can leave some components at the current version. Consider the following:

- If your environment contains a combination of r6.x components, r12.0 SP2 Policy Servers can continue to communicate with r6.x policy stores.
- If your environment contains a combination of r12.0 SP1 components, r12.0 SP2 Policy Servers can continue to communicate with r12.0 SP1 policy stores.
- If you have a mix of Policy Server versions, users can continue to access resources and have the same experience using r6.x QMR x or r12.0 SP1 Agents.
- A mixed environment can support single sign-on.

Use Mixed-Mode Support

Mixed-mode support lets an r12.0 SP2 Policy Server communicate with an r6.x or r12.0 SP1 policy store during a migration. When you upgrade a Policy Server, the Policy Server installer detects that policy store version. If the policy store is operating at a previous version, the installer upgrades the Policy Server and enables mixed (compatibility) mode.

Note: You cannot turn mixed-mode off.

The Policy Server Management Console lets you see what policy store version the r12.0 SP2 Policy Server is using.

To identify the policy store version

1. Start the Policy Server Management Console.
2. Click the Data tab.
3. Select Help, About.

   The About the Policy Server Management Console screen appears. The Policy Server version is listed.

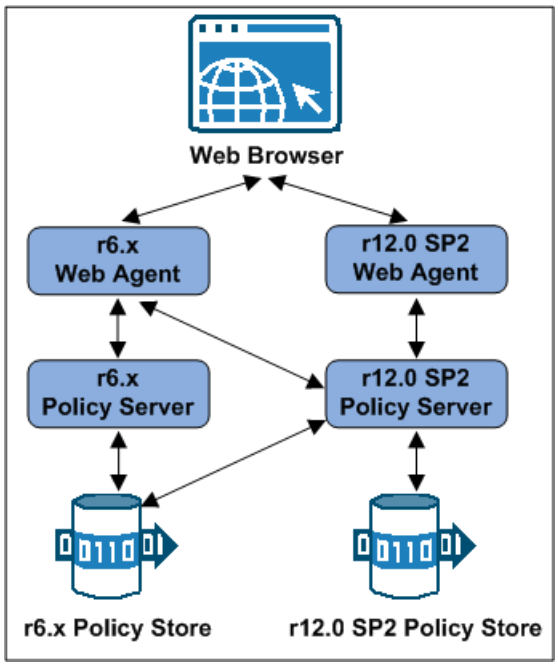
Note: The policy store version is also listed. The policy store version does not match the Policy Server version.

6.x Mixed Mode Support

Consider the following when migrating from r6.x to r12.0 SP2:

- An r6.x Policy Server cannot communicate with an r12.0 SP2 policy store.
- An r12.0 SP2 Policy Server can communicate with an r6.x policy store.
- An r6.x and r12.0 SP2 Policy Server can share the same key store.
- An r6.x and r12.0 SP2 Policy Server can share the same session store.
- An r6.x Web Agent can communicate with an r12.0 SP2 Policy Server.

The following illustration details r6.x mixed mode support:



Limitations of a 6.x Mixed Environment

An r12.0 SP2 Policy Server can communicate with an r6.x policy store, but an r6.x Policy Server cannot connect to an r12.0 SP2 policy store. As a result, all existing r6.x features are available in a mixed environment, but the features specific to r12.0 SP2 are not available.

The following table lists these features:

Feature	Description	Available in Mixed-Mode?
Federal Information Processing Standard (FIPS) 140-2 Support	Use of FIPS 140-2 compliant algorithms	No

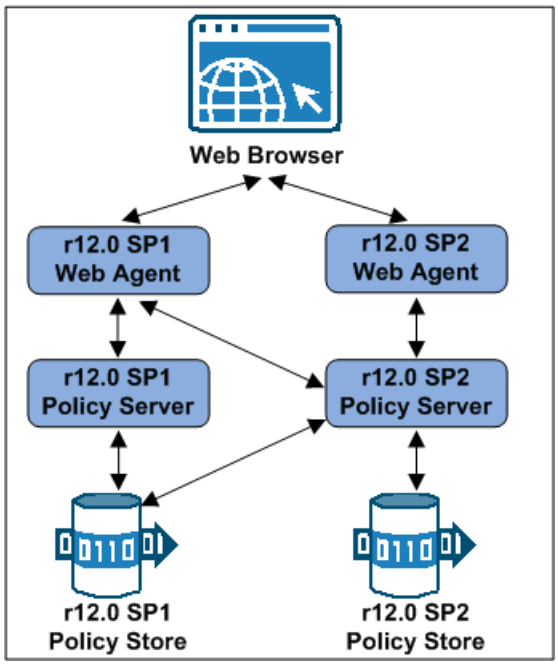
Feature	Description	Available in Mixed-Mode?
Note: FIPS is a US government computer security standard used to accredit cryptographic modules that meet the Advanced Encryption Standard (AES).		
Enterprise Policy Management (EPM)	EPM is an application-centric way to create policies, which requires the r12.0 SP2 Administrative UI.	No
IPv6 Support	Use of the IPv6 TCP/IP protocol	No

r12.0 SP1 Mixed Mode Support

Consider the following when migrating from r12.0 SP1 to r12.0 SP2:

- An r12.0 SP1 Policy Server cannot communicate with an r12.0 SP2 policy store.
- An r12.0 SP2 Policy Server can communicate with an r12.0 SP1 policy store.
- An r12.0 SP1 and r12.0 SP2 Policy Server can share the same key store.
- An r12.0 SP1 and r12.0 SP2 Policy Server can share the same session store.
- An r12.0 SP1 Web Agent can communicate with an r12.0 SP2 Policy Server.

The following illustration details r12.0 SP1 mixed mode support:



Limitations of an r12.0 SP1 Mixed Environment

An r12.0 SP2 Policy Server can communicate with an r12.0 SP1 policy store. As a result, all existing r12.0 SP1 features are available in a mixed environment.

Note: A mixed environment does not affect r12.0 SP2 features.

How to Plan a Parallel Upgrade

Configuring a parallel SiteMinder environment beside an existing environment involves installing the following:

- One or more Policy Servers
- A policy store
- An Administrative UI
- One or more Web Agents
- CA Business Intelligence (Report Server)

Note: This guide lists the requirements for establishing single sign-on between both environments. For more information about installing a Policy Server, a policy store, an Administrative UI, and the Report Server, see the *Policy Server Installation Guide*. For more information about installing a Web Agent, see the *Web Agent Installation Guide*.

How to Upgrade Simple Test Environments

You follow the upgrade paths detailed in this guide only if you must maintain single-sign on or failover.

If your test environment does not require the latter, the most efficient way to upgrade is to:

1. Install an r12.0 SP2 Policy Server.

   Note: Be sure that you install a new Policy Server. Do not upgrade the existing Policy Server. For more information about installing a Policy Server, see the *Policy Server Installation Guide*.

2. Do one of the following:

   - If you are upgrading from r6.x, use smobjexport to export data from the r6.x policy store.
   - If you are upgrading from r12.x, use XPSExport to export data from the r12.x policy store.

   Note: For more information about using either utility, see the *Policy Server Administration Guide*.

3. Do one of the following:

   - If you are upgrading from r6.x, use smobjimport to import the r6.x policy store data into the r12.0 SP2 policy store.
   - If you are upgrading from r12.x, use XPSImport to import the r12.x policy store data into the r12.0 SP2 policy store.

   Note: For more information about using either utility, see the *Policy Server Administration Guide*.

4. Uninstall SiteMinder r6.x or r12.x.

Common SiteMinder Environments

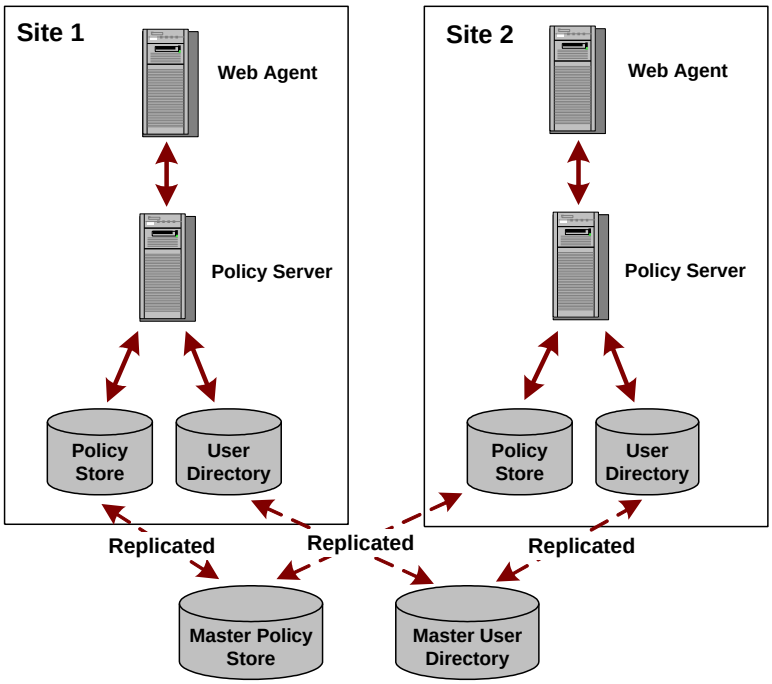
There are several common SiteMinder environments to consider before upgrading to r12.0 SP2. See if your site matches one of the following:

- Single Policy Store, Multiple Policy Servers and Web Agents (see page 24)
- Clustered Environment (see page 25)
- Shared User Directory Environment (see page 26)

Single Policy Store, Multiple Policy Servers and Web Agents

This SiteMinder environment contains a single policy store used by 20 to 100 Policy Servers located across the world. For performance reasons, the policy store and user directories are automatically replicated so that each Policy Server communicates with the closest replicated version. Each Policy Server communicates with 50 to 300 Web Agents.

The following figure illustrates this environment on a smaller scale:



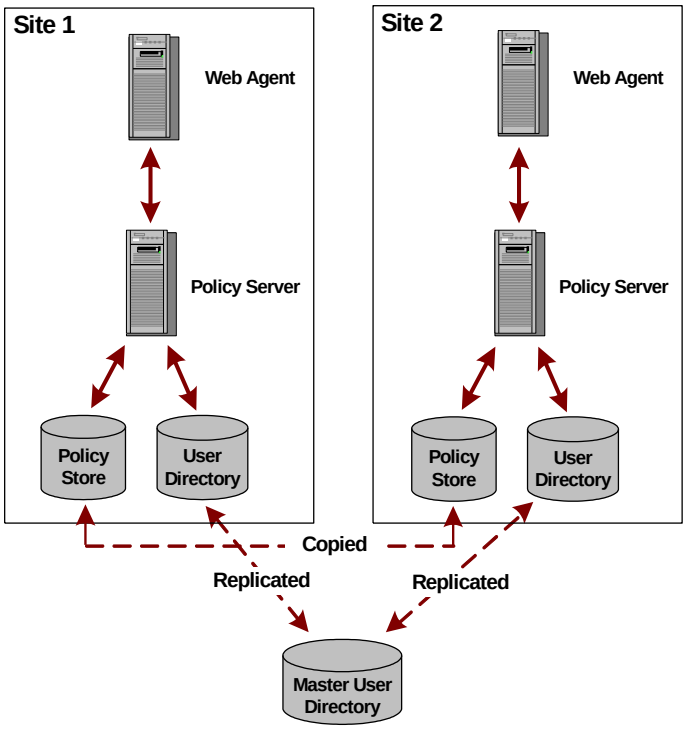
Use the procedures outlined in this guide to upgrade this environment.

Clustered Environment

A clustered environment is similar to the SiteMinder environment with a single policy store and multiple Web Agents and Policy Servers. However, in a cluster, the policy stores are copied, not replicated, the difference being that a copied store is a snapshot of the policy store at a specific point in time; it is not dynamically updated. A replicated store is updated automatically. Typically a change is made to a primary database and then the changes are propagated to secondary databases.

In addition, you can upgrade one cluster site independently from another and still maintain single sign-on between them.

The following figure illustrates the clustered environment on a smaller scale:

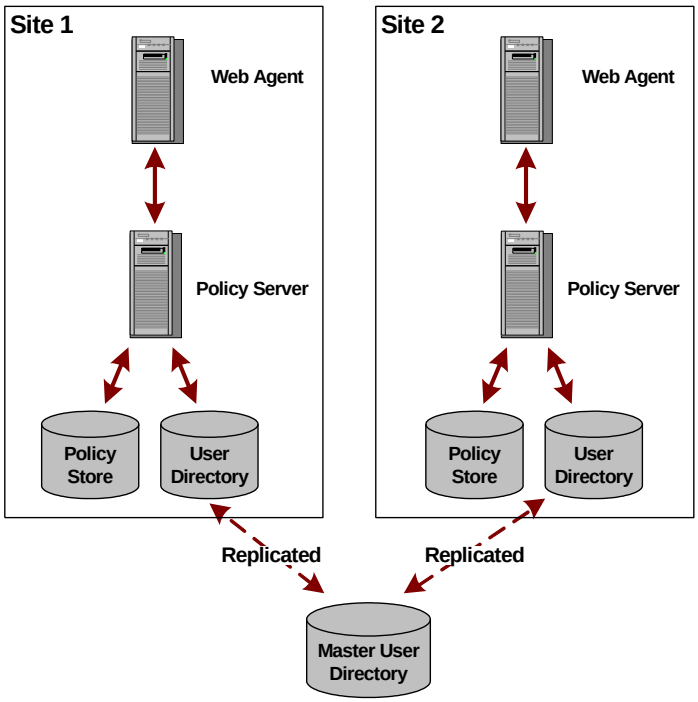


Use the procedures outlined in this guide to upgrade this environment.

Shared User Directory Environment

In this environment, two sites have multiple Web Agents and multiple Policy Servers, but they maintain their own set of policies stored in two separate policy stores. These sites maintain single sign-on by replicating the same master user directory.

The following figure illustrates the shared user directory environment on a smaller scale:



Use the procedures outlined in this guide to upgrade this environment.

Chapter 2: Upgrading from r6.x

This section contains the following topics:

Supported Upgrade Paths

An upgrade consists of deploying r12.0 SP2 components to an existing SiteMinder environment. Upgrading to r12.0 SP2 can be accomplished in two ways:

- Completing a migration.
- Configuring a parallel r12.0 SP2 environment beside an existing environment. Both environments use one or more key stores to maintain single sign-on.

If you are upgrading from r6.x, both upgrade paths are supported.

More information:

Migration (see page 13)
Parallel Upgrade (see page 14)

Migration Considerations

If you are migrating from r6.x, consider the following before beginning the migration.

Policy Server Option Pack Support

Policy Server Option Pack (PSOP) features are part of the core Policy Server functionality. Consider the following if you are migrating an r6.x environment that uses PSOP features:

- The PSOP no longer requires a separate upgrade.
- The Policy Server installer backs ups the PSOP configuration files and uninstalls the PSOP during the Policy Server upgrade.
- The Policy Server installer installs the latest version of the PSOP during the Policy Server upgrade.

Note: For more information about migrating an r6.x environment that uses PSOP features, see How to Migrate from r6.x.

Manage Policy Server Option Pack Features

Two graphical user interfaces (GUIs) are available to manage specific SiteMinder policy objects. Consider the following:

- **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 those 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.

  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.

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 upgrade, the FSS Administrative UI must be registered with the Policy Server before it can be used. Registering the FSS Administrative UI is completed through the Administrative UI. Therefore, you are required to install and configure the Administrative UI before registering the FSS Administrative UI.

Note: For more information about installing and configuring each of these user interfaces during a migration, see How to Migrate from r6.x.

SiteMinder Key Database Password in r12.0 SP2

The SiteMinder key database (smkeydatabase) password, which is used to encrypt the key and certificate data stored in the database, is encrypted using FIPS-compliant algorithms. FIPS is a US government computer security standard used to accredit cryptographic modules that meet the Advanced Encryption Standard (AES). Consider the following as you plan your migration:

- An r12.0 SP2 Policy Server can only communicate with an r12.0 SP2 key database. A key database does not operate in compatibility mode.
- You can upgrade a key database by changing the password during the Policy Server upgrade. Changing the password re-encrypts the database password and existing encrypted data using FIPS-compliant algorithms.
- You can create an r12.0 SP2 key database during the Policy Server upgrade and migrate your existing key and certificate data into the new instance.

This guide details the steps for upgrading a key database. If you want to create an r12.0 SP2 key database and migrate existing key and certificate data into the new instance, do the following:

1. Export the key and certificate data using the smkeytool utility.

   Note: For more information about using the smkeytool utility, see the *Federation Security Services Guide*.

2. Create the r12.0 SP2 key database during the Policy Server upgrade.

   Note: You can use the Policy Server Configuration Wizard to create a key database. For more information about using the Policy Server Configuration Wizard, see the *Policy Server Installation Guide*.

3. Import the key and certificate data using the smkeytool utility.

AM Key Store Data in r12.0 SP2

If you are migrating a Federation Security Services environment from r6.0, r6.0 SP1, r6.0 SP2, r6.0 SP3, or r6.0 SP4, a PKI infrastructure change requires you to migrate AM key store (AM.keystore) data.

The migration requires you to migrate the data in the AM.keystore that resides on the Web Agent at the consuming authority to an r12.0 SP2 SiteMinder key database (smkeydatabase) at the consuming authority.

Note: For more information about the changes to the PKI infrastructure, see the *Federation Security Services Guide*. For more information about when to migrate AM.keystore data to an r12.0 SP2 SiteMinder key database, see How to Migrate from r6.x.

Crystal Reports in 12.x

The r12.0 SP2 Policy Server installer no longer includes the reports files (.rpt) that are compatible with Crystal Reports 9.0. SiteMinder reports are now integrated with the r12.0 SP2 Administrative UI. A separate installer is available to install the Report Server. The Report Server is required to schedule and view reports, including the reports available to you in r6.x.

Consider the following:

- You can continue to use the report files with a Crystal Reports server to schedule and view reports during the migration. An r12.0 SP2 Policy Server can communicate with an r6.x audit logs database.
- The Policy Server upgrade removes the r6.x reports data source. Create a backup of the r6.x reports data source.
- The last step in the migration is to install the Administrative UI and discontinue use of the r6.x Policy Server User Interface. Once you have completed the migration, you cannot access the report files. Additionally, you cannot access reports that were created using the reports files from the r6.x Policy Server User Interface. If you require access to these reports, we recommend backing them up before discontinuing use of the r6.x Policy Server User Interface.
- You can schedule and view reports that were available to you in r6.x using the r12.0 SP2 Administrative UI.

Note: For more information about installing the Report Server, see the Policy Server Installation Guide. For more information about scheduling and viewing reports, see the *Policy Server Administration Guide*.

Administrator Authentication

If you are using SiteMinder to protect an external administrator user store, consider the following:

- During the Policy Server upgrade, the Policy Server User Interface is upgraded to the FSS Administrative UI. You can continue to use SiteMinder to protect the FSS Administrative UI. The existing external connection remains valid for the FSS Administrative UI.
- By default, the Administrative UI uses the policy store as its source of administrator identities. This default configuration lets you manage the environment immediately after installing the Administrative UI. However, existing r6.x administrators stored in an external user are not available to the Administrative UI. Configure an external administrator store connection from the Administrative UI to make the r6.x administrators available.

  Note: Using SiteMinder to protect the Administrative UI is not supported. The Administrative UI login screen only prompts for a user name and password. For more information about configuring an external administrator store connection, see the *Policy Server Configuration Guide*.

Single Sign–on

You can maintain single sign–on during the migration to r12.0 SP2. Consider the following:

- An r12.0 SP2 Policy Server can communicate with an r6.x policy store and an r6.x key store.
- An r12.0 SP2 Policy Server can communicate with an r6.x session store.

Avoid Policy Store Corruption

To avoid possible policy store corruption, be sure that the server that is hosting policy store is configured to store objects in UTF-8 form.

Note: For more information about configuring your server to store objects in UTF-8 form, see your vendor–specific documentation.

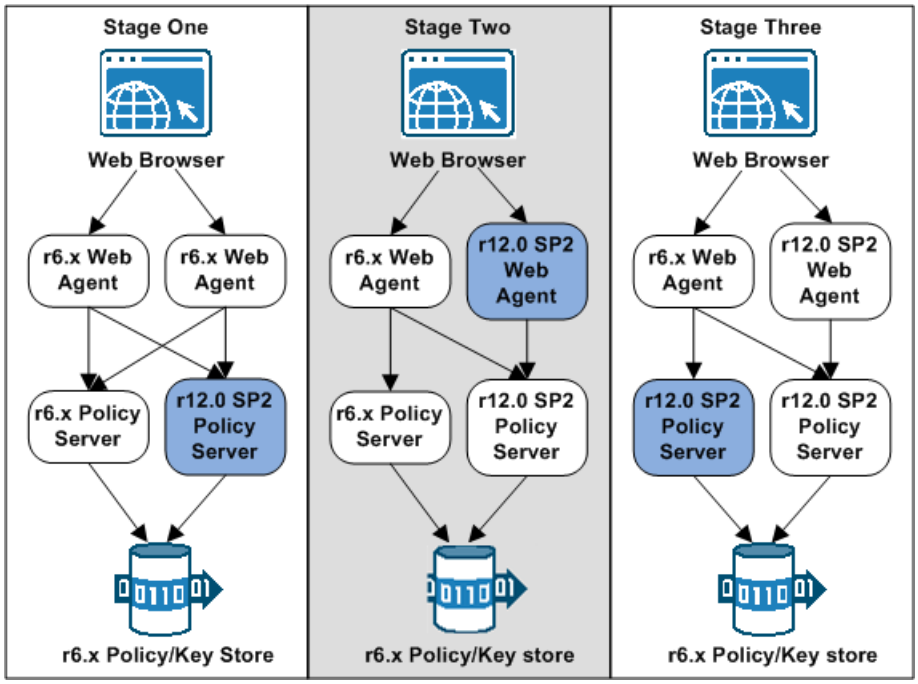
How the r6.x Migration Works

To upgrade a SiteMinder deployment with multiple Policy Servers and Web Agents, remove one of the Policy Servers and Web Agents from the SiteMinder environment. While these components are being upgraded, the remaining Policy Servers and Web Agents continue to protect your resources. Continue removing and upgrading SiteMinder components until all components are upgraded or operating in mixed-mode compatibility.

The following figures illustrate a simple r6.x environment and detail:

- The order in which existing components are upgraded
- The order in which new components are installed

  Note: Each figure depicts a single policy/key store. Your environment can use separate policy and key stores.

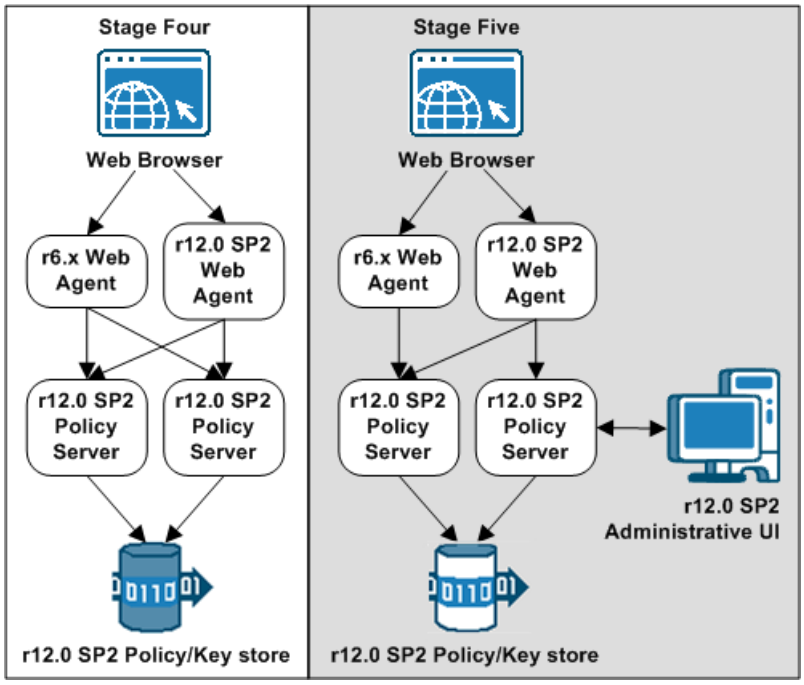


1. In stage one, an r6.x Policy Server is upgraded to r12.0 SP2. The r12.0 SP2 Policy Server operates in compatibility mode. Consider the following:
   - The r6.x Web Agents continue to communicate with the r12.0 SP2 Policy Server.
   - The r12.0 SP2 Policy Server continues to communicate with the r6.x policy and key store.
   - The r6.x Policy Server continues to communicate with the 6.x policy and key store. You can continue to use the r6.x Policy Server User Interface to administer the r6.x policy store through the r6.x Policy Server.

Important! The Policy Server installer replaces the r6.x Policy Server User Interface with the FSS Administrative UI during the upgrade. The r12.0 SP2 Policy Server continues to provide access control and generates log files that contain auditing information. However, you cannot administer the r6.x policy store through r12.0 SP2 Policy Server until the Administrative UI is installed.

2. In stage two, an r6.x Web Agent is upgraded to r12.0 SP2. Consider the following:
   - The r6.x Web Agent continues to communicate with the r6.x and the r12.0 SP2 Policy Servers.
   - The r12.0 SP2 Web Agent only communicates with the r12.0 SP2 Policy Server.
3. In stage three, the remaining Policy Server is upgraded to r12.0 SP2. The r12.0 SP2 Policy Servers operate in compatibility mode with the r6.x policy and key store.

   Important! Although the Policy Servers continue to protect resources and you have access to the Policy Server Management Console, you cannot administer the Policy Servers. The Policy Server installer replaced the Policy Server User Interface with the FSS Administrative UI during the upgrade. You cannot record policy information in the policy store until you have installed the r12.0 SP2 Administrative UI. Account for this time as you plan your migration.



4. In stage four, the r6.x policy and key store is upgraded to r12.0 SP2.

5. In stage five, the Administrative UI is installed and registered with a Policy Server. Consider the following:
   - You can install the Administrative UI before upgrading the policy store. However, you cannot register the Administrative UI until the policy store is upgraded. Installing the Administrative UI before the policy store upgrade minimizes the amount of time the Administrative UI is unavailable to the policy store.
   - An r6.x Web Agent is illustrated as an example of mixed-mode compatibility.
6. (Optional) The final steps, which are not illustrated, include the following:
   - Register each FSS Administrative UI with the respective Policy Server. The FSS Administrative UI is registered using the Administrative UI.
   - Install and register a Report Server.

     Note: For more information about registering a FSS Administrative UI and installing the Report Server, see the *Policy Server Installation Guide*.

How to Migrate from r6.x

Complete the follow procedures to complete a migration from r6.x to r12.0 SP2:

1. Review the sections in Before You Upgrade the Policy Server.
2. Upgrade an r6.x Policy Server to r12.0 SP2.

   Note: Consider the following:
   - The Policy Server installer replaces the r6.x Policy Server User Interface with the FSS Administrative UI during the upgrade. The r12.0 SP2 Policy Server continues to provide access control and generates log files that contain auditing information. However, you cannot administer the r6.x policy store through an r12.0 SP2 Policy Server until the Administrative UI is installed.
   - An r12.0 SP2 Policy Server can only communicate with an r12.0 SP2 key database. If you are upgrading a Federation Security Services environment, do one of the following:
     - Upgrade the existing SiteMinder key database to r12.0 SP2.
     - Migrate the existing keys and certificates to an r12.0 SP2 SiteMinder key database.

     The Policy Server installer lets you upgrade a key database to r12.0 SP2 or create an r12.0 SP2 key database during the Policy Server upgrade.
3. Review After You Upgrade the Policy Server.

4. (Optional) Migrate AM key store (AM.keystore) data into the r12.0 SP2 SiteMinder key database.

   Note: This step is only required if you are upgrading an r6.0, r6.0 SP1, r6.0 SP2, r6.0 SP3, and r6.0 SP4 Federation Security Services environment.

5. Upgrade an r6.x Web Agent to r12.0 SP2.

6. Upgrade the remaining r6.x Policy Servers and r6.x Web Agents to r12.0 SP2, respectively.

   Important! Although the Policy Servers continue to protect resources and you have access to the Policy Server Management Console, you cannot administer the Policy Servers. The Policy Server installer replaced the Policy Server User Interface with the FSS Administrative UI during the upgrade. You cannot record policy information in the policy store until you have installed the r12.0 SP2 Administrative UI. Account for this time as you plan your migration.

   Note: If you are upgrading an r6.0, r6.0 SP1, r6.0 SP2, r6.0 SP3, or r6.0 SP4 Federation Security Services environment, migrate AM.keystore data into the r12.0 SP2 SiteMinder key database.

7. Upgrade the r6.x policy and key stores to r12.0 SP2

   Note: The existing r6.x policy store schema has not changed. The r12.0 SP2 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.0 SP2.

8. Install the r12.0 SP2 Administrative UI.

9. (Optional) Register each FSS Administrative UI with its respective Policy Server.

10. (Optional) Install a Report Server.

    Note: For more information about registering a FSS Administrative UI and installing the Report Server, see the *Policy Server Installation Guide*.

Upgrade an r6.x Policy Server

The following sections detail how to upgrade an r6.x Policy Server on Windows and UNIX.

Before You Upgrade

Consider the following before you upgrade a Policy Server:

- You upgrade 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*.

- If a 5.1 Sun ONE directory server and a Policy Server are installed on the same Windows 2003 system, upgrade the LDAP SDK to 5.0.8 dated July 17, 2002 or later. Failing to upgrade the LDAP SDK results in Policy Server instability.

  Note: Upgrade the LDAP SDK, regardless of the use of the Sun ONE directory server.

- Remove the Policy Server being upgraded from your environment. Removing the Policy Server prevents Web Agents from contacting the Policy Server during the upgrade.

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

- (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 Policy Server installation executable.

- (UNIX) If you execute the Policy Server installer across different subnets, it can crash. Run the installer directly on the Policy Server host system.

- Install the documentation. The SiteMinder documentation is not installed with the Policy Server. We recommend that you install the documentation before you upgrade the Policy Server.

More information:

Locate the Installation Media (see page 136)
SiteMinder Documentation (see page 9)

Windows

To upgrade the Policy Server

1. Exit all applications that are running.
2. Double–click *installation_media*.

   installation_media

   Specifies the Policy Server installation executable.

   The Policy Server 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*.
3. Considering the following when running the installer:
   - The installer prompts you to select SiteMinder components. When selecting components:
     - Reconfigure components that had been previously configured for the environment. Be sure to select the respective components.
     - If you are upgrading a Federation Security Services environment or plan on using the SiteMinder Information Card Authentication Scheme, select the Create SM Key Database/Change SM Key Database Password check box.
     - If you are not configuring a new policy store, clear the Policy Store check box. You do not have to reconfigure existing policy store settings. An upgraded Policy Server retains the policy store settings. You manually upgrade an existing policy store.
   - If you selected the Create SM Key Database/Change SM Key Database Password check box:
     - Create an r12.0 SP2 key database if you are migrating your existing key database data into this repository.
     - Change the password if you intend on upgrading an existing key database. Changing the password re–encrypts the database password and existing encrypted data using FIPS–compliant algorithms.
   - If you cut and paste path information into the wizard, enter a character to enable the Next button.

4. Review the installation settings and click Install.

   The Policy Server is upgraded. The selected components are configured for use with the Policy Server.

   Note: The FSS Administrative UI was installed during the Policy Server upgrade. The FSS Administrative UI is for managing Federation Security Services. Register the FSS Administrative UI with the Policy Sever after upgrading the policy store and installing the Administrative UI. For more information about registering the FSS Administrative UI, see the *Policy Server Installation Guide*.

If you experience problems during the upgrade, you can locate the Policy Server installation log file in *siteminder_home*\siteminder\install_config_info.

siteminder_home

Specifies the Policy Server installation path.

UNIX GUI

To upgrade the Policy Server

1. Exit all applications that are running.
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 navigate to the installation executable.
4. Enter the following command:

   ./installation_media gui

   installation_media

   Specifies the Policy Server installation executable.

   The Policy Server 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. Considering the following when running the installer:
   - The installer prompts you to select SiteMinder components. When selecting components:
     - Reconfigure components that had been previously configured for the environment. Be sure to select the respective components.
     - If you are upgrading a Federation Security Services environment or plan on using the SiteMinder Information Card Authentication Scheme, select the Create SM Key Database/Change SM Key Database Password check box.
     - If you are not configuring a new policy store, clear the Policy Store check box. You do not have to reconfigure existing policy store settings. An upgraded Policy Server retains the policy store settings. You manually upgrade an existing policy store.
   - If you selected the Create SM Key Database/Change SM Key Database Password check box:
     - Create an r12.0 SP2 key database if you are migrating your existing key database data into this repository.
     - Change the password if you are upgrading an existing key database. Changing the password re–encrypts the database password and existing encrypted data using FIPS–compliant algorithms.
   - If you cut and paste path information into the wizard, enter a character to enable the Next button.
6. Review the installation settings and click Install.

   The Policy Server is upgraded. The selected components are configured for use with the Policy Server.

   Note: The upgrade can take several minutes.
7. Click Done and reboot the system.

   Note: The FSS Administrative UI was installed during the Policy Server upgrade. The FSS Administrative UI is for managing Federation Security Services. Register the FSS Administrative UI with the Policy Sever after upgrading the policy store and installing the Administrative UI. For more information about registering the FSS Administrative UI, see the *Policy Server Installation Guide*.

If you experience problems during the upgrade, you can locate the Policy Server installation log file in *siteminder_home*/siteminder/install_config_info.

siteminder_home

Specifies the Policy Server installation path.

UNIX Console

To upgrade the Policy Server

1. Exit all applications that are running.
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 navigate to the installation executable.
4. Enter the following command:

   ./installation_media -i console

   installation_media

   Specifies the Policy Server installation executable.

   The Policy Server 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. Considering the following when running the installer:
   - The installer prompts you to select SiteMinder components. Each component is prefixed with a number. Type numbers separated with a comma (,) to select one or more components. Enter only a comma to select none of the features. When selecting components:
     - Reconfigure components that had been previously configured for the environment. Be sure to select the respective components.
     - If you are upgrading a Federation Security Services environment or plan on using the SiteMinder Information Card Authentication Scheme, select Create SM Key Database/Change SM Key Database Password.
     - Only select Policy Store if you are configuring a new policy store. You do not have to reconfigure existing policy store settings. An upgraded Policy Server retains the policy store settings. You manually upgrade an existing policy store.

- If you selected Create SM Key Database/Change SM Key Database Password:
  - Create an r12.0 SP2 key database if you are migrating your existing key database data into this repository.
  - Change the password if you are upgrading an existing key database. Changing the password re–encrypts the database password and existing encrypted data using FIPS–compliant algorithms.

6. Review the installation settings and press Enter.

   The Policy Server is upgraded. The selected components are configured for use with the Policy Server.

   Note: The upgrade can take several minutes.

7. Press Enter and reboot the system.

   Note: The FSS Administrative UI was installed during the Policy Server upgrade. The FSS Administrative UI is for managing Federation Security Services. Register the FSS Administrative UI with the Policy Sever after upgrading the policy store and installing the Administrative UI. For more information about registering the FSS Administrative UI, see the *Policy Server Installation Guide*.

If you experience problems during the upgrade, you can locate the Policy Server installation log file in *siteminder_home*/siteminder/install_config_info.

siteminder_home

Specifies the Policy Server installation path.

After You Upgrade the Policy Server

If your Policy Server audit log is configured to include administrator changes to policy store objects, consider the following:

- You receive a message instructing you to disable this type of administrator auditing when you open the Policy Server Management Console for the first–time.
- You receive this message because there have been changes to how this type of administrator event is included in the Policy Server audit log. You use the XPSConfig utility, not the Policy Server Management Console, to include this type of administrator event in the audit log. By default, the XPSConfig utility enables the logging of Administrator changes to policy store objects.

You continue to receive the message until you change the Administrator Changes to Policy Store Objects setting, which is located on the Logs tab, to Log No Events. The setting appears disabled after you change it, but administrator changes to policy store objects continue to be logged.

If you want to exclude this type of Administrator event from the Policy Server audit log, disable it using the XPSConfig utility.

Note: For more information about using the XPSConfig utility, see the *Policy Server Administration Guide*.

Migrate AM Key Store Data into a SiteMinder Key Database

If you are upgrading a Federation Security Services environment from r6.0, r6.0 SP1, r6.0 SP2, r6.0 SP3, or r6.0 SP4, a PKI infrastructure change requires that data currently stored in the AM key store (AM.keystore) must be migrated to an r12.0 SP2 SiteMinder key database (smkeydatabase).

You migrate the AM.keystore data to a SiteMinder key database using the migratekeystore utility.

Note: For more information about using the migratekeystore utility, see the *Federated Security Services Guide*.

Upgrade an r6.x Web Agent

Upgrading Web Agents is the second step in the migration process.

SiteMinder r6.x Web Agents can communicate with an r12.0 SP2 Policy Server. Therefore, you upgrade a Policy Server to r12.0 SP2 before upgrading a Web Agent to r12.0 SP2.

Before You Upgrade r6.x Web Agents

Before you upgrade Web Agents:

- (UNIX) Be sure that you upgrade the Web Agent with the same account that was used to install it. If you use a different account, the upgrade can fail.
- Back up the Web Agent Option Pack (WAOP) configuration files and uninstall the WAOP.

  Note: For more information about uninstalling the WAOP, see the *Web Agent Option Pack Guide*.
- Be sure that the Policy Server is configured.
- Identify the required administrator and Policy Server object names.
- Identify the Web Agent requirements.

Ensure the Policy Server is Configured

Before you upgrade the Web Agent:

- Be sure that the Policy Server can connect to the Web Agent host system.
- Be sure that the Policy Server is running before registering trusted hosts. You start the Policy Server on the Status tab of the Policy Server Management Console.

Identify the Required Administrator and Policy Server Object Names

Before upgrading the Web Agent, you need the following information from the Policy Server administrator.

- Name of the SiteMinder Administrator allowed to register hosts.
- Name of the Host Configuration Object.
- Name of the Agent Configuration Object.

Identify the Web Agent Requirements

For more information about patches and other Web Agent requirements, see the *Web Agent Installation Guide*.

Upgrade an r6.x Web Agent

Use the r12.0 SP2 Web Agent installer to upgrade an r6.x Web Agent on Windows or UNIX.

Note: Agents that require option pack functionality must be upgraded to r12.0 SP2 before installing the r12.0 SP2 Web Agent Option Pack. For more information about upgrading a Web Agent, see the *Web Agent Installation Guide*. For more information about installing the r12.0 SP2 Web Agent Option Pack, see the *Web Agent Option Pack Guide*.

Upgrade an r6.x Policy Store

Upgrading the policy and key store is the third step in the migration process. The following sections detail how to upgrade an r6.x policy and key store to r12.0 SP2.

Options for Upgrading a Policy Store

Two paths exist for upgrading an r6.x policy store to r12.0 SP2. You can:

- Upgrade the existing policy and key store to r12.0 SP2.
- Create anr12.0 SP2 policy and key store and import the existing policy and key store data into the new instance.

This guide details the steps for upgrading an existing policy and key store.

If you want to create an r12.0 SP2 policy and key store:

1. Export the policy and key store data using the correct version of smobjexport.

   Note: For more information about the r6.x version of smobjimport, see the *Policy Server Installation Guide* for r6.x.

2. Create an r12.0 SP2 policy and key store.

   Note: For more information about creating an r12.0 SP2 policy and key store, see the *Policy Server Installation Guide*.

3. Import the policy and key store data into the r12.0 SP2 policy and key store using the r12.0 SP2 version of smobjimport.

   Note: For more information about the r12.0 SP2 version of smobjimport, see the *Policy Server Administration Guide*.

How to Upgrade an r6.x Policy Store

A new policy store is not required for an upgrade to r12.0 SP2. You can upgrade an existing policy store to r12.0 SP2.

Complete the following procedures to upgrade a policy store:

1. Extend the policy store schema.

   Note: The existing r6.x policy store schema has not changed. The r12.0 SP2 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.0 SP2.

2. Import the base policy store objects.

   Note: If you are upgrading a Federation Security Services environment, there is no change to the Policy Server Option Pack (PSOP) schema. If your policy store already contains the default objects in the ampolicy.smdif file, you do not have to re-import the file.

3. Import the policy store data Definitions.

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*.

Extend the Active Directory Policy Store Schema

You extend the policy store schema to store objects introduced by r12.0 SP2. The existing r6.x policy store schema has not changed.

To extend the Active Directory policy store schema

1. Navigate to *policy_server_home*\xps\db and open the ActiveDirectory.ldif file.

   policy_server_home

   Specifies the Policy Server installation path.

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

   Example: dc=domain,dc=com

3. Navigate to *policy_server_home*/bin from a command window.

4. Run the following command:

   smldapsetup ldmod -fpolicy_server_home/xps/db/ActiveDirectory.ldif

   The policy store schema is extended to store objects introduced by r12.0 SP2.

Extend the ADAM Policy Store Schema

You extend the policy store schema to store objects introduced by r12.0 SP2. The existing r6.x policy store schema has not changed.

To extend the ADAM policy store schema

1. Navigate to *policy_server_home*/xps/db and open the ADAM.ldif file.

   policy_server_home

   Specifies the Policy Server installation path.

2. Replace each instance of {guid} with the actual value of guid in braces, and save the file.

   Example: {CF151EA3-53A0-44A4-B4AC-DA0EBB1FF200}

3. Navigate to *policy_server_home*/bin from a command window.

4. Run the following command:

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

   The policy store schema is extended for objects required by r12.0 SP2.

Extend the CA Directory Policy Store Schema

You extend the policy store schema to store objects introduced by r12.0 SP2. The existing r6.x policy store schema has not changed.

To extend the CA Directory policy store schema

1. Copy the following file into the CA Directory DXHOME\config\schema directory:

   etrust.dxc

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

   policy_server_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 *policy_server_home*\eTrust.

   policy_server_home

   Specifies the Policy Server installation path.

3. Open the SiteMinder schema file (.dxg), and add the following lines to the bottom of the file:

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

4. Edit the DXI file for the DSA by adding the following lines to the bottom of the file:

   ```
   # 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;
   ```

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

5. Open the default DXC file (default.dxc) for the DSA and locate the following:

```
# size limits
set max-users = 255;
set credits = 5;
set max-local-ops = 100;
set max-dsp-ops = 100;
set max-op-size = 200;
set multi-write-queue = 20000;
```

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

6. Edit the settings to match the following and save the DXC file:

```
# 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;
```

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

7. 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 policy store DSA.

The policy store schema is extended to store objects introduced by r12.0 SP2.

Extend the Sun Java System Directory Server Policy Store Schema

You extend the policy store schema to store objects introduced by r12.0 SP2. The existing r6.x policy store schema has not changed.

To extend the Sun Java System Directory Server policy store schema

1. Navigate to *policy_server_home*/bin with a command window.

policy_server_home

Specifies the Policy Server installation path.

2. Run the following command:

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

The policy store schema is extended to store objects introduced by r12.0 SP2.

Extend the MS SQL Server Policy Store Schema

You extend the policy store schema to store objects introduced by r12.0 SP2. The existing r6.x policy store schema has not changed.

To extend the Microsoft SQL Server policy store schema

1. Log into SQL Server as the user who administers the Policy Server database information.
2. Start the Query Analyzer.
3. Select the policy store database instance from the database list.
4. Open SQLServer.sql in a text editor and copy the contents of the entire file.

   Note: The SQLServer.sql file is in *policy_server_home*\xps\db.

   policy_server_home

   Specifies the Policy Server installation path.
5. Paste the schema from SQLServer.sql into the query and execute the query.

   The policy store schema is extended to store objects introduced by r12.0 SP2.

Extend the Oracle Policy Store Schema

You extend the policy store schema to store objects introduced by r12.0 SP2. The existing r6.x policy store schema has not changed.

To extend the Oracle policy store 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 the 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 r12.0 SP2 script into the 6.x database instance:

   $NETE_PS_ROOT/xps/db/Oracle.sql

   Note: If you are using sqlplus, run the schema using an @ sign.

   Sqlplus example: <@NETE_PS_ROOT>/xps/db/Oracle.sql

   Non-sqlplus example: <$NETE_PS_ROOT>/xps/db/Oracle.sql

   The policy store schema is extended to store objects introduced by r12.0 SP2.

Import the Base Policy Store Objects

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

To import the base policy store objects

1. Run the following command:

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

   -policy_server_home

   Specifies the Policy Server installation path.

   upgrade_smdif_file_name

   Specifies the name of the import file:

   - **r6.0 to r12.0 SP2:** sm_upgrade_60_to_R12sp2.smdif
   - **r6.0 SP1 to r12.0 SP2:** sm_upgrade_60sp1_to_R12sp2.smdif
   - **r6.0 SP2 to r12.0 SP2:** sm_upgrade_60sp2_to_R12sp2.smdif
   - **r6.0 SP3 to r12.0 SP2:** sm_upgrade_60sp3_to_R12sp2.smdif
   - **r6.0 SP4 to r12.0 SP2:** sm_upgrade_60sp4_to_R12sp2.smdif
   - **r6.0 SP5 to r12.0 SP2:** sm_upgrade_60sp5_to_R12sp2.smdif

   -d*siteminder_super_user_name*

   Specifies the name of the SiteMinder administrator account.

   -w*siteminder_super_user_password*

   Specifies the password for the SiteMinder administrator account.

   -v

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

   Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.0 SP2.

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

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

UNIX example: smobjimport

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

The base policy store objects are imported.

2. Run the following command:

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

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

-policy_server_home

Specifies the path and name of the import file.

-dsiteminder_super_user_name

Specifies the name of the SiteMinder administrator account.

-wsiteminder_super_user_password

Specifies the password for the SiteMinder administrator account.

-f

Overrides duplicate objects.

-v

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

Default value: stdout

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

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

You can now import the policy store data definitions.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Install the Administrative User Interface

Unlike previous versions of SiteMinder, the Policy Server User Interface is not installed with the Policy Server. Rather, you are required to install the r12.0 SP2 Administrative UI separately.

Note: More information on installing the Administrative UI exists in the *Policy Server Installation Guide*.

Register 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.

You register the FSS Administrative UI with the Policy Server to ensure that the communication between both components is FIPS-encrypted (AES encryption).

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.

If you 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.

Note: More information on registering the FSS Administrative UI exists in the *Policy Server Installation Guide*.

Upgrade an r6.x Session Server

The r12.0 SP2 session server schema has not changed from r6.0 SP5. If you have an r6.0 SP5 session server, you do not have to upgrade the schema.

Note: For more information about importing the session store schema, see the *Policy Server Installation Guide*.

To upgrade the Session Server import one of the following .sql schema scripts into the existing session store database. The following scripts are located in *policy_server_home*\db\SQL:

- sm_mssql_ss_upgrade_60_to_R12sp2.sql

  Upgrades a SQL Server session store and adds a new Expiry Data table to the session store.

- sm_oracle_ss_upgrade_60_to_R12sp2.sql

  Upgrades an Oracle session store and adds a new Expiry Data table to the session store.

policy_server_home

Specifies the Policy Server installation path.

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*.

Upgrade an r6.x Audit Log Database

Using the iRecorder for SiteMinder, Security Command Center (SCC) can read security-related logging data from a SiteMinder SQL Server or Oracle logs database.

Note: For more information about the iRecorder for SiteMinder, see the *eTrust Audit iRecorder Reference Guide*. For more information about importing the audit log schema, see the *Policy Server Installation Guide*.

The integration requires that you upgrade the schema for the audit log database by importing the sm_mssql_logs_eaudit_upgrade.sql script or sm_oracle_logs_eaudit_upgrade.sql script, which are located in *policy_server_home*\db\SQL. Import this script only if you are integrating SiteMinder with SCC.

policy_server_home

Specifies the Policy Server installation path.

Note: The SiteMinder/SCC integration does not work with DB2 logging databases.

To upgrade the audit log database, import one of the following schema scripts into an existing SiteMinder audit log database:

sm_mssql_logs_eaudit_upgrade.sql

Upgrades a SQL Server audit log database from r6.x to r12.0 SP2.

sm_oracle_logs_eaudit_upgrade.sql

Upgrades an Oracle audit log database from r6.x to r12.0 SP2.

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*.

How a Parallel Upgrade Works

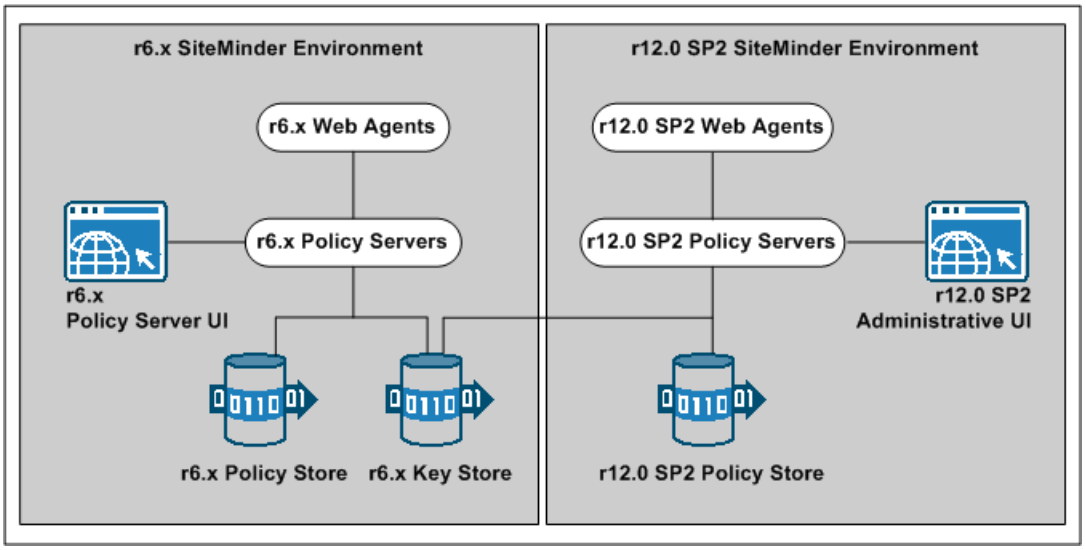
You do not have to migrate an existing r6.x environment to r12.0 SP2. Rather, you can configure a parallel r12.0 SP2 environment beside an existing deployment.

The following figure illustrates a simple parallel upgrade and details:

- An r6.x environment that continues to protect existing resources.
- An r6.x Policy Server User Interface that is used to manage SiteMinder objects in the r6.x policy store.
- An r12.0 SP2 environment that protects new resources.

- An r12.0 SP2 Administrative UI that is used to manage SiteMinder objects in the r12.0 SP2 policy store.
- A common r6.x key store. The common key store enables single sign-on between both environments.

  Note: Although not illustrated, you can enable single sign–on between both environments using multiple key stores.



How to Configure a Parallel Environment

Complete the follow procedures to configure a parallel environment:

1. Review the parallel environment key management options to determine how to implement single sign–on.
2. Create the r12.0 SP2 environment.
3. Do one of the following:
   - Be sure that both environments meet the common key store single sign–on requirements.
   - Be sure that both environments meet the multiple key store single sign–on requirements.
4. (Optional) Migrate the r6.x policy store data.
5. Review the user directory single sign–on requirements.

Parallel Environment Key Management Options

Managing SiteMinder keys to maintain single sign–on between the existing environment and r12.0 SP2 environment is critical to a successful parallel upgrade. Two SiteMinder key management options are available. The option you deploy depends on how you implement one or more key stores across both environments. The options include:

- Multiple policy stores with a common key store
- Multiple policy stores with separate key stores

Common Key Store Deployment

All Policy Servers can use a single key store for key rollover. The following figure illustrates:

- r6.x Policy Servers connecting to an r6.x policy store.
- r12.0 SP2 Policy Servers connecting to an r12.0 SP2 policy store.
- A common r6.x key store maintaining key data for all Policy Servers. The common key store lets Agents associated with all Policy Server share keys. Sharing the keys enables single sign–on between both environments.

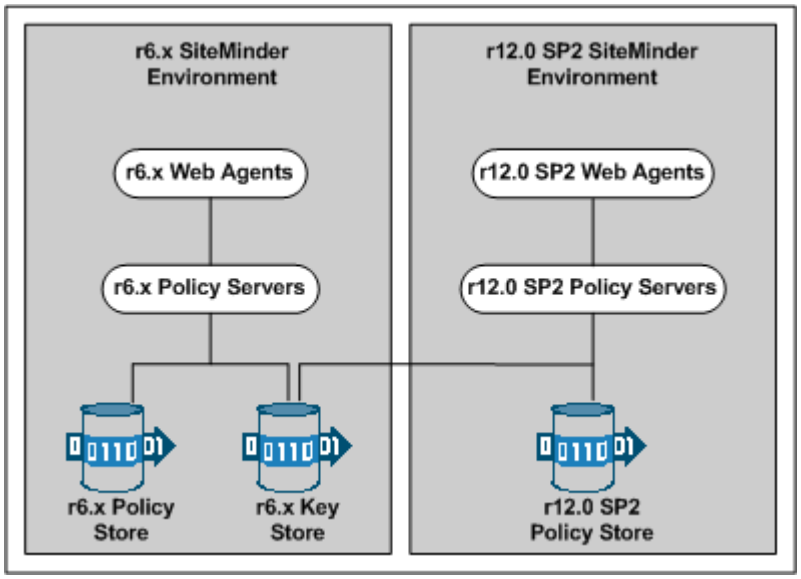
  Important! The r6.x key store must be configured separately from the r6.x policy store.

- All Policy Servers connecting to a common key store to retrieve new keys.

  Important! The r12.0 SP2 Policy Servers must be configured with the r6.x key store. r6.x Policy Servers cannot communicate with an r12.0 SP2 key store.

- All Web Agents polling their respective Policy Server to retrieve new keys.

Note: Although not illustrated, policy store and key store data can be replicated for failover. The database or directory server type determines how you replicate data. For more information about key management in a master/slave environment, see the *Policy Server Administration Guide*. For more information about replicating data, see your vendor–specific documentation.



Multiple Key Store Deployment

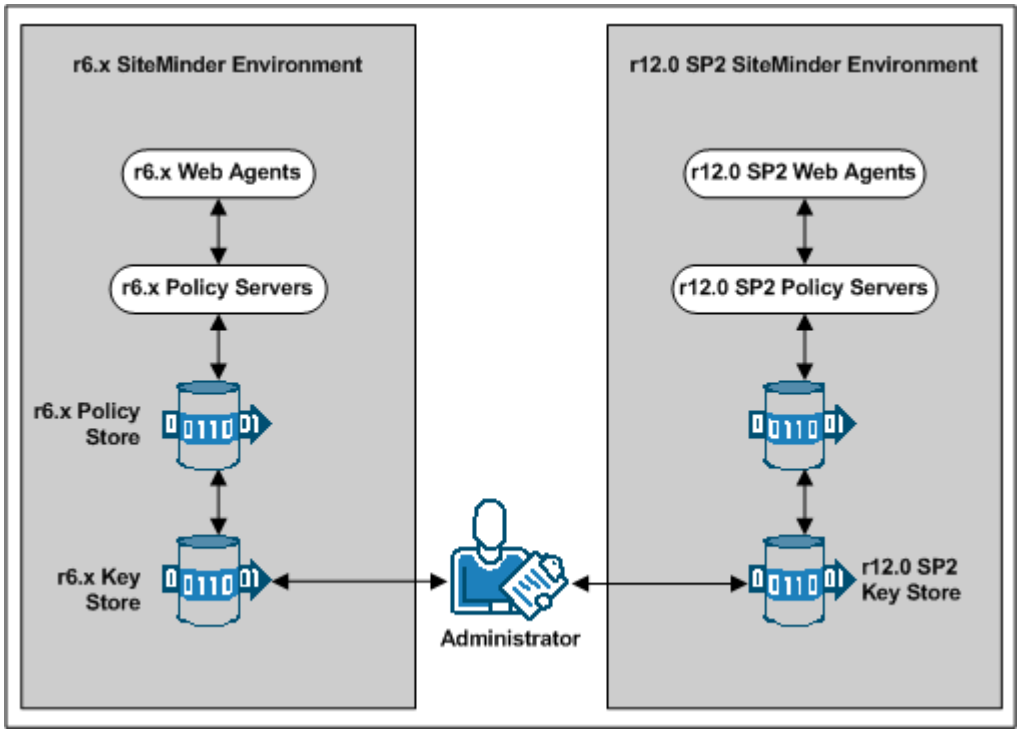
Existing r6.x Policy Servers can use an r6.x key store for key rollover, while r12.0 SP2 Policy Servers can use an r12.0 SP2 key store for key rollover. The following figure illustrates:

- r6.x Policy Servers connecting to an r6.x policy store.
- r12.0 SP2 Policy Servers connecting to an r12.0 SP2 policy store.
- r6.x Policy Servers connecting to an r6.x key store to retrieve new keys.
- r12.0 SP2 Policy Servers connecting to an r12.0 SP2 key store to retrieve new keys.
- A SiteMinder administrator using the Administrative UI to configure static Agent and Session keys for each key store.

  Important! If all key stores do not use the same Agent and Session keys, single sign–on fails.

- r6.x Web Agents polling their respective r6.x Policy Servers to retrieve new keys.
- r12.0 SP2 Web Agents polling their respective r12.0 SP2 Policy Servers to retrieve new keys.

Note: Although not illustrated, policy store and key store data can be replicated for failover. The database or directory server type determines how you replicate data. For more information about key management in a master/slave environment, see the *Policy Server Administration Guide*. For more information about replicating data, see your vendor–specific documentation.



Create the r12.0 SP2 Environment

You can configure an r12.0 SP2 environment independently of the existing environment. Install and configure the r12.0 SP2 components in the following order:

1. One or more Policy Servers.

   Important! If you are maintaining single sign–on with a common key store, all Policy Servers must use the same encryption key. If you do not know the value of the encryption key, you can reset the r6.x value in the policy store. Use the new value when installing r12.0 SP2 Policy Servers.

   Note: For more information about resetting the policy store encryption key, see the *Policy Server Administration Guide*.

2. A policy store.
3. An Administrative UI.
4. One or more Web Agents.
5. A Report Server

Note: For more information about installing a Policy Server, a policy store, an Administrative UI, and a Report Server, see the *Policy Server Installation Guide*. For more information about installing Web Agents, see the *Web Agent Installation Guide*.

Common Key Store Single Sign–on Requirements

If you are deploying a common key store, do the following or single sign–on fails:

- Be sure that the r6.x policy and key store are configured separately.

  Note: For more information about configuring a key store, see the *Policy Server Administration Guide*.

- Leave the key store version at r6.x. r12.0 SP2 Policy Servers can communicate with an r6.x key store, but r6.x Policy Servers cannot communicate with an r12.0 SP2 key store.
- Configure all Policy Servers to use the common r6.x key store.
- Be sure that all Policy Servers use the same encryption key. If you do not know the value of the encryption key, you can reset the r6.x value in the policy store. Use the new value when installing an r12.0 SP2 Policy Server.

  Note: For more information about resetting the policy store encryption key, see the *Policy Server Administration Guide*.

- Nominate a single Policy Server to generate dynamic Agent keys. Disable Agent key generation for the remaining Policy Servers.

  Note: For more information about dynamically generating Agent keys, see the *Policy Server Administration Guide*.

Multiple Key Store Single Sign–on Requirements

If you are deploying multiple key stores, do the following or single sign–on fails:

- Disable dynamic Agent key generation for all Policy Servers.
- Be sure that a SiteMinder administrator has the necessary Policy Server User Interface and Administrative UI permissions to specify the same static Agent key and the same session ticket in the r6.x and r12.0 SP2 key store.

  Note: For more information about delegating administrator permissions, see the *Policy Server Configuration Guide*.
- **Important!** Be sure that the same static Agent key and the same session ticket are configured in the r6.x and r12.0 SP2 key stores.

  Note: For more information about configuring a static Agent key and session ticket, see the *Policy Server Administration Guide*.

Migrate the r6.x Policies

If you plan on using the r12.0 SP2 deployment to protect r6.x resources, we recommend migrating your policy store data to the r12.0 SP2 policy store.

Although not required, if you migrate the policy store data before you begin managing the r12.0 SP2 policy store, you can avoid the possibility of conflicts associated with duplicate objects.

To migrate policies

1. Do one of the following:
   - If you are using Enterprise Policy Management applications in the r6.x environment, use the r6.x version of the XPSExport utility to export the r6.x policy store data.
   - If you are not using Enterprise Policy Management applications in the r6.x environment, use the r6.x version of the smobjimport utility to export the r6.x policy store data.

   Note: For more information about the r6.x version of the smobjimport utility, see the r6.x *Policy Server Installation Guide*. For more information about the r6.x version of the XPSExport utility, see the *Policy Server Administration Guide*.

2. Do one of the following:

   - If you are using Enterprise Policy Management applications in the r6.x environment, use the r12.0 SP2 version of the XPSImport utility to import the policy data into the r12.0 SP2 policy store.
   - If you are not using Enterprise Policy Management applications in the r6.x environment, use the r12.0 SP2 version of the smobjimport utility to import the policy data into the r12.0 SP2 policy store.

   Note: For more information about the r12.0 SP2 version of the smobjimport and XPSImport utilities, see the *Policy Server Administration Guide*.

User Directory Single Sign–on Requirements

Be sure that the SiteMinder user directory objects you create in both environments have the same names. If you use different names to point r6.x and r12.0 SP2 Policy Servers to the same user stores, single sign–on fails.

Chapter 3: Upgrading from r12.x

This section contains the following topics:

Supported Upgrade Paths

An upgrade consists of deploying r12.0 SP2 components to an existing SiteMinder environment. Upgrading to r12.0 SP2 can be accomplished in two ways:

- Completing a migration.
- Configuring a parallel r12.0 SP2 environment beside an existing environment. Both environments use one or more key stores to maintain single sign-on.

If you are upgrading from r12.0, the parallel upgrade is the only supported upgrade path. If you are upgrading from r12.0 SP1, both upgrade paths are supported.

More information:

Migration (see page 13)
Parallel Upgrade (see page 14)

Migration Considerations

If you are migrating from r12.0 SP1, consider the following before beginning the migration.

Policy Server Option Pack Support

Beginning with r12.0 SP1, features associated with the Policy Server Option Pack (PSOP) are considered core Policy Server functionality. If you are migrating an r12.0 SP1 environment that uses PSOP features, consider the following:

- The PSOP no longer requires a separate upgrade. The PSOP is upgraded during the Policy Server upgrade.
- r12.x Agents that require option pack functionality must be upgraded to r12.0 SP2 before installing the r12.0 SP2 Web Agent Option Pack (WAOP).

Note: For more information about upgrading Web Agents, see the *Web Agent Installation Guide*. For more information about installing the WAOP, see the *Web Agent Option Pack Guide*.

Manage Policy Server Option Pack Features

Two graphical user interfaces (GUIs) are available to manage specific SiteMinder policy objects. Consider the following:

- **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 those 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.

  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.

Federation Security Services Components

If you are migrating an r12.0 SP1 environment and plan on using Federation Security Services, consider the following:

- A SiteMinder key database (smkeydatabase) is a required component. You can create a key database during the Policy Server upgrade. You can also use the Policy Server Configuration Wizard to create a key database after you upgrade the Policy Server.

  Note: For more information about the role a key database plays in a federated environment, see the *Federation Security Services Guide*.

- A registered FSS Administrative UI is a required component. Although part of your core r12.0 SP1 environment, the FSS Administrative UI must be registered with a Policy Server before it can be used. If you intended on managing SiteMinder Federation Security Services, register the FSS Administrative UI after upgrading the policy store and the Administrative UI.

- Additional SiteMinder components are required to deploy a federated environment.

  Note: For more information about the required Federation Security Services components, see the *Federation Security Services Guide*.

Administrative UI Upgrade Options

This release introduces a simplified Administrative UI installation that includes an embedded object store and an embedded SiteMinder Administrative UI service (JBoss). If you are migrating to r12.0 SP2, two options exist for upgrading the Administrative UI:

- You can upgrade the r12.0 SP1 Administrative UI to r12.0 SP2. If you upgrade the Administrative UI, you can continue to use:
  - The existing external object store.
  - The existing external administrator user store.
  - The existing Policy Server connections.
  - The existing URL to access the Administrative UI.

  Note: For more information about upgrading an Administrative UI, see How to Migrate from r12.0 SP1.

- You can uninstall the r12.0 SP1 Administrative UI and use the stand–alone installation option to install an r12.0 SP2 Administrative UI. If you install an r12.0 SP2 Administrative UI, you use:
  - The embedded object store, instead of the external object store. The r12.0 SP2 Administrative UI does not require an external object store.
  - The embedded application server, instead of the existing application server infrastructure.
  - The Administrative Authentication wizard to configure a connection to the existing external administrator user store.
  - The new URL to access the Administrative UI. The r12.0 SP2 URL is //*host*:*port*/iam/siteminder/adminui.

  Note: For more information about uninstalling an r12.0 SP1 Administrative UI, see the r12.0 SP1 version of the *Policy Server Installation Guide*. For more information about installing the Administrative UI, see the *Policy Server Installation Guide*. For more information about configuring a connection to an external administrator user store, see the *Policy Server Configuration Guide*.

Single Sign–on

You can maintain single sign–on during the migration to r12.0 SP2. Consider the following:

- An r12.0 SP2 Policy Server can communicate with an r12.0 SP1 policy store and an r12.0 SP1 key store.
- An r12.0 SP2 Policy Server can communicate with an r12.0 SP1 session store.

Avoid Policy Store Corruption

To avoid possible policy store corruption, be sure that the server that is hosting policy store is configured to store objects in UTF-8 form.

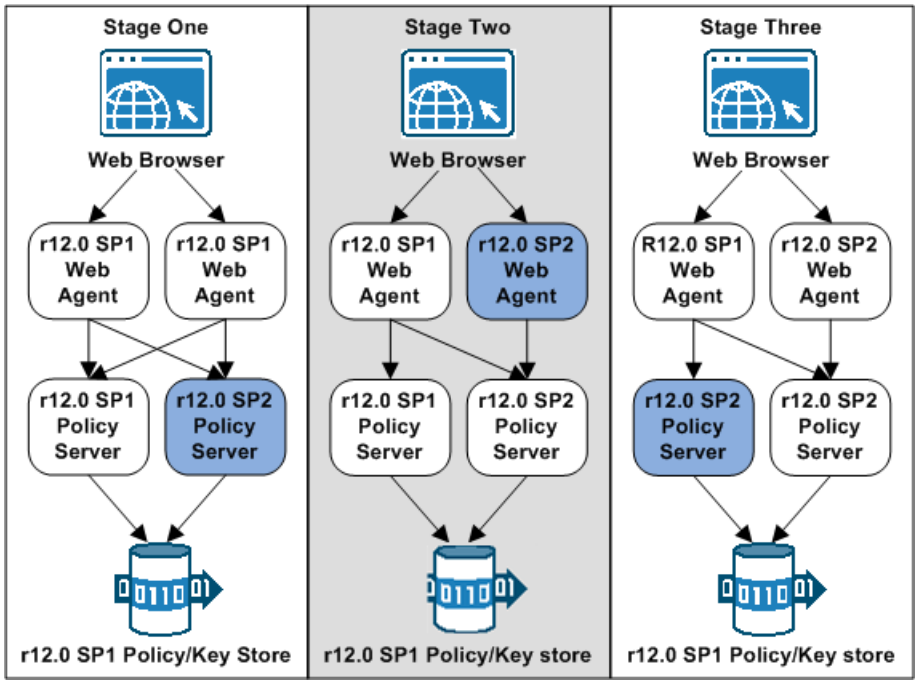
Note: For more information about configuring your server to store objects in UTF-8 form, see your vendor–specific documentation.

How the r12.0 SP1 Migration Works

To migrate a SiteMinder deployment with multiple Policy Servers and Web Agents, remove one of the Policy Servers and Web Agents from the SiteMinder environment. While these components are being upgraded, the remaining Policy Servers and Web Agents continue to protect your resources. Continue removing and upgrading SiteMinder components until all components are upgraded or operating in mixed–mode compatibility.

The following figures illustrate a simple r12.0 SP1 environment and detail the order in which existing components are upgraded.

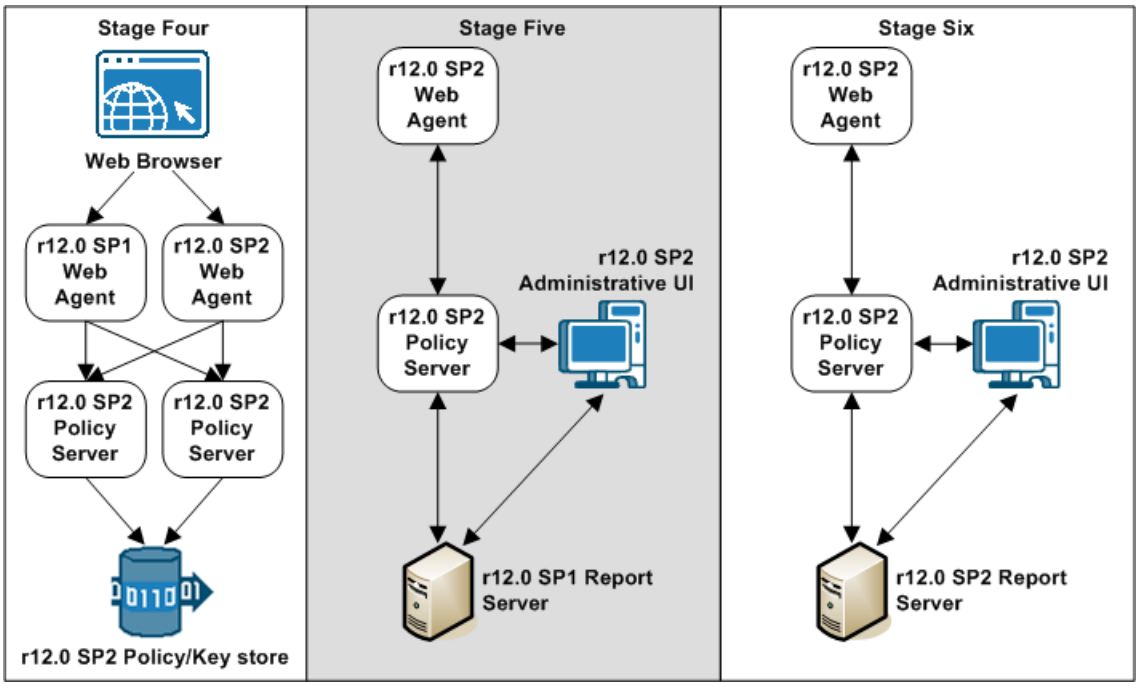
Note: Each figure depicts a single policy/key store. Your environment can use separate policy and key stores.



1. In stage one, an r12.0 SP1 Policy Server is upgraded. The r12.0 SP2 Policy Server operates in compatibility mode. Consider the following:
   - The r12.0 SP1 Web Agents continue to communicate with the r12.0 SP2 Policy Server.
   - The r12.0 SP2 Policy Server continues to communicate with the r12.0 SP1 policy and key store.
   - The r12.0 SP1 Policy Server continues to communicate with the r12.0 SP1 policy and key store.

- If an r12.0 SP1 Administrative UI is configured with the r12.0 SP2 Policy Server, the Administrative UI continues to communicate with the Policy Server to manage objects in the r12.0 SP1 policy store.
- If an r12.0 SP1 Report Server is configured with the r12.0 SP2 Policy Server, the Report Server continues to create reports.

2. In stage two, an r12.0 SP1 Web Agent is upgraded to r12.0 SP2.
   - The r12.0 SP1 Web Agent continues to communicate with the r12.0 SP1 and the r12.0 SP2 Policy Server.
   - The r12.0 SP2 Web Agent only communicates with the r12.0 SP2 Policy Server.
3. In stage three, the remaining Policy Server is upgraded to r12.0 SP2. The r12.0 SP2 Policy Servers operate in compatibility mode with the r12.0 SP1 policy and key store.



4. In stage four, the r12.0 SP1 policy and key store is upgraded to r12.0 SP2.
5. In stage five, the Administrative UI is upgraded.
6. In stage six, the Report Server is upgraded and re–registered with an r12.0 SP2 Policy Server.

How to Migrate from r12.0 SP1

Complete the following procedures to migrate from r12.0 SP1 to r12.0 SP2:

1. Review the sections in Before You Upgrade the Policy Server.
2. Upgrade an r12.0 SP1 Policy Server to r12.0 SP2.
3. Upgrade an r12.0 SP1 Web Agent to r12.0 SP2.
4. Upgrade the remaining r12.0 SP1 Policy Servers and Web Agents to r12.0 SP2, respectively.
5. Upgrade the r12.0 SP1 policy and key stores to r12.0 SP2.
6. Upgrade the r12.0 SP1 Administrative UI.
7. Upgrade the r12.0 SP1 Report Server.

Important! Migrating from r12.0 is not a supported upgrade path. If you are upgrading from r12.0, configure a parallel environment.

Upgrade an r12.0 SP1 Policy Server

The following sections detail how to upgrade an r12.0 SP1 Policy Server on Windows and UNIX.

Before You Upgrade

Before you upgrade a Policy Server, consider the following:

- You upgrade 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*.

- If a 5.1 Sun ONE directory server and a Policy Server are installed on the same Windows 2003 system, upgrade the LDAP SDK to 5.0.8 dated July 17, 2002 or later. Failing to upgrade the LDAP SDK results in Policy Server instability.

  Note: Upgrade the LDAP SDK, regardless of the use of the Sun ONE directory server.

- Remove the Policy Server from the environment. Removing the Policy Server prevents Web Agents from contacting the Policy Server during the upgrade.
- Shut down all instances of the Policy Server Management Console.

- (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 Policy Server installation executable.

- (UNIX) If you execute the Policy Server across different subnets, it can crash. Run the Policy Server installer directly on the host system.
- (UNIX) Upgrade the Policy Server using an account with at least the same permissions as the user who installed the Policy Server. For example, if a root user installed the Policy Server, upgrade the Policy Sever using a root user.
- Install the documentation. The SiteMinder documentation is not installed with the Policy Server. We recommend that you install the documentation before you upgrade the Policy Server.

More information:

Locate the Installation Media (see page 136)
SiteMinder Documentation (see page 9)

Windows

To upgrade the Policy Server

1. Exit all applications that are running.
2. Navigate to the installation media.
3. Double–click *installation_media*.

   installation_media

   Specifies the name of the Policy Server installation executable.

   The Policy Server 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. Considering the following when running the installer:
   - The installer prompts you to select the components. When selecting components:
     - Reconfigure components that had been previously configured for the environment. Be sure to select the respective components.
     - If you do not intend on configuring a new policy store, clear the Policy Store check box. You do not have to reconfigure existing policy store settings. The Policy Server retains the policy store settings after the upgrade. You manually upgrade an existing policy store.
   - Select the Create SM Key Database/Change SM Key Database Password check box if:
     - You plan on using features related to Federation Security Services.
     - You plan on using the SiteMinder Information Card Authentication Scheme. For example, you can use the SiteMinder Information Card Authentication Scheme for the support of Microsoft CardSpace.

   Note: If you create a SiteMinder key database, the installer prompts you 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 the upgrade.
5. Review the installation settings and click Install.

   The Policy Server is upgraded. The selected components are configured for use with the Policy Server.

If you experience problems during the upgrade, you can locate the Policy Server installation log file at *siteminder_home*\siteminder\install_config_info.

siteminder_home

Specifies the Policy Server installation path.

UNIX GUI

To upgrade the Policy Server

1. Exit all applications that are running.
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 navigate to the installation executable.
4. Enter the following command:

   ./installation_media gui

   installation_media

   Specifies the name of the Policy Server installer executable.

   The Policy Server 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. Considering the following when running the installer:
   - The installer prompts you to select the components. When selecting components:
     - Reconfigure components that had been previously configured for the environment. Be sure to select the respective components.
     - If you are not configuring a new policy store, clear the Policy Store check box. You do not have to reconfigure existing policy store settings. The upgraded Policy Server retains the policy store settings. You manually upgrade an existing policy store.
   - Select the Create SM Key Database/Change SM Key Database Password check box if:
     - You plan on using features related to Federation Security Services.
     - You plan on using the SiteMinder Information Card Authentication Scheme. For example, you can use the SiteMinder Information Card Authentication Scheme for the support of Microsoft CardSpace.

   Note: If you create a key database, the installer prompts you 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 the upgrade.

6. Review the installation settings and click Install.

   The Policy Server is upgraded. The selected components are configured for use with the Policy Server.

If you experience problems during the upgrade, you can locate the Policy Server installation log file at *siteminder_home*\siteminder\install_config_info.

siteminder_home

Specifies the Policy Server installation path.

UNIX Console

To upgrade the Policy Server

1. Exit all applications that are running.
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 navigate to the installation executable.
4. Enter the following command:

   ./installation_media -i console

   installation_media

   Specifies the name of the Policy Server installer executable.

   The Policy Server 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. Considering the following when running the installer:
   - The installer prompts you to select SiteMinder components. Each component is prefixed with a number. Type numbers separated with a comma (,) to select one or more components. Enter only a comma to select none of the features. When selecting components:
   - Reconfigure components that had been previously configured for the environment. Be sure to select the respective components.
   - Only select Policy Store if you are configuring a new policy store. You do not have to reconfigure existing policy store settings. The upgraded Policy Server retains the policy store settings. You manually upgrade an existing policy store.
   - Select Create SM Key Database/Change SM Key Database Password if:
     - You plan on using features related to Federation Security Services.
     - You plan on using the SiteMinder Information Card Authentication Scheme. For example, you can use the SiteMinder Information Card Authentication Scheme for the support of Microsoft CardSpace.

   Note: If you create a key database, the installer prompts you to install the default CA certificates. Leave Import default CA certificates selected and install these certificates. You can add additional certificates and private keys to a key database after the upgrade.

6. Review the installation settings and press Enter.

   The Policy Server is upgraded. The selected components are configured for use with the Policy Server.

If you experience problems during the upgrade, you can locate the Policy Server installation log file at *siteminder_home*\siteminder\install_config_info.

siteminder_home

Specifies the Policy Server installation path.

Before You Upgrade an r12.0 SP1 Web Agent

Before you upgrade Web Agents:

- (UNIX) Be sure that you upgrade the Web Agent with the same account that was used to install it. If you use a different account, the upgrade can fail.
- Be sure that the Policy Server is configured.
- Identify the required administrator and Policy Server object names.
- Identify the Web Agent requirements.

Ensure the Policy Server is Configured

Before you upgrade the Web Agent:

- Be sure that the Policy Server can connect to the Web Agent host system.
- Be sure that the Policy Server is running before registering trusted hosts. You start the Policy Server on the Status tab of the Policy Server Management Console.

Identify the Required Administrator and Policy Server Object Names

Before upgrading the Web Agent, you need the following information from the Policy Server administrator.

- Name of the SiteMinder Administrator allowed to register hosts.
- Name of the Host Configuration Object.
- Name of the Agent Configuration Object.

Identify the Web Agent Requirements

For more information about patches and other Web Agent requirements, see the *Web Agent Installation Guide*.

Upgrade an r12.0 SP1 Web Agent

Use the r12.0 SP2 Web Agent installer to upgrade an r12.0 SP1 Web Agent on Windows or UNIX.

Note: Agents that require option pack functionality must be upgraded to r12.0 SP2 before installing the r12.0 SP2 Web Agent Option Pack. For more information about upgrading a Web Agent, see the *Web Agent Installation Guide*. For more information about installing the Web Agent Option Pack, see the *Web Agent Option Pack Guide*.

How to Upgrade an r12.0 SP1 Policy Store

Complete the following procedures to upgrade an r12.0 SP1 policy store to r12.0 SP2:

1. Import the base policy store objects.
2. Import the policy store data definitions.

   Note: There are no upgrade files associated with policy store data definitions. You re–import each file to upgrade the data definitions.

Import the Base Policy Store Objects

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

To import the base policy store objects, run the following command:

smobjimport -i*policy_server_home*\db\smdif\sm_upgrade_R12sp1_to_R12sp2.smdif
-d*siteminder_super_user_name* -w*siteminder_super_user_password*
-v -f

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder administrator account.

-v

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

Default output: stdout

-f

Overwrites duplicate policy store objects with those from r12.0 SP2.

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

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

UNIX example: smobjimport

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

The base policy store objects are imported.

Import the Policy Store Data Definitions

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

To import the base policy store objects

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

   policy_server_home

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

Upgrade an r12.0 SP1 Administrative UI

The following sections detail how to upgrade the Administrative UI on Windows and UNIX.

Before You Upgrade

Consider the following before you upgrade the Administrative UI:

- You upgrade 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
- **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. Run the Administrative UI installer directly on the host system.

More information:

Locate the Installation Media (see page 136)

Windows

To upgrade the Administrative UI

1. Exit all applications that are running.
2. Stop the application server that is hosting the Administrative UI.

   Note: For more information about stopping the application server, see the r12.0 SP1 *Policy Server Installation Guide*.

3. Navigate to Administrative UI installation executable.

   Important! The installation zip also contains a layout.properties file and a Framework folder at the same level as the Administrative UI executable. If you moved the Administrative UI executable after extracting the installation zip, move the following to the same location as the Administrative UI executable or the upgrade will fail:

   - layout.properties file
   - Framework folder

4. Double–click *installation_media*.

   installation_media

   Specifies the Administrative UI 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*.

   The Administrative UI installer starts.

5. Follow the prompts and confirm that the installer can upgrade the Administrative UI.

6. Review the installation settings and click Install.

   The installer confirms that the Administrative UI is installed.

7. Start the application server that is hosting the Administrative UI.

   Note: For more information about starting the application server, see the r12.0 SP1 *Policy Server Installation Guide*.

   The Administrative UI is upgraded.

UNIX GUI

To upgrade the Administrative UI

1. Exit all applications that are running.
2. Stop the application server that is hosting the Administrative UI.

   Note: For more information about stopping the application server, see the r12.0 SP1 *Policy Server Installation Guide*.

3. Open a shell and navigate to the installation executable.

   Important! The installation zip contains a layout.properties file and a Framework folder at the same level as the Administrative UI executable. If you moved the Administrative UI executable after extracting the installation zip, move the following to the same location as the Administrative UI executable or the upgrade will fail:

   - layout.properties file
   - Framework folder

4. 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*.

5. Follow the prompts and confirm that the installer can upgrade the Administrative UI.

6. Review the installation settings and click Install.

   The installer confirms that the Administrative UI is installed.

7. Start the application server that is hosting the Administrative UI.

   Note: For more information about starting the application server, see the r12.0 SP1 *Policy Server Installation Guide*.

   The Administrative UI is upgraded.

UNIX Console

To upgrade the Administrative UI

1. Exit all applications that are running.
2. Stop the application server that is hosting the Administrative UI.

   Note: For more information about stopping the application server, see the r12.0 SP1 *Policy Server Installation Guide*.

3. Open a shell and navigate to the installation executable.

   Important! The installation zip contains a layout.properties file and a Framework folder at the same level as the Administrative UI executable. If you moved the Administrative UI executable after extracting the installation zip, move the following to the same location as the Administrative UI executable or the upgrade will fail:

   - layout.properties file
   - Framework folder

4. 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*.

5. Follow the prompts and confirm that the installer can upgrade the Administrative UI.

6. Review the installation settings and press Enter.

   The installer confirms that the Administrative UI is installed.

7. Start the application server that is hosting the Administrative UI.

   Note: For more information about starting the application server, see the r12.0 SP1 *Policy Server Installation Guide*.

   The Administrative UI is upgraded.

How to Upgrade a Report Server

Complete the following procedures to upgrade a Report Server to r12.0 SP2:

1. Upgrade the Report Server.
2. (r12.0) If you are upgrading the Report Server from r12.0:
   a. (Optional) Export existing reports.

      Important! Existing reports are deleted when you uninstall the report templates. If you require access to existing reports, use the Administrative UI to view the reports and export them to a temporary location. For more information about viewing reports, see the *Policy Server Administration Guide*.

   b. Uninstall the report templates.

3. Install the report templates.
4. Re–register the Report Server.

Upgrade the Report Server on Windows

The following sections detail how to upgrade the Report Server on Windows and UNIX.

Before You Upgrade

Consider the following before you upgrade the Report Server:

- You upgrade 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 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 Report Server installation media.

- (UNIX) If you execute the Report Server installer across different subnets, it can crash. Run the Report Server installer directly on the host system.

More information:

Locate the Installation Media (see page 136)

Windows

To upgrade the Report Server

1. Exit all applications that are running.
2. 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*.
3. Select English from the drop–down list and click Next.

   The installer introduction appears.
4. Click Next.

   The license agreement appears.
5. Accept the license agreement and click Next.

   The installer prompts you to select an installation type.
6. Click Update and click Next.

   The installer displays a patches summary.
7. Click Next.

   The installation summary appears.
8. Click Install.

   The installer upgrades the Report Server.

UNIX GUI

To upgrade the Report Server

1. Exit all applications that are running.
2. Open a Bourne shell and navigate to the CABI folder.

3. 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*.

4. Select English from the drop–down list and click Next.

   The installer introduction appears.

5. Click Next

   The license agreement appears.

6. Accept the license agreement and click Next.

   The installer prompts you to select an installation type.

7. Click Update and click Next.

   The installer displays a patches summary.

8. Click Next.

   The installation summary appears.

9. Click Install.

   The installer upgrades the Report Server.

UNIX Console

To upgrade the Report Server

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

   ./installation_media 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*.

4. Type the value for English and press Enter.

   The installer introduction appears.

5. Press Enter.

   The license agreement appears.

6. 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.

7. Type 2 to select Update and press Enter.

   The installer displays a patches summary.

8. Press Enter.

   The installation summary appears.

9. Press Enter.

   The installer upgrades the Report Server.

Uninstall the Report Templates

If you are upgrading the Report Server from r12.0, uninstall the existing report templates before installing the new report templates. If you are upgrading the Report Server from r12.0 SP1, this step is not required.

Important! Existing reports are deleted when you uninstall the report templates. If you require access to existing reports, use the Administrative UI to view the reports and export them to a temporary location. For more information about viewing reports, see the *Policy Server Administration Guide*.

To uninstall the report templates

1. Do one of the following:
   - (Windows) Click Start, Programs, BusinessObjects XI Release 2, BusinessObjects Enterprise, BusinessObjects Enterprise Java InfoView.
   - (UNIX) Open a web browser and enter the following:

     http://*host_name*:*port*/businessobjects/enterprise115/desktoplaunch/InfoView/logon/logon.do

     host_name

     Specifies the name of the Report Server host system.

     port

     Specifies the port on which Apache Tomcat is listening.

   The InfoView login screen appears.
2. Log into InfoView.

   Note: InfoView requires the administrator credentials supplied when installing the Report Server.

   The InfoView console appears.
3. Expand the Public folder and click the SiteMinder folder.

   A list of reports appears.
4. Click the delete icon under the Folders pane on the left side of the InfoView console.

   The report templates are deleted.
5. Restart the Report Server.

   Note: For more information about restarting the Report Server, see the *Policy Server Installation Guide*.

Install the Report Templates

The Report Server requires the report templates to create SiteMinder policy analysis and audit–based reports. Use the SiteMinder Report Server Configuration Wizard to install the report templates.

Note: For more information about installing the report templates, see the *Policy Server Installation Guide*.

Re–register a Report Server

A Report Server cannot generate reports until it is re–registered with an r12.0 SP2 Policy Server.

Considering the following when re–registering a Report Server:

- The Administrative UI can have a trusted relationship with one or more Policy Servers. However, each trusted relationship only allows one Report Server connection.
- You create a Report Server connection to re–register a Report Server. Before you create the connection, delete the existing Report Server connection.

Note: For more information about deleting a Report Server connection and registering a Report Server connection, see the *Policy Server Installation Guide*.

How a Parallel Upgrade Works

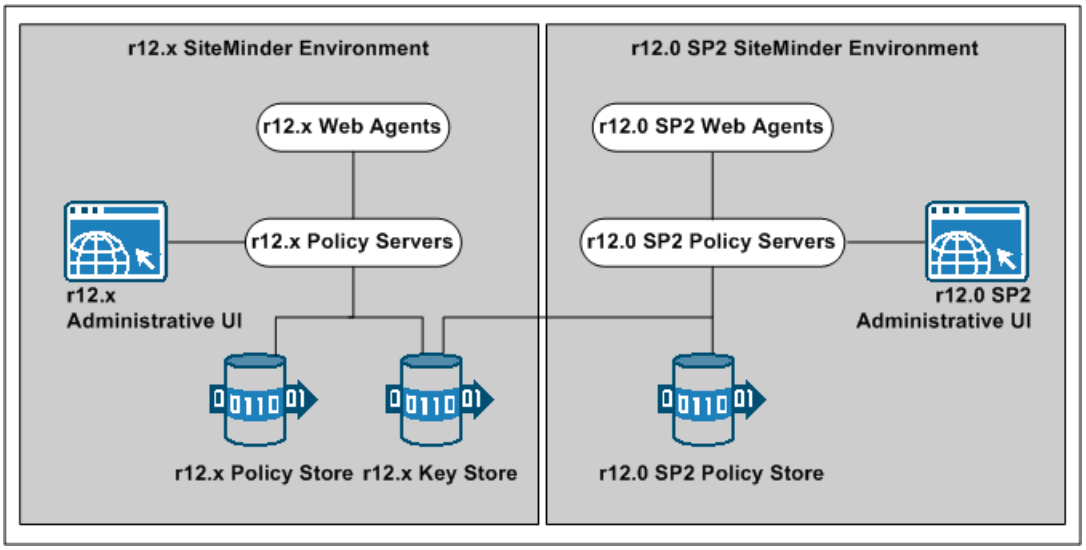
You do not have to migrate an existing r12.x environment to r12.0 SP2. Rather, you can configure a parallel r12.0 SP2 environment beside an existing deployment.

The following figure illustrates a simple parallel upgrade and details:

- An r12.x environment that continues to protect existing resources.
- An r12.x Administrative UI that is used to manage SiteMinder objects in the r12.x policy store.
- An r12.0 SP2 environment that protects new resources.

- An r12.0 SP2 Administrative UI that is used to manage SiteMinder objects in the r12.0 SP2 policy store.
- A common r12.x key store. The common key store enables single sign-on between both environments.

  Note: Although not illustrated, you can enable single sign–on between both environments using multiple key stores.



How to Configure a Parallel Environment

Complete the follow procedures to configure a parallel environment:

1. Review the parallel environment key management options to determine how to implement single sign–on.
2. Create the r12.0 SP2 environment.
3. Do one of the following:
   - Be sure that both environments meet the common key store single sign–on requirements.
   - Be sure that both environments meet the multiple key store single sign–on requirements.
4. (Optional) Migrate the r12.x policy store data.
5. Review the user directory single sign–on requirements.

Parallel Environment Key Management Options

Managing SiteMinder keys to maintain single sign–on between the existing environment and r12.0 SP2 environment is critical to a successful parallel upgrade. Two SiteMinder key management options are available. The option you deploy depends on how you implement one or more key stores across both environments. The options include:

- Multiple policy stores with a common key store
- Multiple policy stores with separate key stores

Common Key Store Deployment

All Policy Servers can use a single key store for key rollover. The following figure illustrates:

- r12.x Policy Servers connecting to an r12.x policy store.
- r12.0 SP2 Policy Servers connecting to an r12.0 SP2 policy store.
- A common r12.x key store maintaining key data for all Policy Servers. The common key store lets Agents associated with all Policy Server share keys. Sharing the keys enables single sign–on between both environments.

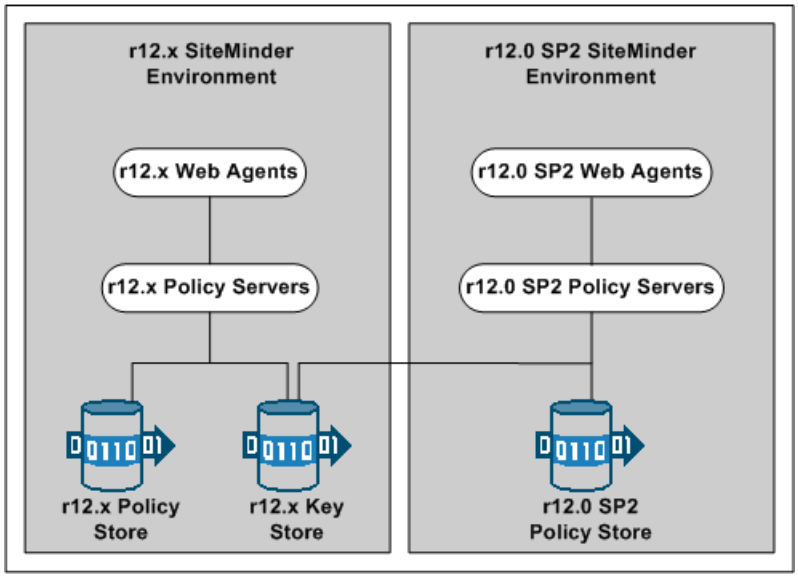
  Important! The r12.x key store must be configured separately from the r12.x policy store.

- All Policy Servers connecting to a common key store to retrieve new keys.

  Important! The r12.0 SP2 Policy Servers must be configured with the r12.x key store. r12.x Policy Servers cannot communicate with an r12.0 SP2 key store.

- All Web Agents polling their respective Policy Server to retrieve new keys.

Note: Although not illustrated, policy store and key store data can be replicated for failover. The database or directory server type determines how you replicate data. For more information about key management in a master/slave environment, see the *Policy Server Administration Guide*. For more information about replicating data, see your vendor–specific documentation.



Multiple Key Store Deployment

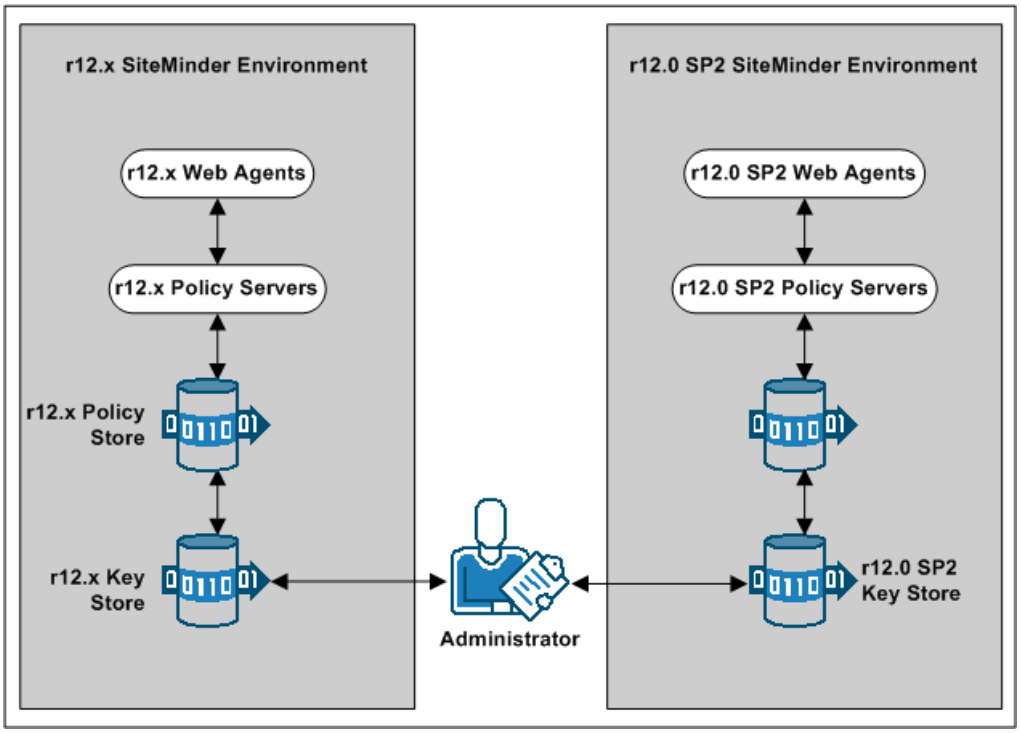
Existing r12.x Policy Servers can use an r12.x key store for key rollover, while r12.0 SP2 Policy Servers can use an r12.0 SP2 key store for key rollover. The following figure illustrates:

- r12.x Policy Servers connecting to an r12.x policy store.
- r12.0 SP2 Policy Servers connecting to an r12.0 SP2 policy store.
- r12.x Policy Servers connecting to an r12.x key store to retrieve new keys.
- r12.0 SP2 Policy Servers connecting to an r12.0 SP2 key store to retrieve new keys.
- A SiteMinder administrator using the Administrative UI to configure static Agent and Session keys for each key store.

  Important! If all key stores do not use the same Agent and Session keys, single sign–on fails.

- r12.x Web Agents polling their respective r12.x Policy Servers to retrieve new keys.
- r12.0 SP2 Web Agents polling their respective r12.0 SP2 Policy Servers to retrieve new keys.

Note: Although not illustrated, policy store and key store data can be replicated for failover. The database or directory server type determines how you replicate data. For more information about key management in a master/slave environment, see the *Policy Server Administration Guide*. For more information about replicating data, see your vendor–specific documentation.



Create the r12.0 SP2 Environment

You can configure an r12.0 SP2 environment independently of the existing environment. Install and configure the r12.0 SP2 components in the following order:

1. One or more Policy Servers.

   Important! If you are maintaining single sign–on with a common key store, all Policy Servers must use the same encryption key. If you do not know the value of the encryption key, you can reset the r12.x value in the policy store. Use the new value when installing r12.0 SP2 Policy Servers.

   Note: For more information about resetting the policy store encryption key, see the *Policy Server Administration Guide*.

2. A policy store.
3. An Administrative UI.
4. One or more Web Agents.
5. A Report Server

Note: For more information about installing a Policy Server, a policy store, an Administrative UI, and a Report Server, see the *Policy Server Installation Guide*. For more information about installing Web Agents, see the *Web Agent Installation Guide*.

Common Key Store Single Sign–on Requirements

If you are deploying a common key store, do the following or single sign–on fails:

- Be sure that the r12.x policy and key store are configured separately.

  Note: For more information about configuring a key store, see the *Policy Server Administration Guide*.

- Leave the key store version at r12.x. r12.0 SP2 Policy Servers can communicate with an r12.x key store, but r12.x Policy Servers cannot communicate with an r12.0 SP2 key store.
- Configure all Policy Servers to use the common r12.x key store.

- Be sure that all Policy Servers use the same encryption key. If you do not know the value of the encryption key, you can reset the r12.x value in the policy store. Use the new value when installing an r12.0 SP2 Policy Server.

  Note: For more information about resetting the policy store encryption key, see the *Policy Server Administration Guide*.

- Nominate a single Policy Server to generate dynamic Agent keys. Disable Agent key generation for the remaining Policy Servers.

  Note: For more information about dynamically generating Agent keys, see the *Policy Server Administration Guide*.

Multiple Key Store Single Sign–on Requirements

If you are deploying multiple key stores, do the following or single sign–on fails:

- Disable dynamic Agent key generation for all Policy Servers.
- Be sure that a SiteMinder administrator has the necessary Administrative UI permissions to specify the same static Agent key and the same session ticket in the r12.x and r12.0 SP2 key stores.

  Note: For more information about delegating administrator permissions, see the *Policy Server Configuration Guide*.

- Be sure that the same static Agent key and the same session ticket are configured in the r12.x and r12.0 SP2 key stores.

  Note: For more information about configuring a static Agent key and session ticket, see the *Policy Server Administration Guide*.

Migrate the r12.x Policies

If you plan on using the r12.0 SP2 deployment to protect r12.x resources, we recommend migrating your policy store data to the r12.0 SP2 policy store.

Although not required, if you migrate the policy store data before you begin managing the r12.0 SP2 policy store, you can avoid the possibility of conflicts associated with duplicate objects.

To migrate policies

1. Use the r12.x version of the XPSExport utility to export the r12.x policy store data.
2. Use the r12.0 SP2 version of the XPSImport utility to import the policy data into the r12.0 SP2 policy store.

Note: For more information about the r12.x version of XPSExport, see the r12.x *Policy Server Administration Guide*. For more information about the r12.0 SP2 version of XPSImport, see the *Policy Server Administration Guide*.

User Directory Single Sign on Requirements

Be sure that the SiteMinder user directory objects you create in both environments have the same names. If you use different names to point r12.x and r12.0 SP2 Policy Servers to the same user stores, single sign–on fails.

Chapter 4: Using FIPS-Compliant Algorithms

This section contains the following topics:

FIPS 140-2 Migration Overview

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). These libraries provide a FIPS mode of operation when a SiteMinder environment only uses FIPS–compliant algorithms to encrypt sensitive data. A SiteMinder environment can operate in one of the following FIPS modes of operation:

- FIPS–compatibility
- FIPS–migration
- FIPS–only

By default, a SiteMinder environment upgraded to r12.0 SP2 is operating in FIPS–compatibility mode. In FIPS–compatibility mode, the environment uses algorithms existing in previous versions of SiteMinder to encrypt sensitive data and is compatible with previous versions SiteMinder. If your organization does not require the use of FIPS–compliant algorithms, the Policy Server can operate in FIPS–compatibility mode without further configuration.

Migrating your environment to use only FIPS–compliant algorithms is comprised of two stages.

1. **Re–encrypt existing sensitive data**—In stage one, you configure the environment to operate in 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 environment continues to use existing SiteMinder encryption algorithms as you re–encrypt existing sensitive data using FIPS-compliant algorithms.

2. **Configure FIPS–only mode**—In stage two you configure your environment to operate in FIPS–only mode. In FIPS–only mode, the environment only uses FIPS–compliant algorithms to encrypt sensitive data.

   Important! An environment that is running in FIPS–only mode cannot interoperate with and is not 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 FIPS–only mode.

Note: More information on the FIPS Certified Module and the algorithms being used; the data that is being protected; and the SiteMinder Cryptographic Boundary exists in the *Policy Server Administration Guide*.

FIPS 140-2 Migration Requirements

Ensure that your environment meets the minimum requirements before migrating the environment to only use FIPS-compliant algorithms. You may want to print the following to use as a checklist:

- ☐ Ensure that your entire SiteMinder environment, including the SDK, is upgraded to r12.0 SP2.
- ☐ If the environment contains custom agents, ensure that they are re-linked to the respective SDK.

  Note: More information on re-linking custom agents exists in the *API Reference Guide for C* and the *API Reference Guide for Java*.
- ☐ Ensure that at least one Policy Server in the environment is configured to enable Agent key generation.

  Note: More information on enabling agent key generation exists in the *Policy Server Administration Guide*.
- ☐ If the environment uses X.509 Client Certificate authentication schemes, ensure that the user certificates are generated using only FIPS-compliant algorithms.
- ☐ If the Policy Servers are to connect to policy stores and/or user stores via SSL, ensure that the certificates used by the Policy Servers and the directory stores for the connection are FIPS-compliant.

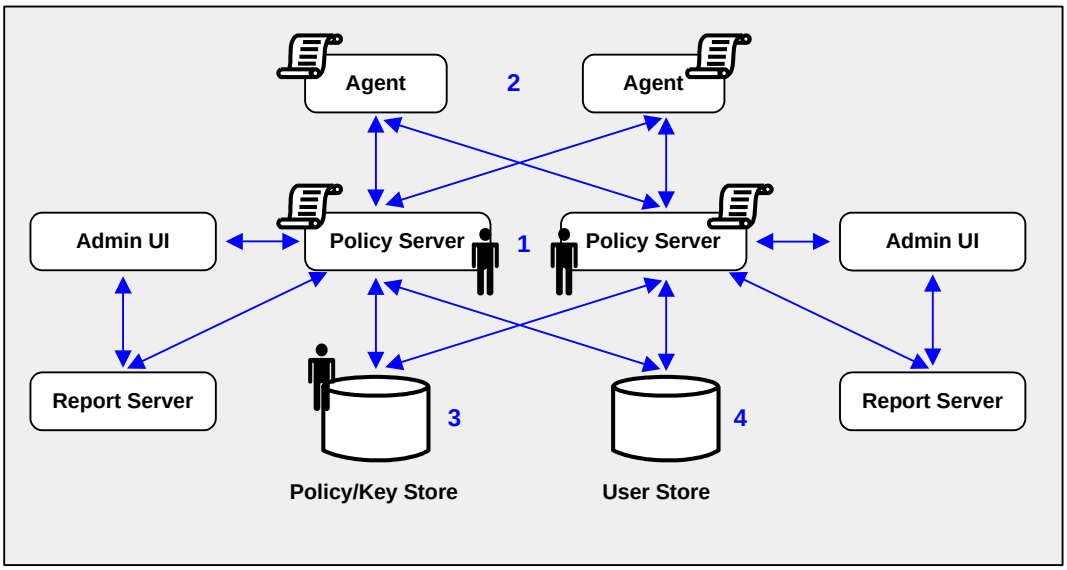
Migration Roadmap—Re-Encrypt Sensitive Data

Before your environment can operate in FIPS-only mode, you must:

- Set specific components to operate in FIPS-migration mode.
- Re-encrypt existing sensitive data using FIPS-compliant algorithms.

The following figure illustrates a sample r12.0 SP2 environment and details:

- The order in which you configure components to operate in FIPS-migration mode
- The existing sensitive data that you must re-encrypt



1. Each Policy Server in the environment is set to operate in FIPS-migration mode.
   - The policy store key, which is located in the EncryptionKey.txt file, is encrypted using algorithms that are not FIPS compliant. Re-encrypt this key for each Policy Server in the environment before configuring the environment for FIPS-only mode.
   - The policy store administrator password is encrypted using algorithms that are not FIPS compliant. Re-encrypt this password before configuring the environment for FIPS-only mode.

     Important! If you have configured a separate database for a key store, audit logs, token data, or a session server, these passwords are encrypted using algorithms that are not FIPS compliant. Re-encrypt these passwords before configuring the environment for FIPS-only mode.
   - The SiteMinder Super User password is encrypted using algorithms that are not FIPS compliant. Re-encrypt the password before configuring the environment for FIPS-only mode.

     Note: This is the password for the default SiteMinder administrator account. This account is used for all administrative tasks that do not require direct access to the Administrative UI. This is not the password for the Administrative UI administrator account with Super User privileges.

2. Each SiteMinder Web agent, including custom Agents, in the environment is set to operate in FIPS-migration mode.

   The shared secrets that the Policy Servers and Agents use to establish encrypted communication channels are encrypted using algorithms that are not FIPS compliant. Re-encrypt the shared secrets before configuring the environment for FIPS-only mode.

3. Keys and sensitive policy store data is re-encrypted.

   Note: The previous figure depicts a single database instance as a policy/key store. Your environment may use separate database instances for individual policy and key stores.

   Sensitive data stored in a policy store or policy and key stores is encrypted using algorithms that are not FIPS compliant. Re-encrypt the keys and sensitive policy store data before configuring the environment for FIPS-only mode.

4. (Optional) If your environment uses Basic Password Services, a Policy Server operating in FIPS-migration mode re-encrypts each Password Blob with FIPS compliant algorithms when the respective user is challenged for authentication. To prevent users from losing their password history and being locked out, identify the Password Blobs that the Policy Server did not re-encrypt and notify users that they must log in or change their password.

   Note: How the password policy is configured determines when the Policy Server re-encrypts the Password Blob:

   - If the password policy is configured to track successful and/or failed logins, the Policy Server re-encrypts the Password Blob when the user logs in.
   - If the password policy is not configured to track logins, the Policy Server re-encrypts the Password Blob when the user changes the password.

How to Re-Encrypt Existing Sensitive Data

Complete the following procedures to re-encrypt existing sensitive data using FIPS-compliant algorithms:

1. Gather environment information.
2. Set FIPS-migration mode for all Policy Servers.
3. Re-encrypt the policy store key.
4. Re-encrypt the policy store administrator password.
5. Re-encrypt the SiteMinder Super User password.
6. Set FIPS-migration mode for all Agents.

7. Re-encrypt policy and key store data.
8. (Optional) If your environment uses Basic Password Services, verify that Password Blobs are re-encrypted.

Gather Environment Information

Re-encrypting existing sensitive data while the Policy Server operates in FIPS-migration mode requires specific environment information.

Note: A FIPS information worksheet is provided to help you gather and record information prior to re-encrypting sensitive data. You may want to print this worksheet and use it to record required information.

- **Policy store key**—For each Policy Server in the environment, copy the policy store encryption key from the EncryptionKey.txt file and save them to a single location from which you can copy them. The EncryptionKey.txt file is located in *policy_server_home*\bin.

  policy server home

  Specifies the Policy Server installation path.

- **SiteMinder Super User account name and password**— Identify the SiteMinder Super User account name and password. SiteMinder tools you use to re-encrypt data require this information.

  Note: This is the account that is used for all administrative tasks that do not require direct access to the Administrative UI. These are not the credentials for the Administrative UI administrator account with Super User privileges.

- **Policy store administrator password**—Identify the policy store administrator password. This is the password that was supplied when the connection between the policy store and the Policy Server was configured.

More information:

FIPS Information Worksheet (see page 133)

Set a Policy Server to FIPS-Migration Mode

You set the Policy Servers to FIPS-migration mode so the environment can continue to use the existing SiteMinder encryption algorithms as you re-encrypt existing sensitive data using FIPS-compliant algorithms.

To set a Policy Server to FIPS-migration mode

1. Open a command prompt from the computer hosting the Policy Server and run the following command:

   setFIPSmigration

   MIGRATION appears in the command window.

2. Stop the Policy Server.

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

3. Do one of the following:

   a. If the Policy Server is installed on a Windows system, reboot the machine.

   b. If the Policy Server is installed on a UNIX system, log in as the user who is used to start the Policy Server.

4. Start the Policy Server.

5. Open the smps.log file and verify that the following line appears:

   Policy Server migrating from classic SiteMinder to FIPS-140 cryptographic algorithms.

6. Close the log file.

   The Policy Server is set to operate in FIPS-migration mode.

7. Repeat the previous steps for each Policy Server in the environment.

You may now re-encrypt the policy store key for each Policy Server in the environment.

Re-encrypt a Policy Store Key

You re-encrypt the policy store key to replace the existing key with a version that is encrypted using FIPS-compliant algorithms.

To re-encrypt the policy store key

1. Open a command prompt from the computer hosting the Policy server and run the following command:

   smreg -cf MIGRATE -key *key_value*

   -cf MIGRATE

   Specifies that smreg run in FIPS-migration mode.

   Note: When smreg runs in FIPS-migration mode, the policy store key is re-generated using FIPS-compliant algorithms.

-key *key value*

Specifies the current policy store key.

smreg generates a new policy store key and encrypts it using FIPS-compliant algorithms.

2. Open the EncryptionKey.txt file, and verify that a new encryption key is present and prefixed with a FIPS-compliant algorithm.

   Prefix example: {AES}

   The policy store key is re-encrypted.

3. Repeat the latter steps for each Policy Server in the environment.

You may now re-encrypt the policy store administrator password.

Re-Encrypt the Policy Store Administrator Password

You re-encrypt the policy store administrator password to ensure that the data is encrypted using FIPS-compliant algorithms.

To re-encrypt the policy store administrator password

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

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

   Policy Store connection information appears.

2. Re-enter the administrator password in the Password field, and click Apply.

   The administrator password is encrypted using FIPS-compliant algorithms.

3. (Optional) If you have configured a separate database for one or more of the following, re-encrypt the administrator password for each:

   - key store
   - audit logs
   - token data
   - session server

   Important! A Policy Server operating in FIPS-only mode cannot decrypt a database password that remains encrypted with algorithms that are not FIPS compliant.

You may now re-encrypt the SiteMinder Super User password.

Re-encrypt the SiteMinder Super User Password

You re-encrypt the SiteMinder Super User password to ensure that the data is encrypted using FIPS-compliant algorithms.

Note: This is the password for the default administrator account. This account is used for all administrative tasks that do not require direct access to the Administrative UI. This is not the password for the Administrative UI administrator account with Super User privileges.

To reset the SiteMinder Super User password, open a command prompt and run the following command:

smreg -cf MIGRATE -su *password*

-cf MIGRATE

Specifies that smreg run in FIPS-migration mode.

Note: When smreg runs in FIPS-migration mode, the existing Super User password is saved using FIPS-compliant algorithms.

password

Specifies the existing Super User password.

Note: You do not have to supply a new password. You are entering the same password to ensure that the data is encrypted using FIPS-compliant algorithms.

The SiteMinder Super User password is encrypted using FIPS-compliant algorithms.

You may now set each of the Agents in the environment to FIPS-migration mode.

Set an Agent to FIPS-Migration Mode

You set the Agents to FIPS-migration mode so the environment can continue to use existing SiteMinder encryption algorithms as you re-encrypt sensitive data using FIPS-compliant algorithms.

To change the FIPS mode of an agent

1. Open the SmHost.conf file with a text editor.

   The following line appears in the file:

   fipsmode="COMPAT"

2. Edit the line to read:

   fipsmode="MIGRATE"

3. Save and close the file.
4. Restart the machine that is hosting the Agent.

   The agent is operating in FIPS-migration mode.
5. Repeat the previous steps for each machine in the environment on which a trusted hosted is registered.

You may now encrypt agent shared secrets.

Re-encrypt Client Shared Secrets

You re-encrypt the agent shared secrets to replace the existing secrets with secrets that are encrypted using FIPS-compliant algorithms. You re-encrypt shared secrets either:

- Manually rolling over the shared secret from the Administrative UI.
- Using smreghost in FIPS-migration mode

  Note: You only have to use smreghost if the agent was not configured for shared secret rollover when you registered the trusted host.

Use the Administrative UI to Re-encrypt a Shared Secret

To rollover the shared secret from the Administrative UI

1. Log into the Administrative UI and click Administration, Policy Server, Shared Secret Rollover.

   The Shared Secret Rollover pane appears.
2. Select the Rollover Shared Secret every radio button.

   Rollover Now becomes active.
3. Click Rollover Now.

   The Policy Server rolls over the shared secrets for all trusted hosts configured to allow shared secret rollover.

You may now re-encrypt sensitive policy and key data in the policy store.

Use smreghost to Re-encrypt a Shared Secret

To use smreghost to re-encrypt a shared secret

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

   smreghost -i *policy_server_ip_address* -u *administrator_user_name*
   -p *administrator_password* -hn *hostname_for_registration* -hc *host_config_object*
   -f *path_to_host_config_file* -o -cf MIGRATE

-i *policy server ip address*

Specifies the IP address of the Policy Server to which the trusted host is registered.

-u *administrator user name*

Specifies the name of the SiteMinder administrator with the rights to register a trusted host.

- p *administrator password*

Specifies the password of the administrator who is allowed to register a trusted host.

-hn *hostname for registration*

Specifies the current name of the host that is registered.

-hc *host configuration object*

Specifies the Host Configuration Object configured at the Policy Server.

-f *path to host config file*

Specifies the full path to the file that contains the registration data. The default file name is SmHost.conf.

Note: If you do not specify a file path, the updated file is saved in the location where you are running smreghost.

-o

Overwrites an existing trusted host. If you do not use this argument, you will have to delete the existing trusted host using the Administrative UI. We recommend using smreghost with this argument.

-cf MIGRATE

Specifies that smreghost run in FIPS-migration mode.

Note: When smreghost runs in FIPS-migration mode, the shared secret created and encrypted using FIPS-compliant algorithms.

smreghost re-registers the trusted host and creates a new shared secret that is encrypted using FIPS-approved algorithms.

2. Open the file that contains the trusted host registration data and verify that a new shared secret is present and prefixed with a FIPS-approved algorithm.

   The shared secret is encrypted using FIPS-compliant algorithms.

   Prefix example: {AES}

You may now re-encrypt sensitive policy and key data in the policy store.

Re-encrypt Policy and Key Store Data

You re-encrypt policy and key store data to ensure that sensitive data that is encrypted using existing SiteMinder algorithms is encrypted using FIPS-compliant algorithms.

Options for Re-encrypting Policy and Key Store Data

There are three ways to re-encrypt policy and key store data. You can:

- Re-encrypt the policy and key store data in an existing policy store.
- Re-encrypt policy data in an existing policy store and key data in an existing key store.
- Re-encrypt the policy and key store data, and migrate the data into a new r12.0 SP2 policy store or policy and key store, respectively.

This guide details the steps for re-encrypting the policy and key store data for existing stores.

If you want to create a new r12.0 SP2 policy store or policy and key store:

1. Export the key data using smkeyexport.

   Note: XPSExport does not export keys that are stored in a policy or key store. More information on using smkeyexport exists in the *Policy Server Administration Guide*.

2. Export the policy store data using XPSExport.

   Note: More information on using XPSExport exists in the *Policy Server Administration Guide*.

3. Create an r12.0 SP2 policy store or policy and key store.

   Note: More information on creating a policy and key stores exists in the *Policy Server Installation Guide*.

4. Import the key data into the new policy store, or if created, the new key store using smkeyimport.

   Note: More information on using smkeyimport exists in the *Policy Server Administration Guide*.

5. Import the policy store data into the new policy store using XPSImport.

   Note: More information on using XPSImport exists in the *Policy Server Administration Guide*.

Re-encrypt Keys Stored in the Policy or Key Store

You re-encrypt the keys stored in the policy or key store to replace the existing keys with versions that are encrypted using FIPS-compliant algorithms.

To re-encrypt the keys stored in the policy or key store

1. Open a command prompt from the computer hosting the Policy server and run the following command:

   smkeyexport -d*admin_name* -w*admin_password* -o*output_file_name* -l -v -t -cf

   -d*admin_name*

   Specifies the name of the SiteMinder administrator account.

   -w*admin_password*

   Specifies the password for the SiteMinder administrator account.

   -o*output_file_name*

   (Optional) Specifies the name of the exported file. If you do not specify a file name, the default file name is stdout.smdif.

   Note: Ensure that the file name contains the .smdif extension.

   Example: pskeys.smdif

   -l

   Specifies that a log file be created.

   -v

   (Optional) Enables verbose mode for troubleshooting.

   -t

   (Optional) Enables tracing for troubleshooting.

   -cf

   Specifies that smkeyexport run in FIPS-migration mode.

   Note: When smkeyexport runs in FIPS-migration mode, the keys stored in the policy store are exported and re-encrypted using FIPS-compliant algorithms.

   smkeyexport exports an smdif file that contains the re-encrypted keys.

2. Run the following command:

   smkeyimport -i*input_file_name* -d*admin_name* -w*admin_password* -l -v -t -cf

-i*input_file_name*

Specifies the name of the file output file you created.

Note: Ensure that the file name you specify includes the .smdif extension.

-d*admin_name*

Specifies the name of the SiteMinder administrator account.

-w*admin_password*

Specifies the password for the SiteMinder administrator account.

-l

Specifies that a log file be created.

-v

(Optional) Enables verbose mode for troubleshooting.

-t

(Optional) Enables tracing for troubleshooting.

-cf

Specifies that smkeyimport run in FIPS-migration mode.

smkeyimport imports the re-encrypted keys into the respective store.

You may now re-encrypt policy store data.

Re-encrypt the Policy Store Data

To re-encrypt the policy store data

1. Open a command prompt from the machine hosting the Policy Server and navigate to the location to which you want to export the policy store data file.
2. Run the following command:

   XPSExport *outputfile* -xa -passphrase *phrase* -vT -vI -vW -vE -vF -e file_name -l log_file

   Note: Although you can use XPSExport to export one or more granular objects, this procedure provides the arguments for exporting all of the policy store data. This ensures that the export includes all of the sensitive data. More information on exporting one or more granular objects exists in the *Policy Server Administration Guide*.

outputfile

Specifies the name of the XML output file.

Note: The file name must be unique. The export fails if a file with the same name exists.

Example: psdata

-xa

Specifies that all of the policy data is to be exported.

-passphrase *phrase*

Specifies a passphrase required for encryption of sensitive data. Record this value as it is required to import the sensitive data back into the policy store.

Limit: The passphrase must be contain at least:

- Eight (8) characters
- One (1) digit
- One (1) upper-case character
- One (1) lower-case character

Note: If the passphrase contains spaces, enclose it in quotes (").

-vT

(Optional) Sets verbosity level to TRACE.

-vI

(Optional) Sets verbosity level to INFO.

-vW

(Optional) Sets verbosity level to WARNING (default).

-vE

(Optional) Sets verbosity level to ERROR.

-vF

(Optional) Sets verbosity level to FATAL.

-l *log_path*

(Optional) Outputs log to the specified path.

-e *file_name*

(Optional) Specifies the file to which errors and exceptions are logged. If omitted, stderr is used.

XPSExport exports the policy store data and places the data file in the directory from which you ran the tool.

3. Run the following command:

   XPSImport *input_file* -passphrase *phrase* -vT -vI -vW -vE -vF -l *log_path*

   input_file

   Specifies the input XML file.

   -passphrase *phrase*

   Specifies the passphrase required for the decryption of sensitive data.

   Limit: The phrase must match the phrase you specified during export or the decryption fails.

   -vT

   (Optional) Sets verbosity level to TRACE.

   -vI

   (Optional) Sets verbosity level to INFO.

   -vW

   (Optional) Sets verbosity level to WARNING (default).

   -vE

   (Optional) Sets verbosity level to ERROR.

   -vF

   (Optional) Sets verbosity level to FATAL.

   -l *log_path*

   (Optional) Outputs log to the specified path.

   -e *file_name*

   (Optional) Specifies the file to which errors and exceptions are logged. If omitted, stderr is used.

   XPSImport imports the data into the policy store. Sensitive data is encrypted using FIPS-compliant algorithms.

If your environment users Basic Password Services, you may now verify that the Password Blobs are re-encrypted using FIPS-approved algorithms.

Verify that Password Blobs are Re-encrypted

You verify that the Policy Server has re-encrypted every Password Blob in the user store to prevent users from losing their password history and being locked out by Password Services.

When you configured the user store connection for password policies, you specified the Password Data user profile attribute. This value represents where Password Blobs are stored in the user store and is the value you use to identify Password Blobs that are not re-encrypted.

To verify that Password Blobs are re-encrypted

1. Using the directory server or database-specific tool, search for Password Data entries that are not prefixed with:

   {AES}

   Example: If "audio" is the value you specified in the Password Data field when configuring the user store connection, search for all entries stored in "audio" that are not prefixed with {AES}.

2. Identify the users whose Password Blobs are not prefixed with {AES}. The Policy Server has not re-encrypted these Password Blobs.

3. Notify these users that they must either log in or change their password.

   Note: How the password policy is configured determines when the Policy Server re-encrypts the Password Blob:

   - If the password policy is configured to track successful and/or failed logins, the Policy Server re-encrypts the Password Blob when the user logs in.
   - If the password policy is not configured to track logins, the Policy Server re-encrypts the Password Blob when the user changes the password.

Important! Password Services locks out users whose Password Blobs are not re-encrypted when the Policy Server is operating in FIPS-only mode. A user cannot regain access until you have deleted the Password Blob and cleared any disabled flags. Deleting the Password Blob results in the loss of the user's password history.

Migration Roadmap—Configure FIPS-Only Mode

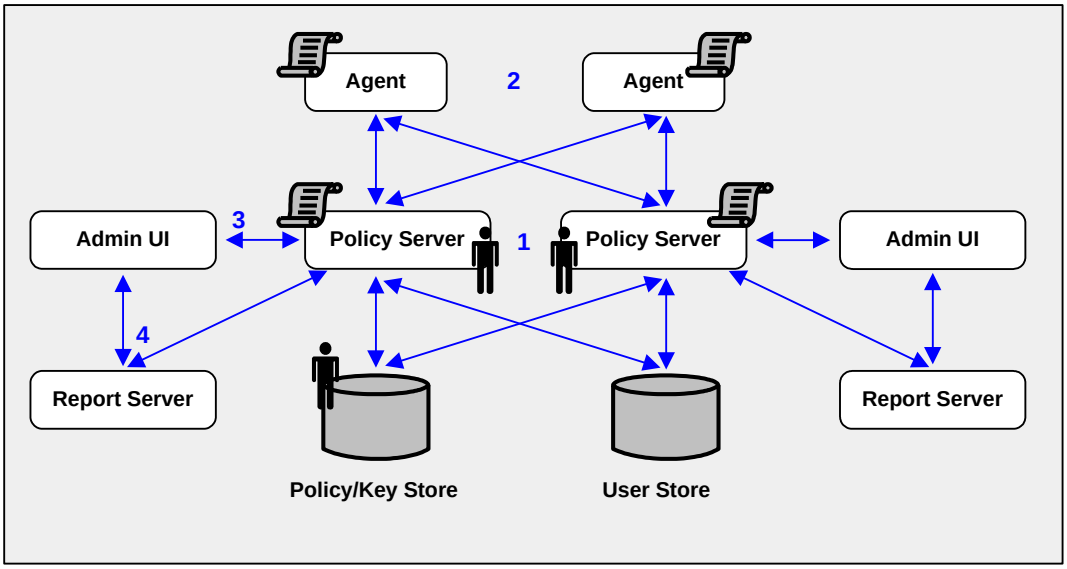
The following diagram illustrates a sample r12.0 SP2 environment operating in FIPS-migration mode and lists the order in which you configure each component and connection to operate in FIPS-only mode.

The shaded components represent sensitive data that must be re-encrypted using FIPS-approved algorithms. Do not continue with the migration process until you have:

- Re-encrypted the policy store key for each Policy Server in the environment
- Re-encrypted the policy store administrator password
- Re-encrypted the SiteMinder Super User password

- Re-encrypted the shared secret for each Agent in the environment
- Re-encrypted the policy store data
- Verified that the Policy Server has re-encrypted every user Password Blob in the user store, if the environment is using Basic Password Services.

  Important! Password Services locks out users whose Password Blobs are not re-encrypted when the Policy Server is operating in FIPS-only mode. A user cannot regain access until you have deleted the Password Blob and cleared any disabled flags. Deleting the Password Blob results in the loss of the user's password history.



1. Each Policy Server in the environment is set to operate in FIPS-only mode.
2. Each SiteMinder Web Agent, including custom Agents, is set to operate in FIPS-only mode.
3. The existing connection between each Administrative UI and its respective Policy Server is encrypted using algorithms that are not FIPS compliant. Re-register each Administrative UI with its respective Policy Server to encrypt the connection using FIPS-compliant algorithms.
4. The existing connection between a Report Server and a Policy Server is encrypted using algorithms that are not FIPS compliant. Re-register each Report Server with its respective Policy Server to encrypt the connection using FIPS-compliant algorithms.

How to Configure FIPS-only Mode

Complete the following procedures to be sure that your environment only encrypts sensitive data using FIPs–compliant algorithms:

1. Set each Agent in the environment to FIPS–only mode.
2. Set each Policy Server in the environment to FIPS–only mode.
3. Re–register an Administrative UI with its respective Policy Server. Consider the following:
   - The Administrative UI is unavailable during registration process. However, the Policy Server continues to provide access control and generate log files that contain auditing information during this time.
   - The Administrative UI can be configured for internal or external administrator authentication.
     - An Administrative UI configured for internal authentication is one that is using the policy store as it source for administrator credentials.
     - An Administrative UI configured for external authentication is one that is using an external user store as its source for administrator credentials.

     The process you follow to re–register an Administrative UI depends on how it is authenticating SiteMinder administrators.

   Note: Repeat this step until all Administrative UI connections are re–registered.
4. Re–register a Report Server with its respective Policy Server.

   Note: Repeat this step until all Report Server connections are re–registered.

Set an Agent to FIPS-only Mode

You set an Agent to FIPS-only mode to ensure that the Agent only accepts session keys, Agent Keys, and shared secrets that are encrypted using FIPS-compliant algorithms.

To set an Agent to FIPS-only mode

1. Open the SmHost.conf file with a text editor.

   The following line appears in the file:

   ```
   fipsmode="MIGRATE"
   ```

2. Edit the line to read:

   ```
   fipsmode="ONLY"
   ```

3. Save and close the file.

4. Restart the machine that is hosting the Agent.

   The agent is operating in FIPS-migration mode.

5. Repeat the previous steps for each machine in the environment that is registered as a trusted hosted.

You may now set Policy Servers to operate in FIPS-only mode.

Set the Policy Server to FIPS-only Mode

Setting the Policy Server to FIPS-only mode configures the Policy Server to only read and write encrypted information using FIPS-compliant algorithms.

Important! Password Services locks out users whose Password Blobs are not re-encrypted when the Policy Server is operating in FIPS-only mode. A user cannot regain access until you have deleted the Password Blob and cleared any disabled flags. Deleting the Password Blob results in the loss of the user's password history.

Note: More information on identifying Password Blobs that are not re-encrypted exists in Verify that Password Blobs are Re-encrypted (see page 111).

To set the Policy Server to FIPS-only mode

1. Open a command prompt from the machine hosting the Policy Server and run the following command:

   setFIPSonly

   ONLY appears in the command window.

2. Stop the Policy Server.

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

3. Do one of the following:

   a. If the Policy Server is installed on a Windows system, reboot the machine.

   b. If the Policy Server is installed on a UNIX system, log in as the user who is used to start the Policy Server.

4. Start the Policy Server.

5. Open the smps.log file and verify that the following line appears:

   Policy Server employing only FIPS-140 cryptographic algorithms.

6. Close the log file.

   The Policy Server is set to operate in FIPS-only mode.

7. Repeat the latter steps for each Policy Server in the environment.

You may now re-register each Administrative UI with its respective Policy Server.

How to Re–Register an Administrative UI Configured for Internal Authentication

Existing SiteMinder algorithms continue to encrypt the shared secret that the Administrative UI and the Policy Server use to establish an encrypted connection. Re–registering the Administrative UI creates a new shared secret that is encrypted using FIPS–compliant algorithms.

Complete the following procedures to re–register an Administrative UI configured for internal authentication:

1. Stop the application server.
2. Delete the Administrative UI data directory.
3. Reset the Administrative UI registration window.
4. Start the application server.
5. Register the Administrative UI.

Stop the Application Server

To stop the application server

1. Log into the Administrative UI host system.
2. Do one of the following:
   - If you installed the Administrative UI using the stand–alone installation option, stop the SiteMinder Administrative UI service.
   - If you installed the Administrative UI to an existing application server infrastructure, stop the application server.

   Note: For more information about stopping the application server, see the *Policy Server Installation Guide*.

Delete the Administrative UI Data Directory

Delete the Administrative UI data directory to remove the existing trusted connection between the Administrative UI and the Policy Server.

To delete the Administrative UI data directory

1. Log into the Administrative UI host system.
2. Do one of the following:
   - (Stand–alone) If you installed the Administrative UI using the stand–alone installation option, navigate to *administrative_ui_home*/CA/SiteMinder/adminui/server/default and delete the following folder:

     data

     administrative_ui_home

     Specifies the Administrative UI installation path.
   - (JBoss) If you installed the Administrative UI to an existing JBoss infrastructure, navigate to *JBoss_home*/server/default/data.

     JBoss_home

     Specifies the JBoss installation path.

     The data folder contains the apacheds, derby, and siteminder folders.

     a. Delete the siteminder folder.

     b. Open the apacheds folder and delete the siteminder folder.

     c. Open the derby folder and delete the siteminder folder.
   - (WebLogic) If you installed the Administrative UI to an existing WebLogic infrastructure, navigate to *WebLogic_domain_folder,* and delete the following folder:

     data

     WebLogic_domain_folder

     Specifies the path to the WebLogic domain created for the Administrative UI.

- (WebSphere) If you installed the Administrative UI to an existing WebSphere infrastructure, navigate to *WebSphere_home*/profiles/*profile,* and delete the following folder:

  data

  WebSphere_home

  Specifies the full path of the WebSphere installation.

  profile

  Specifies the name of the profile used for the Administrative UI.

The Administrative UI data dictionary is deleted.

Reset the Administrative UI Registration Window

Reset the registration window to submit the credentials of any super user in the policy store. The Policy Server uses these credentials to verify that the registration request is valid and that the relationship between the Administrative UI and the Policy Server can be trusted.

To reset the Administrative UI 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 with super user permissions.

   Note: If a super user account is not available, 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 re–registered with a Policy Server.

-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 to complete 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 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.

Start the Application Server

To start the application server

1. Log into the Administrative UI host system.
2. Do one of the following:
   - If you installed the Administrative UI using the stand–alone installation option, start the SiteMinder Administrative UI service.
   - If you installed the Administrative UI to an existing application server infrastructure, start the application server.

   Note: For more information about starting the application server, see the *Policy Server Installation Guide*.

Register the Administrative UI

Register the Administrative UI to create a new shared secret that is encrypted using FIPS–compliant algorithms.

Note: For more information about registering the Administrative UI, see the *Policy Server Installation Guide*.

How to Re–Register an Administrative UI Configured for External Authentication

Existing SiteMinder algorithms continue to encrypt the shared secret that the Administrative UI and the Policy Server use to establish an encrypted connection. Re–registering the Administrative UI creates a new shared secret that is encrypted using FIPS–compliant algorithms.

Complete the following procedures to re–register an Administrative UI configured for external authentication:

1. Delete the existing connection between the Administrative UI and the Policy Server.
2. Run the Administrative UI registration tool.
3. Gather registration information.
4. Configure the Administrative UI and Policy Server connection.
5. Delete the previous trusted host.

Delete an Administrative UI Connection to the Policy Server

You delete the Administrative UI connection to the Policy Server so that you can re–register the connection.

To delete the Administrative UI connection to the Policy Server

1. Log into the Administrative UI and click Administration, Admin UI.

   A list of connection types appears.

2. Click Policy Server Connections, Delete Policy Server Connection.

   The Delete Policy Server Connection pane appears.

3. Enter search criteria, and click Search.

   Connections matching your criteria appear.

4. Select the connection you want to delete, and click Select.

   You are prompted to confirm the request.

5. Click Yes.

   The connection between the Administrative UI and the Policy Server is deleted.

Run the Registration Tool

You run the Administrative UI registration tool to create a client name and passphrase. A client name and passphrase pairing are values that the Policy Server uses to identify the Administrative UI you are registering. You submit the client and passphrase values from the Administrative UI to complete the registration process.

To run the registration tool

1. Open a command prompt from the Policy Server host system.
2. Run the following command:

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

   Note: Inserting a space between *client_name* and [:*passphrase*] results in an error.

   client_name

   Identifies the Administrative UI being registered.

   Limit: This value must be unique. For example, if you have previously used smui1 to register an Administrative UI, enter smui2.

   Note: Record this value. This value is to complete the registration process from the Administrative UI.

   passphrase

   Specifies the password required to complete the registration of the Administrative UI.

   Limits:

   - The passphrase must contain at least six (6) characters.
   - The passphrase cannot include an ampersand (&) or an asterisk (*).
   - If the passphrase contains a space, it must be enclosed in quotation marks.
   - If you are registering the Administrative UI as part of an upgrade, you can reuse a previous passphrase.

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

   Important! Record the passphrase, so that you can refer to it later.

   -adminui

   Specifies that an Administrative UI is being registered.

   -t *timeout*

   (Optional) Specifies how long you have to complete the registration process from the Administrative UI. The Policy Server denies the registration request when the timeout value is reached.

   Unit of measurement: minutes

   Default: 240 (four hours)

Minimum Limit: 1

Maximum Limit: 1440 (one day)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you complete the registration process from the Administrative UI. A failed attempt can result from an incorrect client name or passphrase submitted to the Policy Server during the registration process.

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comments with quotes.

-l *log_path*

(Optional) Specifies where to export the registration log file.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

The registration tool lists the name of the registration log file and prompts for a passphrase.

3. Press Enter.

   The registration tool creates the client name and passphrase pairing.

You can now register the Administrative UI with a Policy Server. You complete the registration process from the Administrative UI.

Gather Registration Information

The Administrative UI requires specific information about the Policy Server and the client name and passphrase you created to complete the registration process. Gather the following information before logging into the Administrative UI:

- **Client name**—The client name you specified using the XPSRegClient tool.
- **Passphrase**—The passphrase you specified using the XPSRegClient tool.
- **Policy Server host**—The IP address or name of the Policy Server host system.
- **Policy Server authentication port**—The port on which the Policy Server is listening for authentication requests.

  Default: 44442

Note: A worksheet is provided to help you gather and record information before registering the Administrative UI.

Configure the Connection to the Policy Server

You configure the Administrative UI and Policy Server connection so SiteMinder administrators can use the Administrative UI to manage policy information through the Policy Server. You configure the connection from the Administrative UI.

To configure the Administrative UI and Policy Server connection

1. Open a supported web browser and enter the following:

   http://*host.domain*/iam/siteminder/adminui

   The Administrative UI login screen appears.

2. Log in as a super user.
3. Click Administration, Admin UI.

4. Click Policy Server Connections, Register Policy Server Connection.

   The Register Policy Server Connection pane opens.

   Note: Click Help for descriptions of settings and controls, including their respective requirements and limits.

5. Type a connection name in the Name field on the General group box.
6. Type the name or IP address of the Policy Server host system in the Policy Server Host field.
7. 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.

8. Type the client name and passphrase you created using the registration tool in the fields on the General group box.
9. Select the FIPS only mode radio button.
10. Click Submit.

    The connection between the Administrative UI and Policy Server is configured. The shared secret the Administrative UI and Policy Server use to establish an encrypted connection is encrypted using FIPS-approved algorithms.

You have completed the process for re–registering the Administrative UI.

Delete the Previous Trusted Host

Re–registering the Administrative UI with a Policy Server creates a new trusted host. You delete the previous trusted host as it is no longer needed.

To delete the trusted host connection

1. Log into the Administrative UI and click Infrastructure, Hosts.
2. Click Trusted Hosts, Delete Trusted Host.

   The Delete Trusted Host pane appears.

3. Search for and select the previous trusted host connection.

   Note: A trusted host that is created as a result of the Administrative UI registration process has the following description: Generated by XPSRegClient.

4. Click Select.

   The Administrative UI prompts you to verify the selection.

   Important! Be sure that you delete the trusted host that was created the last time you registered the Administrative UI and not the new trusted host.

5. Click Yes.

   The trusted host connection is deleted.

How to Re-Register the Report Server Connection

Re-registering the Report Server ensures that the connection between the Report Server and the Policy server is encrypted using FIPS-approved algorithms.

Complete the following steps to re-register a report server:

1. Create the Report Server client name and passphrase.
2. Gather registration information.
3. Register the Report Server with the policy server.

Create a Client Name and Passphrase

You run the XPSRegClient utility to create a client name and passphrase. A client name and passphrase are:

- Values that the Policy Server uses to identify the Report Server you are registering
- Values that you use with the XPSRegClient tool to register the Report Server with the Policy Server

To run the registration tool

1. Open a command–line window from the Policy Server host system.
2. Navigate to *siteminder_home*/bin.

   siteminder_home

   Specifies the Policy Server installation path.

3. Run the following command:

   XPSRegClient *client_name*[:*passphrase*] -report -t *timeout* -r *retries* -c *comment* -cp -l *log_path* -e *error_path* -vT -vI -vW -vE -vF

client_name

Identifies the name of Report Server you are registering.

Limit: The value must be unique. For example, if you have previously used reportserver1, enter reportserver2.

Note: Record this value. This value is required to complete registration process from the Report Server host system.

passphrase

Specifies the password required to complete the Report Server registration.

Limits: The passphrase

- Must contain at least six (6) characters.
- The passphrase cannot include an ampersand (&) or an asterisk (*).
- If the passphrase contains a space, it must be enclosed in quotation marks.

If you do not specify the passphrase in this step, XPSRegClient prompts you to enter and confirm it.

Note: Record this value. This value is required to complete registration process from the Report Server host system.

-report

Specifies that a Report Server is being registered.

-t *timeout*

(Optional) Specifies how long you have to complete the registration process from the Report Server host system. The Policy Server denies the registration request when the timeout value is reached.

Unit of measurement: minutes

Default: 240 (4 hours)

Minimum Limit: 1

Maximum Limit: 1440 (one day)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you complete the registration process from the Report Server host system. A failed attempt can result from submitting an incorrect passphrase to the Policy Server during the registration.

Default: 1

Maximum Limit: 5

-c *comment*

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

Note: Surround comments with quotes.

-cp

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

Note: Surround comment with quotes.

-l *log path*

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

Default: siteminder_home\log, where siteminder_home is where the Policy Server is installed.

-e *error path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

The utility lists the name of the registration log file. If you did not provide a passphrase, the utility prompts for one.

4. Press Enter.

   The registration tool creates the client name and passphrase.

You can now register the Report Server with the Policy Server. You complete the registration process from the Report Server host system.

Gather Registration Information

Completing the registration process between the Report Server and the Policy Server requires specific information. Gather the following information before running the XPSRegClient utility from the Report Server host system.

- **Client name**—The client name you specified using the XPSRegClient tool.
- **Passphrase**—The passphrase you specified using the XPSRegClient tool.
- **Policy Server host**—The IP address or name of the Policy Server host system.

Register the Report Server with the Policy Server

You register the Report Server with the Policy Server to create a trusted relationship between both components. You configure the connection from the Report Server host system using the Report Server registration tool.

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 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 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

Specifies how the communication between the Report Server and the Policy Server is encrypted.

- Zero (0) specifies FIPS–compatibility mode
- One (1) specifies FIPS–only mode.

Default: 0

3. Press Enter.

You receive a message stating that the registration is successful. You have completed re–registering the Report Server with the Policy Server. The connection between the Report Server and the Policy Server is encrypted using FIPS-compliant algorithms.

Appendix A: Upgrade and FIPS Worksheets

You can use the following worksheets to record the necessary information to upgrade:

- A supported LDAP database as a policy store
- A supported relational database as a policy store
- An individual relational database as an audit logging database, key store, token store or session store

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	

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	

Information Needed	Your Value
Administrative DN	
Administrative password	

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	

Microsoft ADAM Information Worksheet

You can use this worksheet to gather the required information for configuring a Microsoft ADAM 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	

Administrative UI Registration Worksheet

You can use this worksheet to gather the required registration information for the Administrative UI installation:

Required Information	Your Value
Client name	
Passphrase	
Policy Server host name	
Policy Server port number	

FIPS Information Worksheet

You can use this worksheet to gather the required information for re-encrypting existing sensitive data while Policy Servers are operating in FIPS-migration mode.

Information Needed	Your Value
SiteMinder Super User account name and password	
Policy store administrator password	

More information:

Gather Environment Information (see page 101)

Appendix B: Platform Support and Installation Media

This section contains the following topics:

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

I

L

M

O

P

R

S

U

V

W