

CA SiteMinder®

Upgrade Guide

12.52



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

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA SiteMinder®
- CA SiteMinder® Web Services Security (CA SOA Security Manager)
- CA Security Command Center
- CA Audit iRecorder for CA SiteMinder®

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

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

- [How to Upgrade Your Audit Store to Accommodate Assertion Attribute Logging](#)—Revised DB2 instructions. Upgrade script adds NULL values properly, manual editing of the upgrade script is no longer required.
- [How to Configure a Parallel Environment](#) (see page 105)—Revised steps and XPSImport command switches.
- [Component versions in this guide](#) (see page 9)—Added reference to r12.5 to indicate support for upgrading from r12.5.
- [Korn Shell \(ksh\) Package Required on Linux](#) (see page 51)—Added to describe the libraries required for upgrading the Policy Server.
- [Verify that Existing Federated SAML Partnerships Do Not Have the Same Backchannel Username](#) (see page 89)—Added topic to describe upgrade requirement that no existing partnerships can have incoming backchannel usernames (within the same protocol) that are the same. Resolves CQ 177179.
- [How the 12.x Migration Works](#) (see page 82)—Removed a note that stated that a 12.52 web agent could not be installed and configured with a 12.52 Policy Server, until the policy store has been upgraded. Added a note revising guidance about installing a 12.52 web agent before the policy store is upgraded.

Contents

Chapter 1: Planning an Upgrade	9
Component Versions in this Guide.....	9
Upgrade Paths.....	10
Migration.....	10
Parallel Upgrade.....	11
How to Plan a Migration	12
Review the Policy Server Release Notes	13
Analyze Your SiteMinder Environment.....	13
Plan a Recovery Strategy.....	15
Determine the Upgrade Path.....	16
Mixed SiteMinder Environments	17
How to Plan a Parallel Upgrade.....	20
How to Upgrade Simple Test Environments	21
Common CA SiteMinder® Environments	22
Single Policy Store, Multiple Policy Servers and Web Agents.....	22
Clustered Environment	23
Shared User Directory Environment	24
Chapter 2: Upgrading from r6.x	27
Migration Considerations.....	27
Policy Server Option Pack Support.....	27
Crystal Reports in 12.x	27
Administrator Authentication	28
Certificate Data Management.....	29
Federation Integration	30
Single Sign-on	30
Avoid Policy Store Corruption	30
Advanced Password Services	30
How the r6.x Migration Works.....	31
How to Migrate from r6.x	34
Download the Policy Store Schema Files	34
Extend the Policy Store Schema.....	35
Synchronize Key Database Instances	47
Upgrade an r6.x Policy Server	48
After You Upgrade the Policy Server.....	58
Upgrade an r6.x Web Agent.....	58

Upgrade an r6.x Policy Store.....	60
Install the Administrative User Interface	65
Upgrade an r6.x Session Store	65
Upgrade an r6.x Audit Log Database.....	65
How a Parallel Upgrade Works.....	66
How to Configure a Parallel Environment.....	67
Parallel Environment Key Management Options.....	67
Create the 12.52 Environment.....	70
Common Key Store Single Sign-on Requirements.....	71
How to Separate a Key Store from a Policy Store	71
Multiple Key Store Single Sign-on Requirements.....	75
Migrate Keys and Certificates	75
Migrate the Assertion Issuer ID.....	77
Migrate the r6.x Policies	78
User Directory Single Sign-on Requirements	78
Chapter 3: Upgrading from r12.x	79
Migration Considerations.....	79
Administrative UI Upgrade Paths	79
Administrative UI Protection with SiteMinder	80
Single Sign-on	80
Certificate Data Management.....	80
Federation Integration	81
Avoid Policy Store Corruption	82
Advanced Password Services	82
How the r12.x Migration Works.....	82
How to Migrate from r12.x	85
Synchronize Key Database Instances	85
Upgrade an r12.x Policy Server	86
Upgrade an r12.x Web Agent.....	94
How to Upgrade an r12.x Policy Store	96
Upgrade an r12.x Administrative UI.....	99
Upgrade an r12.x Report Server.....	104
How a Parallel Upgrade Works.....	105
How to Configure a Parallel Environment.....	105
Parallel Environment Key Management Options.....	106
Create the 12.52 Environment.....	109
Common Key Store Single Sign-on Requirements.....	109
How to Separate a Key Store from a Policy Store	110
Multiple Key Store Single Sign-on Requirements.....	114
Migrate Keys and Certificates	114

Migrate the Assertion Issuer ID.....	116
Migrate the r12.x Policies	116
User Directory Single Sign on Requirements	117

Chapter 4: Using FIPS-Compliant Algorithms 119

FIPS 140-2 Migration Overview.....	119
FIPS 140-2 Migration Requirements	120
Migration Roadmap—Re-Encrypt Sensitive Data	120
How to Re-Encrypt Existing Sensitive Data	122
Gather Environment Information	123
Set a Policy Server to FIPS-Migration Mode.....	123
Re-encrypt a Policy Store Key	125
Re-Encrypt the Policy Store Administrator Password	126
Re-encrypt the CA SiteMinder® Super User Password	126
Set an Agent to FIPS-Migration Mode.....	127
Re-encrypt Client Shared Secrets.....	127
Re-encrypt Policy and Key Store Data.....	129
Verify that Password Blobs are Re-encrypted.....	134
Migration Roadmap—Configure FIPS-Only Mode	135
How to Configure FIPS-only Mode	136
Set an Agent to FIPS-only Mode.....	137
Set the Policy Server to FIPS-only Mode	137
How to Re-Register an Administrative UI Configured for Internal Authentication	138
How to Re-Register an Administrative UI Configured for External Authentication	143
How to Re-Register the Report Server Connection.....	148

Chapter 5: Troubleshoot a SiteMinder Key Database Migration 153

Status of CA SiteMinder® Key Database Migration Unknown	153
Certificate Data Store Error Appears.....	154
Migration Failed Error Appears	155
Migrate a CA SiteMinder® Key Database Manually	155

Index 159

Chapter 1: Planning an Upgrade

Component Versions in this Guide

This guide details the paths for upgrading a CA SiteMinder® environment to 12.52. An upgrade to 12.52 is supported from the following versions:

- r6.0 SP5 CR32
- r6.0 SP5 J
- r12.0 SP2
- r12.0 SP3
- r12.0 SP3 J
- r12.5

The component versions in this guide include:

- CA SiteMinder® Administrative UI upgrades from r12.x. In this guide:
 - r12.x is r12.0 SP2, r12.0 SP3, and r12.5
- Policy Server and policy store upgrades from r6.x and r12.x. In this guide:
 - r6.x is r6.0 SP5.
 - r12.x is r12.0 SP2, r12.0 SP3, and r12.5
- CA Business Intelligence Common Reporting component (Report Server) upgrades from r12.x. In this guide:
 - r12.x is r12.0 SP2 and r12.0 SP3 up to and including cr3.

Note: If you installed and configured an r12.0 SP3 cr4 or higher Report Server, an upgrade is not required.
- Web Agent upgrades from r6.x and r12.x. In this guide:
 - r6.x is r6.x QMR 5.
 - r12.x is r12.0 SP2, r12.0 SP3, and r12.5.

Upgrade Paths

An upgrade consists of deploying 12.52 components to an existing CA SiteMinder® environment. Upgrading to 12.52 can be accomplished in two ways:

- Completing a migration.
- Configuring a parallel 12.52 environment next to an existing environment. Both environments use one or more key stores to maintain single sign-on.

Migration

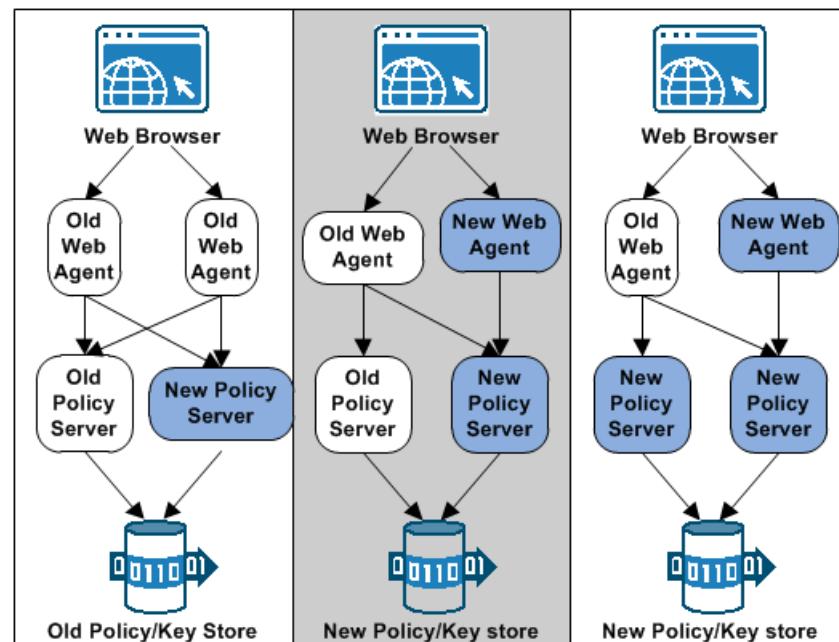
A migration is the process of upgrading individual CA SiteMinder® components until your environment is operating at 12.52. Upgrading individual components consists of one or more steps during which you:

- 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 diagram illustrates the concept of a migration. For more information about migrating from r6.x or r12.x, see the respective chapter:

Figure 1: Simple migration overview



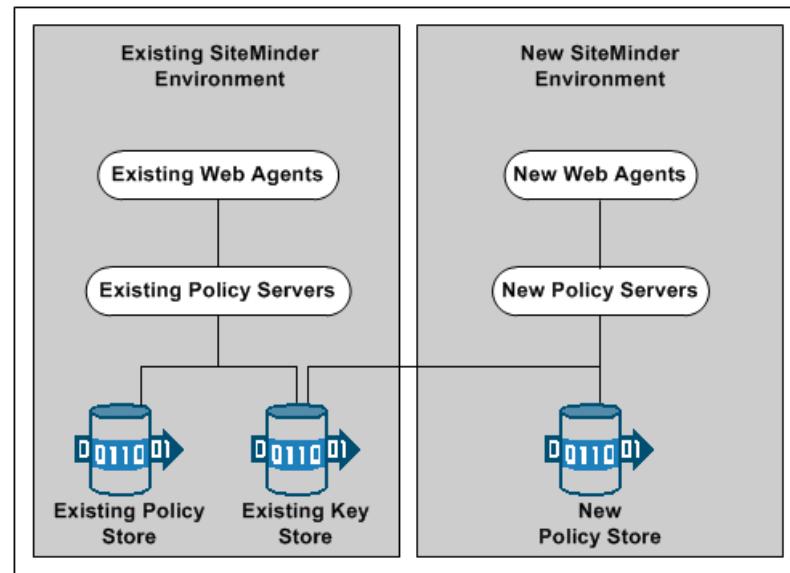
Parallel Upgrade

A parallel upgrade is the process of configuring an 12.52 environment next to an existing environment. Configuring a parallel upgrade consists of multiple steps during which you:

- Leave the existing environment unchanged.
- Configure an 12.52 environment.
- Use a common key store or multiple key stores to enable single sign-on between both environments.

The following diagram 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.

Figure 2: Parallel upgrade overview



How to Plan a Migration

Migrating a complex CA 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 12.52 supports your current third-party products and hardware.

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

- A site analysis
Determine the current state of your CA SiteMinder® environment and when it is the best time to update each component.
- CA SiteMinder® Components
List the individual CA 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.

Review the Policy Server Release Notes

The Policy Server Release Notes includes installation and upgrade considerations. We recommend that you review this material before beginning a migration.

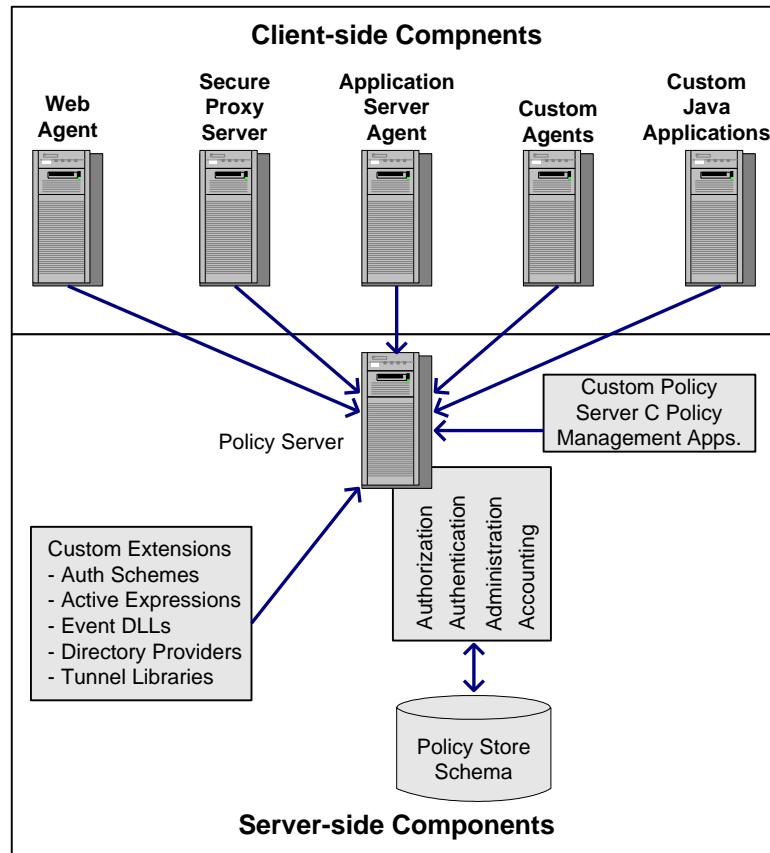
Analyze Your SiteMinder Environment

Analyze your CA 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.
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.

Question	Recommendation
Are your Web Agents working in failover or round robin mode?	To maintain failover and round robin, refer to Mixed CA SiteMinder® Environments.
Are you using single sign-on across the CA SiteMinder® environment?	See this guide for more information about maintaining single sign-on.
Are you using credential collectors for authentication schemes?	See the <i>Web Agent Configuration Guide</i> for more information about using credential collectors in a mixed environment.
Does 12.52 support your third-party hardware and software?	See the CA SiteMinder® 12.52 Platform Support Matrix on the Technical Support Site.
Do you have CA SiteMinder® software that Professional Services customized?	Contact Customer Support for instructions.
Do you have access to previous versions of CA SiteMinder® documentation? This guide refers to the previous CA SiteMinder® documentation.	Locate the CA 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 CA SiteMinder® components to consider before upgrading:



Plan a Recovery Strategy

Implement a recovery plan that lets you recover 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, complete the following steps:

- 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 12.52 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 managing Web Agents centrally, 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.x, 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.

Determine the Upgrade Path

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

- r6.x and 12.52 components
- r12.x and 12.52 components

The following table lists the supported Policy Server upgrade paths for a migration to 12.52:

Policy Server Versions	Upgrade To
r6.0 SP5	12.52
r12.0 SP2	12.52
r12.0 SP3	12.52

The following table lists the supported Web Agent upgrade paths for a migration to 12.52:

Web Agent Versions	Upgrade To
r6.x QMR 5	12.52
r12.0 SP2	12.52
r12.0 SP3	12.52

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 12.52:

Administrative UI Versions	Upgrade To
r12.0 SP2	12.52
r12.0 SP3	12.52

The following table lists the supported Report Server upgrade path for a migration to 12.52:

Report Server Versions	Upgrade To
r12.0 SP2	12.52
r12.0 SP3 up to and including cr3	12.52

Note: If you installed and configured an r12.0 SP3 cr4 or higher Report Server, an upgrade is not required.

Mixed SiteMinder Environments

As you migrate to 12.52, your environment can contain a combination of CA SiteMinder® components at different versions. In addition, you do not have to upgrade all of your components to 12.52. You can leave some components at the current version. Consider the following items:

- If your environment contains a combination of r6.x components, 12.52 Policy Servers can continue to communicate with r6.x policy stores.
- If your environment contains a combination of r12.x components, 12.52 Policy Servers can continue to communicate with r12.x policy stores.
- If your environment contains a mix of Policy Server versions, users can continue to access resources and have the same experience using r6.x QMR6, r12.0 SP2, or r12.0 SP3 agents.
- A mixed environment can support single sign-on.

Use Mixed-Mode Support

Mixed-mode support lets an 12.52 Policy Server communicate with an r6.x or an r12.x 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. You cannot disable mixed-mode support.

The Policy Server Management Console lets you see what policy store version the 12.52 Policy Server is using.

Follow these steps:

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

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

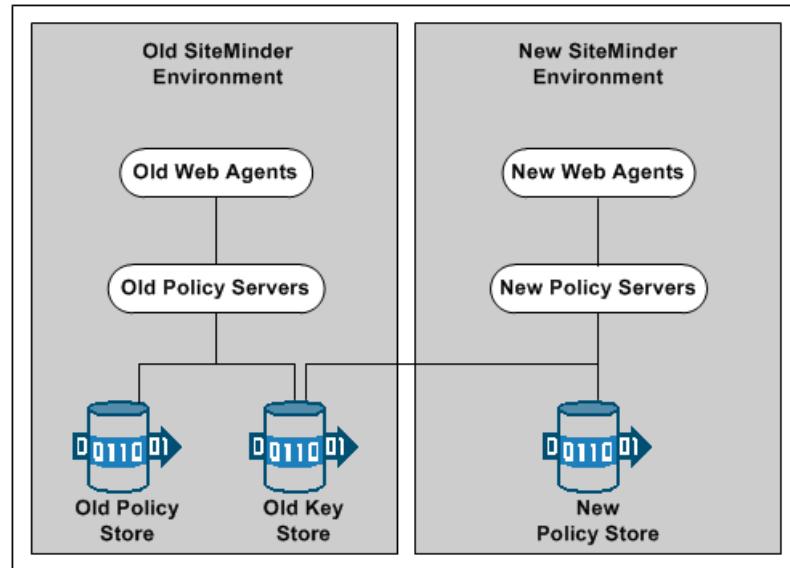
6.x Mixed Mode Support

Consider the following items when migrating from r6.x to 12.52:

- An r6.x Policy Server cannot communicate with an 12.52 policy store.
- An 12.52 Policy Server can communicate with an r6.x policy store.
- An r6.x and an 12.52 Policy Server can share a key store.
- An r6.x and an 12.52 Policy Server can share a session store.
- An r6.x Web Agent can communicate with an 12.52 Policy Server.

The following figure details r6.x mixed-mode support:

Figure 3: r6.x common key store deployment



Limitations of a 6.x Mixed Environment

An 12.52 Policy Server can communicate with an r6.x policy store, but an r6.x Policy Server cannot connect to an 12.52 policy store. As a result, all existing r6.x features are available in a mixed environment, but the features specific to r12.x and 12.52 are not available.

Note: For more information about features in r12.x and 12.52, see the release notes.

r12.x Mixed Mode Support

Consider the following items when migrating from r12.0 SP1 or r12.0 SP2 to 12.52:

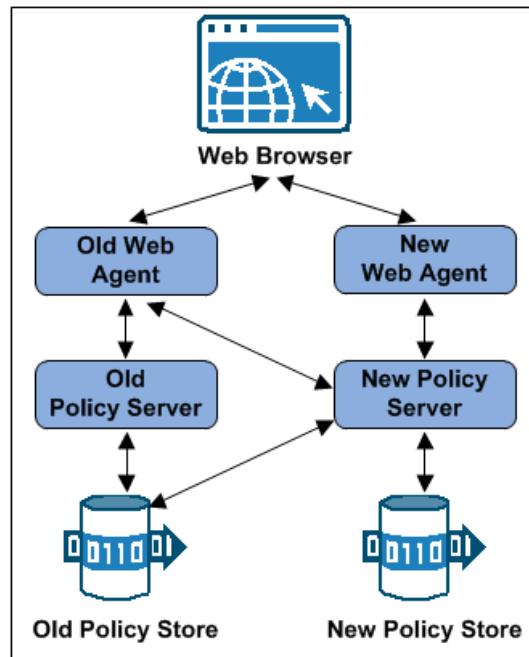
- An r12.x Policy Server cannot communicate with an 12.52 policy store.

An 12.52 Policy Server can communicate with an 12.52 policy store.

- An r12.x Policy Server can share a key store with an 12.52 Policy Server.
- An r12.x Policy Server can share a session store with an 12.52 Policy Server.
- An r12.x Web Agent can communicate with an 12.52 Policy Server.

The following figure details mixed-mode support:

Figure 4: r12.x mixed-mode support



Limitations of an r12.x Mixed Environment

An 12.52 Policy Server can communicate with an r12.x policy store, but an r12.x Policy Server cannot connect to an 12.52 policy store. As a result, all existing r12.x features are available in a mixed environment, but the features specific to 12.52 are not available.

Note: For more information about features in 12.52, see the release notes.

How to Plan a Parallel Upgrade

Configuring a parallel CA 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 12.52 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 12.52 policy store.
- If you are upgrading from r12.x, use XPSImport to import the r12.x policy store data into the 12.52 policy store.

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

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

When moving CA SiteMinder® policies from one environment to another, either as part of an upgrade or a policy migration, some objects that are environment-specific are included in the export file. Examples of these objects include:

- Trusted hosts
- HCO Policy Server settings
- Authentication scheme URLs
- Password services redirects
- Redirect responses

Depending on the mode you select when using XPSExport, these objects may be added to the new environment or can overwrite existing settings. Be sure that you do not adversely affect environment settings when importing the objects.

Common CA SiteMinder® Environments

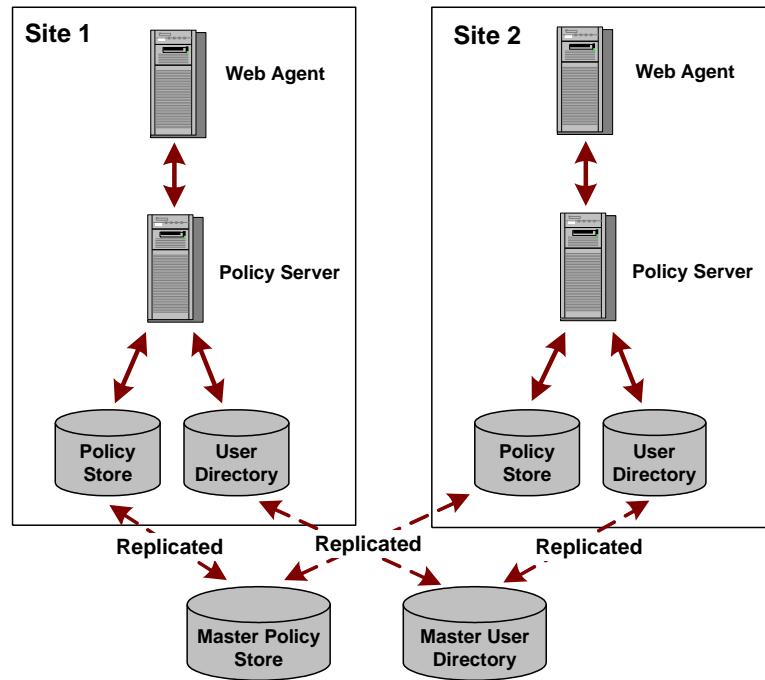
There are several common CA SiteMinder® environments to consider before upgrading to 12.52. See if your site matches one of the following:

- [Single Policy Store, Multiple Policy Servers and Web Agents](#) (see page 22)
- [Clustered Environment](#) (see page 23)
- [Shared User Directory Environment](#) (see page 24)

Single Policy Store, Multiple Policy Servers and Web Agents

This CA 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:



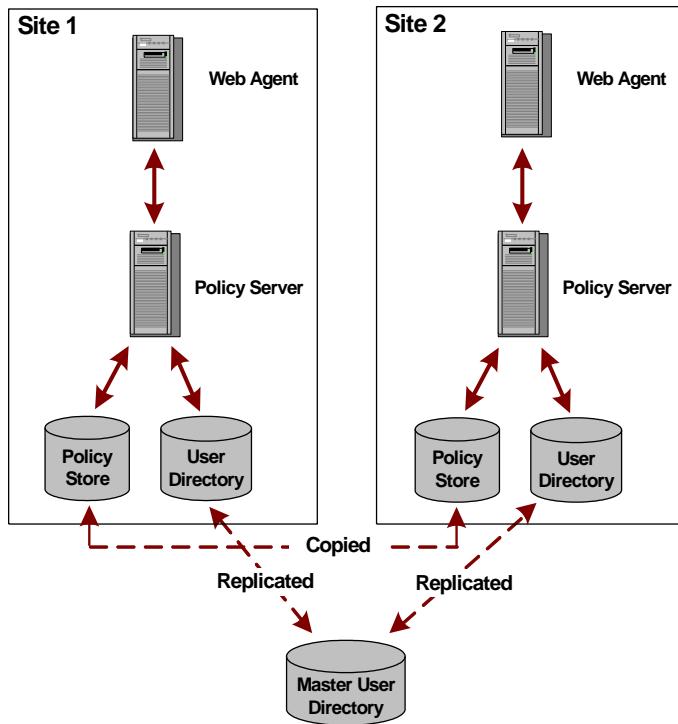
Use the procedures outlined in this guide to upgrade this environment.

Clustered Environment

A clustered environment is similar to the CA 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:

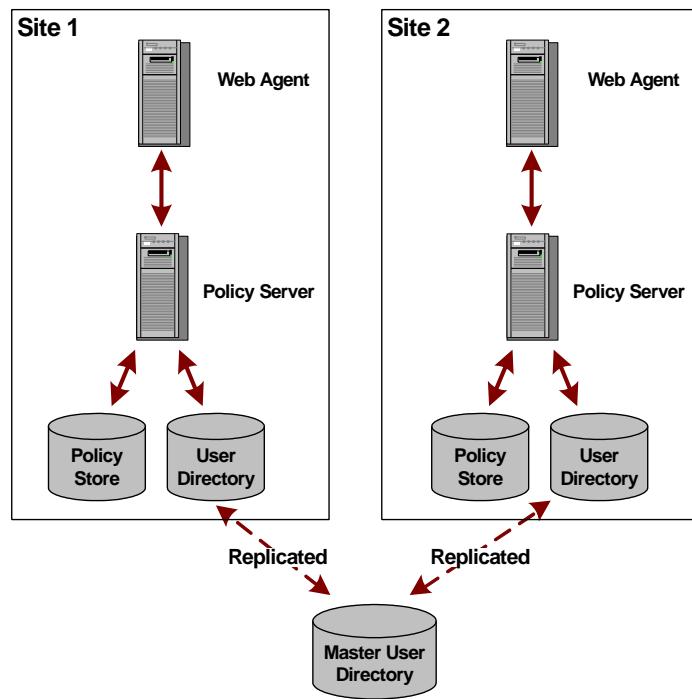


Use the procedures outlined in this guide to upgrade this environment.

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:

- [Migration Considerations](#) (see page 27)
- [How the r6.x Migration Works](#) (see page 31)
- [How to Migrate from r6.x](#) (see page 34)
- [How a Parallel Upgrade Works](#) (see page 66)
- [How to Configure a Parallel Environment](#) (see page 67)

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 up 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](#).

Crystal Reports in 12.x

The 12.52 Policy Server installer no longer includes the reports files (.rpt) that are compatible with Crystal Reports 9.0. CA SiteMinder® reports are now integrated with the 12.52 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 12.52 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 12.52 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

This release replaces the Policy Server User interface with the CA SiteMinder® Administrative UI.

By default, the Administrative UI:

- Uses the policy store as its source of administrator identities.
The default configuration lets you manage the environment immediately after installing the Administrative UI. Existing r6.x administrators stored in an external user store are not available to the Administrative UI.
- Only prompts for a user name and password. CA SiteMinder® does not protect the Administrative UI.

Configure an external administrator store connection to:

- Make the r6.x administrators available to the Administrative UI.
- Protect the Administrative UI with CA SiteMinder®.

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

Certificate Data Management

The certificate data store is replacing the CA SiteMinder® key database (smkeydatabase). If you have one or more smkeydatabases deployed in your environment, consider the following items:

- The certificate data store is collocated with the 12.52 policy store. A single certificate data store replaces the need for an individual smkeydatabase instance on each Policy Server host system.
- As part of a Policy Server upgrade, all smkeydatabase content is automatically backed up and migrated to the certificate data store.
- A 12.52 Policy Server can only communicate with a certificate data store. A 12.52 Policy Server and the respective local smkeydatabase do not operate in compatibility mode. However, all Policy Servers that have not been upgraded continue to communicate with their local version of the smkeydatabase.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

- Synchronize all smkeydatabase instances before beginning the migration. Synchronizing all instances helps avoid data collisions. Data collisions prevent a successful migration.
- All Policy Servers that share a common view into the same policy store have access to the same keys, certificates, and certificate revocation lists (CRL).
- The purpose of the certificate data store remains unchanged from the purpose of the smkeydatabase. This store makes the following available to the CA SiteMinder® environment:
 - Certificate authority (CA) certificates
 - Public and private keys
 - Certificate revocation lists

- You can continue to use the CA SiteMinder® key tool to manage the certificate data store. However, several options are deprecated.

Note: For more information, see the *Policy Server Release Notes*.

- If a CRL is stored in an LDAP directory service, consider the following items:
 - CA SiteMinder® no longer requires that the issuer of the CRL is the same CA that issued the corresponding root certificate.
 - CA SiteMinder® no longer performs this check. This behavior is consistent with the requirements for a text-based CRL.

More information:

[Synchronize Key Database Instances](#) (see page 47)

Federation Integration

This release replaces the Policy Server User Interface with the Administrative UI. If you were managing Federation Security Services, this functionality is referred to as legacy federation.

The Administrative UI also includes partnership federation. This functionality is specific to the partnership-based federation that CA SiteMinder® Federation makes available.

Single Sign-on

You can maintain single sign-on during the migration to 12.52. Consider the following:

- An 12.52 Policy Server can communicate with an r6.x policy store and an r6.x key store.
- An 12.52 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.

Advanced Password Services

If you have deployed Advanced Password Services, a Policy Server upgrade retains all LANG (translation), CFG (configuration), and mail files. The default 12.52 versions of the files are installed to *siteminder_home\samples*.

siteminder_home

Specifies the Policy Server installation path.

How the r6.x Migration Works

To upgrade a CA SiteMinder® deployment with multiple Policy Servers and Web Agents, remove one of the Policy Servers and Web Agents from the CA SiteMinder® environment. While these components are being upgraded, the remaining Policy Servers and Web Agents continue to protect your resources.

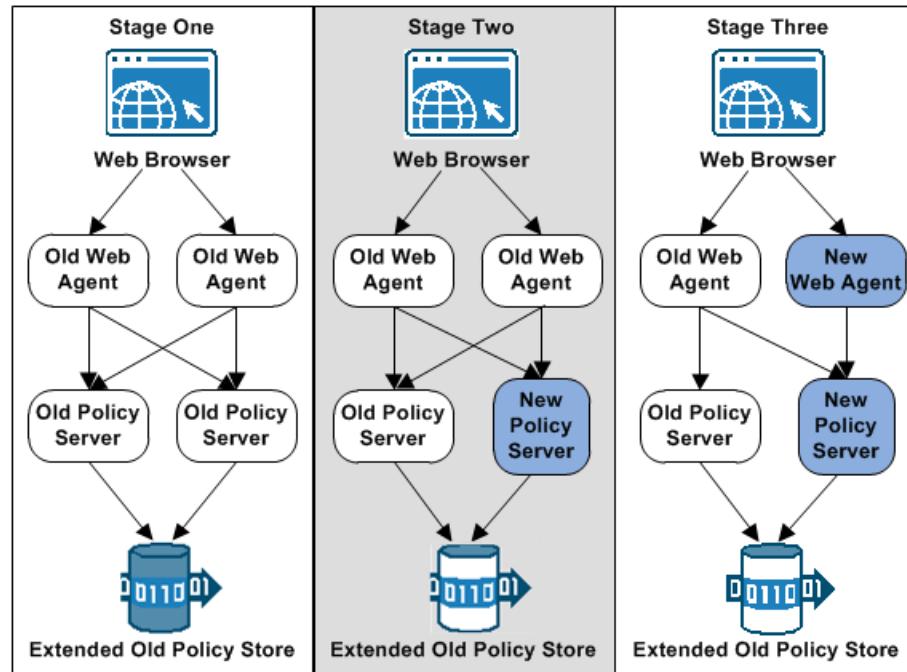
Continue removing and upgrading CA SiteMinder® components until all components are upgraded or operating in mixed-mode compatibility.

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 store. This policy store includes the key store. Your environment can use separate policy and key stores.

Figure 5: r6 SP5 migration. Stages 1 through 3



1. In stage one, the r6.x policy store schema is extended.

The existing r6.x policy store schema has not changed. The 12.52 migration requires that you extend the policy store schema for policy store for objects that 12.52 requires.

If you have deployed a smkeydatabase, extend the policy store schema before upgrading your first Policy Server. Extending the schema prepares the policy store for the smkeydatabase migration to the certificate data store during a Policy Server upgrade. Extending the schema does not affect compatibility mode. The policy store continues to function as it did in r6.x.

If you have not deployed a smkeydatabase, extend the schema as part of the policy store upgrade process.

2. In stage two, an r6.x Policy Server is upgraded to 12.52. The 12.52 Policy Server operates in compatibility mode. Consider the following items:

- The r6.x Web Agents continue to communicate with the 12.52 Policy Server.
- The 12.52 Policy Server continues to communicate with the r6.x policy and key store.
- The r6.x Policy Server continues to communicate with the r6.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.
- The Policy Server installer removes the Policy Server User Interface during the upgrade. The 12.52 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 12.52 Policy Server until the Administrative UI is installed.
- An 12.52 Policy Server can only communicate with an 12.52 certificate data store. If you are upgrading a legacy federation environment, the Policy Server installer attempts to migrate all existing smkeydatabase content to the certificate data store.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

3. In stage three, an r6.x Web Agent is upgraded to 12.52. Consider the following items:

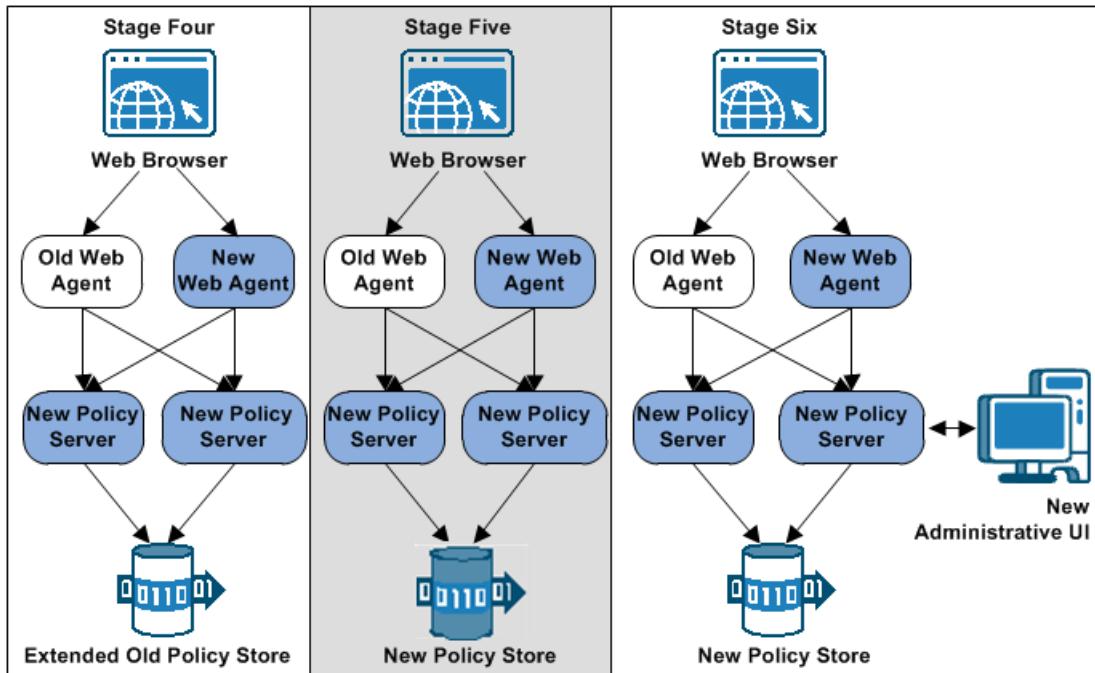
- The r6.x Web Agent continues to communicate with the r6.x and the 12.52 Policy Servers.
- The 12.52 Web Agent only communicates with the 12.52 Policy Server.

Note: You cannot configure a new 12.52 agent with an 12.52 Policy Server until the policy store is upgraded to 12.52.

4. In stage four, the remaining Policy Server is upgraded to 12.52. The 12.52 Policy Servers operate in compatibility mode with the r6.x policy and key store.

Important! Although all 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 removed the Policy Server User Interface during the upgrade. You cannot manage policy information in the policy store until you have installed the 12.52 Administrative UI. Account for this time as you plan your migration.

Figure 6: r6 SP^A Migration. Stages 4 through 6.



5. In stage five, the r6.x policy and key store is upgraded to 12.52.
6. In stage six, the Administrative UI is installed and registered with a Policy Server. Consider the following items:
 - 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.
7. (Optional) The final step, which is not illustrated, is to install and register a Report Server.

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

How to Migrate from r6.x

Follow these steps to complete a migration from r6.x to 12.52:

1. Review the installation and upgrade considerations in the *Policy Server Release Notes*.
2. Download the policy store schema files.
3. Extend the r6.x policy store schema.
4. If your environment includes multiple smkeydatabase instances, synchronize them. During a Policy Server upgrade, the installer tries to migrate all content in the smkeydatabase to the certificate data store.
5. Review the sections in *Before You Upgrade the Policy Server*.
6. Upgrade an r6.x Policy Server to 12.52.
7. Review *After You Upgrade the Policy Server*.
8. Upgrade an r6.x Web Agent to 12.52.
9. Upgrade the remaining r6.x Policy Servers and r6.x Web Agents to 12.52, respectively.
10. Upgrade the r6.x policy and key stores to 12.52.
11. Install the 12.52 Administrative UI.
12. (Optional) Install a Report Server.

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

Download the Policy Store Schema Files

The file or files that you require to extend the policy store schema are at the root of the Policy Server installation zip.

If you are upgrading to the base release of 12.52, follow these steps:

1. Log in to the [CA Support site](#).
2. Under Support, click Support by Product.
3. Type CA SiteMinder® in the Select a Product Page field and press Enter.
4. Under the Select a Product Page list, click Downloads.
5. Locate your specific CA SiteMinder® product in the Use the Select a Product list to locate your CA SiteMinder® product. Click the name.

6. Select a release and gen level, and click Go.
7. Save the Policy Server installation zip locally and extract the kit to a temporary location.

The policy store schema files are included in the policy_store_schema_ext.zip.

If you are upgrading to a cumulative release (cr) of 12.52, follow these steps:

1. Log in to the [CA Support site](#).
2. Under Support, click Support by Product.
3. Type CA SiteMinder® in the Select a Product Page field and press Enter.
4. Under the Select a Product Page list, click Recommended Reading.
5. Click CA SiteMinder® Hotfix/Cumulative Release Hot Index in the Recommend Reading list.
6. Click CA SiteMinder® Web Access Manager.
7. Click the cumulative release that you want.
8. Download the cumulative release.
9. Save the Policy Server installation zip locally and extract the kit to a temporary location.

The policy store schema files are included in the policy_store_schema_ext.zip.

Extend the Policy Store Schema

The existing r6.x policy store schema has not changed. The 12.52 migration requires that you extend the policy store schema for policy store for objects that 12.52 requires.

If you have deployed a smkeydatabase, extend the policy store schema before upgrading your first Policy Server. Extending the schema prepares the policy store for the smkeydatabase migration to the certificate data store during a Policy Server upgrade. Extending the schema does not affect compatibility mode. The policy store continues to function as it did in r6.x.

If you have not deployed a smkeydatabase, extend the schema as part of the policy store upgrade process.

Extend the Policy Store Schema for Your Active Directory Server

Follow these steps:

1. Copy the following ZIP file to a Policy Server host system and extract it to a temporary location:
`policy_store_schema_ext.zip`
2. Navigate to the following directory:
`schema_extension\db\Active Directory`
3. Open the ActiveDirectory.ldif file and manually replace each instance of <RootDN> with the DN (domain name) that represents the policy store schema location. Do not use the policy store object location.

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

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

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

`dc=domain,dc=com`

4. Save the file.
5. Navigate to *siteminder_home/bin* from a command window.

siteminder_home

Specifies the Policy Server installation path.

6. Run the following command:

`sldapsetup_ldmod -fpath/ActiveDirectory.ldif`
path

Specifies the path to the schema file.

The policy store schema is extended.

Extend Policy Store Schema for Your Active Directory LDS Server

Follow these steps:

1. Copy the following ZIP file to a Policy Server host system and extract it to a temporary location:
`policy_store_schema_ext.zip`
2. Navigate to the following directory:
`schema_extension\db\Active Directory LDS`
3. Open the ADLDS.ldif file and replace each instance of {guid} with the actual value of guid in the braces.

Example: {CF151EA3-53A0-44A4-B4AC-DAOEBB1FF200}

4. Save the file.
5. Navigate to *siteminder_home/bin* from a command window.

siteminder_home

Specifies the Policy Server installation path

6. Run the following command:

`smldapsetup ldmod -fpath/ADLDS.ldif`

path

Specifies the path to the schema file.

The policy store schema is extended.

Extend Policy Store Schema for Your CA Directory Server

Follow these steps:

1. Copy the following ZIP file to the CA Directory host system and extract it to a temporary location:

`policy_store_schema_ext.zip`

2. Navigate to the following directory:

`schema_extension\db\CA Directory`

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

`etrust.dxc`

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

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

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

■ **r12**

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

Note: The DXI file is located in DXHOME\config\servers. The max-cache-size entry is the total cache size in MB. Adjust this value according to the total memory available on the CA Directory server and overall size of the policy store.

■ **r12 SP1 or later**

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

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

```
# 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 = 2000;
```

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

7. Edit the settings to match the following settings 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 = 4000;
set multi-write-queue = 20000;
```

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

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

8. Use JXplorer to access the policy store DSA.
9. Locate the root element, and then locate the following base tree structure:
Netegrity, SiteMinder, PolicySvr4
10. Create an organizational unit (root element) under PolicySvr4 that is named:
XPS
11. Stop and restart the DSA (as the DSA user) with 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.

Extend the Policy Store Schema for Your IBM DB2 Server

Follow these steps:

1. Copy the following ZIP file to the IBM DB2 host system and extract it to a temporary location:

`policy_store_schema_ext.zip`

2. Navigate to the following directory:

`schema_extension\db\IBM DB2`

3. Locate the following file:

`DB2.sql`

4. Open a command prompt and run the following command:
`db2 -td@ [-v] -f path\DB2.sql`

path

Specifies the path to the DB2 schema file.

The policy store schema is extended.

Extend the Policy Store Schema for Your IBM Tivoli Directory Server

Follow these steps:

1. Use the IBM Tivoli Directory Server administration tool to update the policy store base tree structure. Create the following root node under `ou=Netegrity,ou=SiteMinder,ou=PolicySrv4`:

`ou=XPS`

2. Copy the following ZIP file to the IBM Directory Server host system and extract it to a temporary location:

`policy_store_schema_ext.zip`

3. Navigate to the following directory:

`schema_extension\db\IBM Tivoli Directory Server`

4. Locate the following file:

`IBMDirectoryServer.ldif`

5. Use the IBM Directory Server Configuration Tool to add the following file to the Manage Schema Files section of the schema configuration:

`IBMDirectoryServer.ldif`

6. Restart the directory server.

The policy store schema is extended.

Extend the Policy Store Schema for Your Novell eDirectory Server

Follow these steps:

1. Copy the following ZIP file to a Policy Server host system and extract it to a temporary location:

`policy_store_schema_ext.zip`

2. Navigate to the following directory:

`schema_extension\db\Novell eDirectory`

3. Locate and open the following file:

`Novell.ldif`

4. Navigate to `siteminder_home\bin` from a command window.

`siteminder_home`

Specifies the Policy Server installation path.

5. Run the following command:

```
ldapsearch -hhost -pport -bcontainer -ssub -DAdminDN -wAdminPW  
objectclass=ncpServer dn
```

Example:

```
ldapsearch -h192.168.1.47 -p389 -b=ncpServer -ssub  
-Dcn=admin,o=ncpServer -wpassword objectclass=ncpServer dn
```

The Novell server DN opens.

6. Edit the open schema file. Replace every `<ncpserver>` variable with the value of the Novell server DN (domain name).

Example: If your Novell server DN value is `cn=servername,o=servercontainer`, replace all instances of `<ncpserver>` with the following value:

`cn=servername,o=servercontainer`

7. Save and close the schema file.

8. Run the following command:

```
sldapsetup ldmod -fpath\Novell.ldif  
-fpath
```

Specifies the path to the schema file.

The policy store schema is extended.

Extend the Policy Store Schema for Your OpenLDAP Server

Follow these steps:

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

1. Update the policy store base tree structure. Create the following root node under ou=Netegrity,ou=SiteMinder,ou=PolicySrv4:


```
ou=XPS
```
2. Copy the following ZIP file to the OpenLDAP host system and extract it to a temporary location:


```
policy_store_schema_ext.zip
```
3. Navigate to the following directory:


```
schema_extension\db\OpenLDAP
```
4. Locate the following schema files:


```
openldap_attribute_XPS.schema
openldap_object_XPS.schema
```
5. Copy the schema files located in Step 4 to the schema folder in the OpenLDAP installation directory.
6. Type the following entry in the include section of the slapd configuration file:

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

The policy store schema is extended.

Extend the Policy Store Schema for Your Oracle Internet Directory Server

Follow these steps:

1. Log in to the Oracle Internet Directory host system.
2. Use the Oracle catalog command line tool to index the following attribute. Indexing the attribute prevents an error from occurring when you import the default policy store objects:

```
modifyTimestamp
```

Run the following command:

```
oracle_home/ldap/bin/catalog connect=conn_str add=TRUE
attribute=modifyTimestamp
```

oracle_home

Specifies the Oracle Internet Directory installation path.

conn_str

Specifies the directory database connect string. If you have configured a tnsnames.ora file, then enter the net service name specified in the file.

Note: For more information about the catalog command line tool, see the Oracle documentation.

3. Copy the following ZIP file to a Policy Server host system and extract it to a temporary location:

`policy_store_schema_ext.zip`

4. Navigate to the following directory:

`schema_extension\db\Oracle Internet Directory`

5. Locate the following file:

`OID_10g.ldif`

6. Navigate to `siteminder_home\bin` from a command window.

siteminder_home

Specifies the Policy Server installation path.

7. Run the following command:

```
ldapmodify -hhost -pport -dAdminDN -wAdminPW  
-c -fpath\OID_10g.ldif  
-Z -Pcert
```

-hhost

Specifies the IP address of the LDAP directory server.

Example: 123.123.12.12

-pport

Specifies the port number of the LDAP directory server.

Example: 3500

-dAdminDN

Specifies the name of the LDAP user who has the privileges to create the LDAP schema.

-wAdminPW

Specifies the password of the administrator that the ***-d*** option specifies.

-c

Specifies continuous mode (do not stop on errors).

-fpath

Specifies the path to the extracted schema file.

-Z

Specifies a connection that is encrypted by SSL.

-Pcert

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

Example:

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

-Papp/siteminder/ssl

The policy store schema is extended.

Extend the Policy Store Schema for Your Red Hat Directory Server

Follow these steps:

1. Copy the following ZIP file to a Policy Server host system and extract it to a temporary location:

`policy_store_schema_ext.zip`

2. Navigate to the following directory:

`schema_extension\db\Red Hat Directory Server`

3. Locate the following file:

`RedHat_7_1.ldif`

4. Navigate to `siteminder_home/bin` from a command window.

`siteminder_home`

Specifies the Policy Server installation path.

5. Run the following command:

`smldapsetup ldmod -fpath/RedHat_7_1.ldif`

`path`

Specifies the path to the extracted schema file.

The policy store schema is extended.

Extend the Policy Store Schema for Your Siemens DirX Server

Follow these steps:

1. Use the DirXmanage tool to update the policy store base tree structure. Under the existing root path:

ou=Netegrity,ou=SiteMinder,ou=PolicySvr4

Create the following root node:

ou=XPS

2. Copy the ZIP file, policy_store_schema_ext.zip, to the Siemens DirX host system and extract it to a temporary location.

3. Navigate to the following directory:

schema_extension\db\Siemens DirX

4. Locate the following extracted files and copy them to *DirX_install_path\scripts\security\Netegrity\SiteMinder*:

- bind.tcl
- GlobalVar.tcl
- l-bind.cp
- schema_ext_for_XPS.adm

DirX_install_path

Specifies the DirX installation path.

Example: C:\program files\siemens\dirx

5. Locate the extracted file dixxabbr-ext.XPS and copy it to *DirX_install_path\client\conf*.

6. Stop and restart the DirX service.

7. Edit the GlobalVar.tcl file to update the global variables that the DirX scripts reference.

Default values:

- LDAP port: 389
- Root DN: o=pqr
- Admin username: cn=admin,o=pqr
- Admin password: dirx

Note: Correct the values so they apply to your existing setup.

8. Navigate to *DirX_install_path\scripts\security\CA\SiteMinder*.

9. Execute the following command:

```
dirxadm schema_ext_for_XPS.adm
```

10. Use the DirXmanage utility to rebind to the DSA.

Note: Watch for errors.

The policy store schema is extended.

Extend the Policy Store Schema for Your Sun Java System Directory Server

Follow these steps:

1. Copy the following ZIP file to a Policy Server host system and extract it to a temporary location:

```
policy_store_schema_ext.zip
```

2. Navigate to the following directory:

```
schema_extension\db\Sun Java System Directory Server
```

3. Locate the following file:

```
OracleDirectoryServer.ldif
```

4. Navigate to *siteminder_home\bin* from a command window.

siteminder_home

Specifies the Policy Server installation path.

5. Run the following command:

```
smldapsetup ldmod -fpath\OracleDirectoryServer.ldif
```

-fpath

Specifies the path to the extracted schema file.

The policy store schema is extended.

Extend the Policy Store Schema for Your Microsoft SQL Server

Follow these steps:

1. Copy the following ZIP file to the SQL Server host system and extract it to a temporary location:

```
policy_store_schema_ext.zip
```

2. Navigate to the following directory:

```
schema_extension\db\Microsoft SQL Server
```

3. Locate the following file:

```
SQLServer.sql
```

4. Log in to SQL Server as the user who administers the policy store database.
5. Start the Query Analyzer.
6. Select the policy store database instance from the database list.
7. Open the file in a text editor and copy the contents of the entire file.
8. Paste the schema into the query and execute the query.

The policy store schema is extended.

Extend the Policy Store Schema for Your MySQL Server

Follow these steps:

1. Copy the following ZIP file to the MySQL host system and extract it to a temporary location:
`policy_store_schema_ext.zip`
2. Navigate to the following directory:
`schema_extension\db\MySQL`
3. Locate the following file:
`MySQL.sql`
4. Open the file in a text editor and copy the contents of the entire file.
5. Paste the file contents into a query.
6. Use the MySQL command line tool to execute the query.

The policy store schema is extended.

Extend the Policy Store Schema for Your Oracle Server

Follow these steps:

1. Copy the following zip file to the Oracle host system and extract it to a temporary location:
`policy_store_schema_ext.zip`
2. Navigate to the following directory:
`schema_extension\db\Oracle`
3. Locate the following file:
`Oracle.sql`
4. Log in to the Oracle server with sqlplus or another Oracle utility as the user who administers the policy store database.

Note: We recommend that you do not create the CA SiteMinder® schema with the SYS or SYSTEM users. If necessary, create an Oracle user, such as SMOWNER, and create the schema with that user.

5. Import the file into the r6.x database instance.

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

The policy store schema is extended.

Synchronize Key Database Instances

Synchronize all smkeydatabase instances before beginning the migration to a new version.

Note: Use the smkeytool utility to synchronize the smkeydatabases and resolve all data inconsistencies between smkeydatabase instances. For more information about the smkeytool utility, see the *Policy Server Administration Guide*.

Previous versions of CA SiteMinder® used a local smkeydatabase to store certificate data. Each Policy Server required its own smkeydatabase. For version 12.52, a centralized certificate data store replaces the local smkeydatabases.

As part of a Policy Server upgrade, the installer automatically backs up the local smkeydatabase and tries to migrate all content to the certificate data store. This process includes a comparison of both stores before starting the migration.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

Use the following guidelines to identify and resolve data inconsistencies among your smkeydatabases:

- Verify that each certificate-authority certificate references certificate revocation lists consistently across instances.
Example: A certificate-authority certificate consistently references certificate revocation lists in an LDAP directory service.
- Verify that the defaultenterpriseprivatekey alias represents the same private key/certificate pair in all instances.
- Verify that the same alias maps to the same certificate or key/certificate pair.
- Verify that the same certificate-authority certificates map to the same certificate revocation lists.
- Verify that a revoked or expired certificate is not present.
- Verify that all CRL information is valid.

Important! After you resolve all data inconsistencies, we recommended that you do not modify a smkeydatabase until all migrations are complete.

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 items before you upgrade a Policy Server:

- If the environment contains multiple smkeydatabase instances, be sure to synchronize all content. Synchronizing resolves data inconsistencies that can prevent the Policy Server installer from migrating content to the certificate data store.
- You upgrade the Policy Server using the installation media on the Technical Support site.
Note: For a list of installation media names, see the *Policy Server Release Notes*.
- (Linux) Be sure that the required Linux libraries are installed to the Policy Server host system. For more information, see Required Linux Libraries.
- 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 Policy Server Management Console instances.
- During the upgrade, leave the policy store check box on the configuration wizard cleared to preserve your existing policy store. However, the configuration wizard prompts you for the encryption key for the advanced authentication server. This key is stored on each Policy Server, but all Policy Servers require the same key.
- (UNIX) The user account upgrading the Policy Server must have executable permissions on the directory that contains the installation media. If the user account does not have these permissions, run the following command:

```
chmod +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.
- The CA SiteMinder® documentation is not installed with the Policy Server. We recommend that you locate the documentation before you upgrade.

More information:

[Synchronize Key Database Instances](#) (see page 47)

Required Linux Libraries

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

`java.lang.UnsatisfiedLinkError`

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

Red Hat 5.x:

`compat-gcc-34-c++-3.4.6-patch_version.i386`

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

Red Hat 6.x:

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

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

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

libXau-1.0.5-1.el6.i686.rpm

libxcb-1.5-1.el6.i686.rpm

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

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

libX11-1.3-2.el6.i686.rpm

libXrender-0.9.5-1.el6.i686.rpm

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

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

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

libICE-1.0.6-1.el6.i686.rpm

libuuid-2.17.2-12.7.el6.i686.rpm

libSM-1.1.0-7.1.el6.i686.rpm

libXext-1.1-3.el6.i686.rpm

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

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

libXi-1.3-3.el6.i686.rpm

libXtst-1.0.99.2-3.el6.i686.rpm

libXft-2.1.13-4.1.el6.i686.rpm

libXt-1.0.7-1.el6.i686.rpm

libXp-1.0.0-15.1.el6.i686.rpm

Korn Shell (ksh) Package Required on Linux

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

Red Hat 5.x 32-bit

ksh-20100621-12.el5.i386.rpm

Red Hat 5.x 64-bit

ksh-20100621-12.el5.x86_64.rpm

Red Hat 6.x 32-bit

ksh-20100621-16.el6.i686.rpm

Red Hat 6.x 64-bit

ksh-20100621-16.el6.x86_64.rpm

Windows

Follow these steps:

1. Review Before You Upgrade.
2. Exit all applications that are running.
3. Stop the Policy Server that you want to upgrade.
4. 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, see the *Policy Server Release Notes*.

5. Considering the following items when running the installer:
 - The installer prompts you to select CA SiteMinder® components. When selecting components:
 - Reconfigure any components that had been previously configured for the environment. Be sure to select the respective components.
 - During the upgrade, leave the policy store check box on the configuration wizard cleared to preserve your existing policy store. You manually upgrade an existing policy store. However, the configuration wizard prompts you for the encryption key for the advanced authentication server. This key is stored on each Policy Server, but all Policy Servers require the same key.
 - If you are upgrading another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.

If the installer detects a smkeydatabase, it:

- Backs up the smkeydatabase.
- Attempts to migrate the content to the certificate data store.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

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

1. Review the installation settings and click Install.

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

2. Enable the [advanced authentication server](#) (see page 55) for the Policy Server that you are upgrading.

More information:

[Troubleshoot a Policy Server Upgrade](#) (see page 57)

UNIX GUI

Follow these steps:

1. Review Before You Upgrade.
2. Exit all applications that are running.
3. Stop the Policy Server that you want to upgrade.
4. Execute the following script in a ksh shell from the CA SiteMinder® installation directory:

`./ca_ps_env.ksh`

Note: Be sure that there is a space between the periods.

5. Open a shell and navigate to the installation executable.
6. Enter the following command:

`./installation_media`

installation_media

Specifies the Policy Server installation executable.

The Policy Server installer starts.

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

7. Considering the following items when running the installer:

- The installer prompts you to select CA SiteMinder® components. When selecting components:
 - Reconfigure components that had been previously configured for the environment. Be sure to select the respective components.
 - During the upgrade, leave the policy store check box on the configuration wizard cleared to preserve your existing policy store. You manually upgrade an existing policy store. However, the configuration wizard prompts you for the encryption key for the advanced authentication server. This key is stored on each Policy Server, but all Policy Servers require the same key.
 - If you are upgrading another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
- If the installer detects a smkeydatabase, it:
 - Backs up the smkeydatabase.
 - Attempts to migrate the content to the certificate data store.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

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

8. 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.

9. Click Done.

10. Execute the following script in a ksh shell from the CA SiteMinder® installation directory:

```
./ca_ps_env.ksh
```

Note: Be sure that there is a space between the periods.

11. Enable the [advanced authentication server](#) (see page 55) for the Policy Server that you are upgrading.

More information:

[Troubleshoot a Policy Server Upgrade](#) (see page 57)

UNIX Console

Follow these steps:

1. Review Before You Upgrade.
2. Exit all applications that are running.
3. Stop the Policy Server that you want to upgrade.
4. Execute the following script in a ksh shell from the CA SiteMinder® installation directory:

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

Note: Be sure that there is a space between the periods.

5. Open a shell and navigate to the installation executable.
6. 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, see the *Policy Server Release Notes*.

7. Considering the following items when running the installer:
 - The installer prompts you to select CA SiteMinder® components. Each component is prefixed with a number. Type numbers that are 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.
 - During the upgrade, leave the policy store check box on the configuration wizard cleared to preserve your existing policy store. You manually upgrade an existing policy store. However, the configuration wizard prompts you for the encryption key for the advanced authentication server. This key is stored on each Policy Server, but all Policy Servers require the same key.
 - If you are upgrading another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.

- If the installer detects a smkeydatabase, it:
 - Backs up the smkeydatabase.
 - Attempts to migrate the content to the certificate data store.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

8. 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.

9. Press Enter.

10. Click Done.

11. Execute the following script in a ksh shell from the CA SiteMinder® installation directory:

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

Note: Be sure that there is a space between the periods.

12. Enable the [advanced authentication server](#) (see page 55) for the Policy Server that you are upgrading.

More information:

[Troubleshoot a Policy Server Upgrade](#) (see page 57)

Enable the Advanced Authentication Server

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

Follow these steps:

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

The master key screen appears.

4. Create the master encryption key for the advanced authentication server.

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

5. Complete the rest of the Policy Server configuration wizard.

The advanced authentication server is enabled.

Policy Server Upgrade Creates New Files

During a Policy Server upgrade, the installer creates new versions of certain files for 12.52. The installer creates the following files in the *policy_server_home/config* directory:

- conapi.conf
- JVMOptions.txt
- profiler_templates
- siteminder.conf
- SMocsp.sample.conf
- SmSWEC.cfg
- smtracedefault.txt
- snmp.conf
- snmptrap.conf
- trace.conf

The installer creates the following files in the *policy_server_home/properties* directory:

- AMAssertionGenerator.properties
- AssertionGeneratorFramework.properties
- cdslog4j.properties
- EntitlementGenerator.properties
- FederationAttributeConfig.properties
- InfoCard.properties
- JSAMLAffirmationStrings.properties
- JSAMLPacketStrings.properties
- log4j.properties
- LoggerConfig.properties
- logging.properties
- openformatexpression.conf
- scriptActiveExpConfig.properties
- smkeydatabase.properties
- WebServiceConfig.properties
- xsw.properties

These 12.52 files use the .new extension: For example, the JVMOptions.txt file from the previous version remains untouched. The installer creates an 12.52 version of the JVMOptions.txt file that is named JVMOptions.new.

If the original file included customized settings, be sure to modify the .new file with your customized settings. Rename the .new file with the extension from the original file.

For example, if you had custom settings in your JVMOptions.txt file, copy those changes to JVMOptions.txt.new. Rename the JVMOptions.txt.new to JVMOptions.txt.

Custom Server-Side Code Requirements

Your Policy Server operating system determines whether recompiling custom server-side code is required. Use the following table to identify the requirement:

Operating System	Required?
Microsoft Windows and UNIX	No. Recompiling the custom code is optional.
Red Hat Linux	Yes. Upgrade the SDK and recompile the custom code using GCC 3.4.

Troubleshoot a Policy Server Upgrade

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.
- You can locate the smkeydatabase migration log (smkeydatabaseMigration.log) in *siteminder_home\log*.
Note: A Policy Server upgrade and a smkeydatabase migration are separate processes. If the smkeydatabase migration fails, the Policy Server upgrade does not fail.

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*.

Upgrade an r6.x Web Agent

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

CA SiteMinder® r6.x Web Agents can communicate with an 12.52 Policy Server. Therefore, you upgrade a Policy Server to 12.52 before upgrading a Web Agent to 12.52.

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 CA 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 12.52 web agent installer to upgrade an r6.x web agent. Consider the following items:

- Agents that require option pack functionality must be upgraded to 12.52 before installing the 12.52 Web Agent Option Pack.

Note: For more information about upgrading a web agent, see the *Web Agent Installation Guide*. For more information about installing the 12.52 Web Agent Option Pack, see the *Web Agent Option Pack Guide*.

- If you have deployed Advanced Password Services, a web agent upgrade retains all LANG (translation) and CFG (configuration) files. The default 12.52 versions of the files are installed to *agent_home\samples*.

agent_home

Specifies the web agent installation path.

- If you used a startup script for r6, replace all instances of “*nete_wa...*” with “*ca_wa...*”

Custom Agent Requirements

To determine if you are required to recompile your custom agent, use the following table:

Agent Type	Required?
CA SiteMinder® agent	Operating system-specific. If the agent operating system has reached end-of-life, you must recompile the custom agent. Upgrade the CA SiteMinder® SDK and recompile the agent on a supported operating system.
Third-party agent	Vendor-specific. Contact your third-party vendor to determine whether the agent is supported.

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 12.52.

Options for Upgrading a Policy Store

Two paths exist for upgrading an r6.x policy store to 12.52. You can:

- Upgrade the existing policy and key store to 12.52.
- Create an 12.52 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 migrate an existing policy store to a 12.52 policy and key store, follow these steps:

1. Export the policy and key store data using the r6.x version of smobjexport.
Note: For more information, see the *Policy Server Installation Guide* for r6.x.
2. Create an 12.52 policy and key store.
Note: For more information, see the *Policy Server Installation Guide*.
3. Import the policy and key store data into the 12.52 policy and key store using the 12.52 version of smobjimport.
Note: For more information, see the *Policy Server Administration Guide*.

Options for Upgrading a Key Store

Two paths exist for upgrading an r6.x key store to 12.52. You can:

- Upgrade the existing policy and key store to 12.52.
- Create a stand-alone 12.52 key store and import the existing agent keys in to the new instance.

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

If you want to create a stand-alone 12.52 key store:

1. Use the r6.x version of smobjexport to export only the agent keys that are stored in the policy store.
Note: For more information, see the *r6.x Policy Server Installation Guide*.
2. Create an 12.52 key store using the default policy store schema.
Note: For more information, see the *Policy Server Installation Guide*.
3. Use the 12.52 version of smobjimport to import the agent keys in to the 12.52 key store.
Note: For more information, see the *Policy Server Administration Guide*.
4. Use the Policy Server Management Console to point the Policy Server to the stand-alone key store.
Note: For more information, see the *Policy Server Management Console Help*.

How to Upgrade an r6.x Policy Store

To upgrade an r6.x policy store to 12.52, complete the following procedures:

1. Stop all Policy Servers that are communicating with the policy store.
2. If you have not extended the policy store schema to facilitate a smkeydatabase migration during a Policy Server upgrade, extend the schema.
3. Import the policy store data definitions.
4. Import the default policy store objects.
- Note:** If you are upgrading a legacy federation environment, there is no change to the Policy Server Option Pack (PSOP) schema.
5. If you managed your r6.x legacy federation environment using the FSS Administrative UI, run the XPS sweeper utility to complete the migration of your legacy federation objects.
6. Start all Policy Servers that are communicating with the policy store.

Stop all Policy Servers

Stopping all of the Policy Servers that are communicating with the policy store helps to prevent policy store corruption during the upgrade.

Follow these steps:

1. Log in to the Policy Server host system.
2. Complete one of the following steps:
 - (Windows)
 - a. Open the Policy Server Management Console and click Stop.
 - b. Click OK to close the console.
 - (UNIX) Use the following supplied script:
install_path/siteminder/stop-all

install_path
Specifies the Policy Server installation path.
3. Repeat this procedure for each Policy Server that is communicating with the policy store.

Import the Policy Store Data Definitions

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

Follow these steps:

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

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

XPSDDInstall SmMaster.xdd

XPSDDInstall
Imports the required data definitions.

Import the Default Policy Store Objects

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

The default policy store objects exist in the following XML files:

- smpolicy.xml
- smpolicy-secure.xml

The smpolicy-secure.xml file provides more restrictive security settings than the smpolicy.xml file. Pick only *one* of the previous files to import the default policy store objects.

Either file configures a new policy store and upgrades an existing store. When imported as part of an upgrade, the file does *not* overwrite existing default objects that were modified. These objects include the default security settings in the default Agent Configuration Object (ACO) templates.

Importing either file makes legacy federation and Web Service Variables functionality available. These features are separately licensed. If you intend to use the Web Service Variables functionality, contact your CA account representative for licensing information.

Follow these steps:

1. Open a command line window and navigate to *siteminder_home*\db.
2. Import *one* of the following files:

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

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

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

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

-npass

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

The policy store objects are imported.

Make the legacy federation Objects Available in the Administrative UI

If you manage your Federation Security Services (legacy federation) objects using the Policy Server UI, run the XPS sweeper utility to migrate these objects to the Administrative UI.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to make your legacy federation objects available to the Administrative UI:

`XPSSweeper`

All legacy federation created using the Policy Server UI are available in the Administrative UI.

You are ready to proceed to the next stage of the upgrade process, upgrading your Administrative UI.

Start all Policy Servers

Starting all Policy Servers resumes communication between all of the Policy Servers and the upgraded policy store.

Follow these steps:

1. Log in to the Policy Server host system.
2. Complete one of the following steps:
 - (Windows)
 - a. Open the Policy Server Management Console and click Start.
 - b. Click OK to close the console.
 - (UNIX) Use the following supplied script:
`install_path/siteminder/start-all`
`install_path`
Specifies the Policy Server installation path.
3. Repeat this procedure for each Policy Server that is communicating with the policy store.

The policy store is upgraded.

Install the Administrative User Interface

Unlike previous versions of CA SiteMinder®, the Policy Server User Interface is not installed with the Policy Server. Rather, you are required to install the 12.52 Administrative UI separately.

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

Upgrade an r6.x Session Store

A session store upgrade is not required. The 12.52 session store schema has not changed from r6.0 SP5.

Upgrade an r6.x Audit Log Database

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

Note: For more information about the iRecorder for CA 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 CA SiteMinder® with SCC.

policy_server_home

Specifies the Policy Server installation path.

Note: The CA 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 CA SiteMinder® audit log database:

sm_mssql_logs_eaudit_upgrade.sql

Upgrades a SQL Server audit log database from r6.x to 12.52.

sm_oracle_logs_eaudit_upgrade.sql

Upgrades an Oracle audit log database from r6.x to 12.52.

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

How a Parallel Upgrade Works

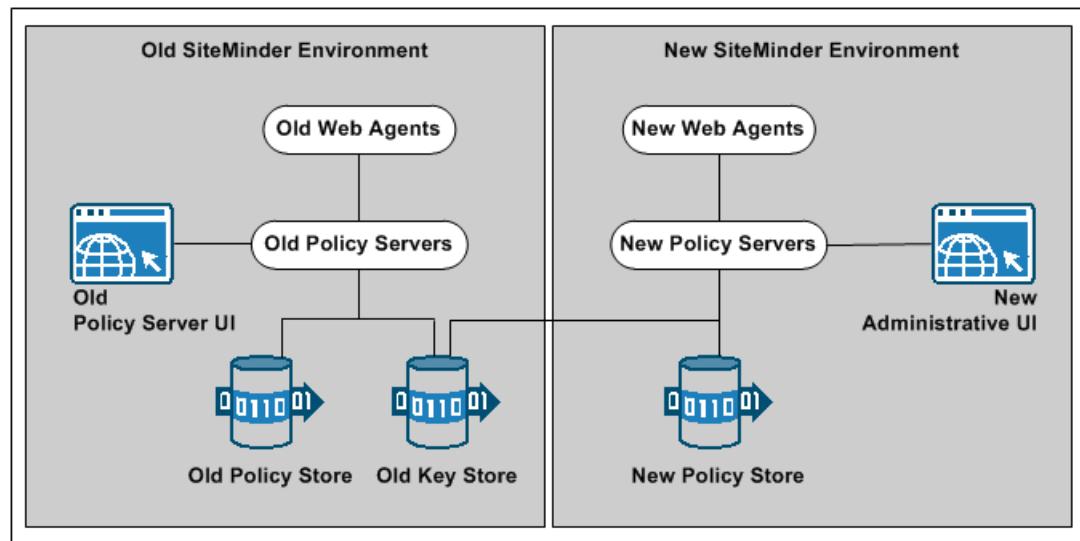
You do not have to migrate an existing r6.x environment to 12.52. Rather, you can configure a parallel 12.52 environment with an existing deployment.

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 CA SiteMinder® objects in the r6.x policy store.
- An 12.52 environment that protects new resources.
- An 12.52 Administrative UI that is used to manage CA SiteMinder® objects in the 12.52 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.

Figure 7: r6.x parallel upgrade overview



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 12.52 environment.
3. Complete one of the following steps:
 - 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. If your r6.x environment contains smkeydatabases:
 - a. Synchronize all instances.
 - b. Migrate the content of a smkeydatabase to the 12.52 certificate data store.
5. If you are managing legacy federation (Federation Security Services) objects in your r6.x environment, migrate the assertion issuer ID.
6. (Optional) Migrate the r6.x policy store data.
7. Review the user directory single sign-on requirements.

More information:

[Certificate Data Management](#) (see page 29)

[Synchronize Key Database Instances](#) (see page 47)

Parallel Environment Key Management Options

Managing CA SiteMinder® keys to maintain single sign-on between the existing environment and 12.52 environment is critical to a successful parallel upgrade. Two CA 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.
- 12.52 Policy Servers connecting to an 12.52 policy store.
- A common r6.x key store maintaining key data for all Policy Servers. The common key store lets agents that are 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.

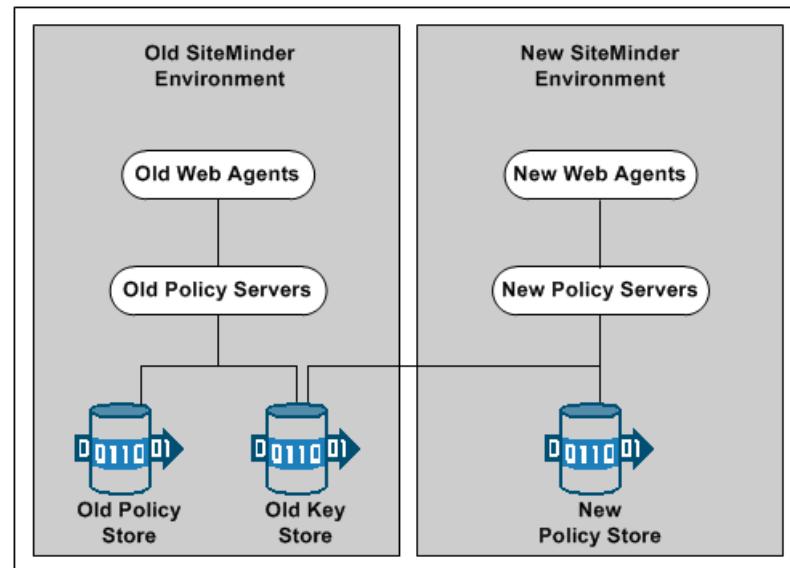
- All Policy Servers connecting to a common key store to retrieve new keys.

Important! The 12.52 Policy Servers must be configured with the r6.x key store. r6.x Policy Servers cannot communicate with an 12.52 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.

Figure 8: r6.x common key store deployment



Multiple Key Store Deployment

Existing r6.x Policy Servers can use an r6.x key store for key rollover, while 12.52 Policy Servers can use an 12.52 key store for key rollover. The following figure illustrates:

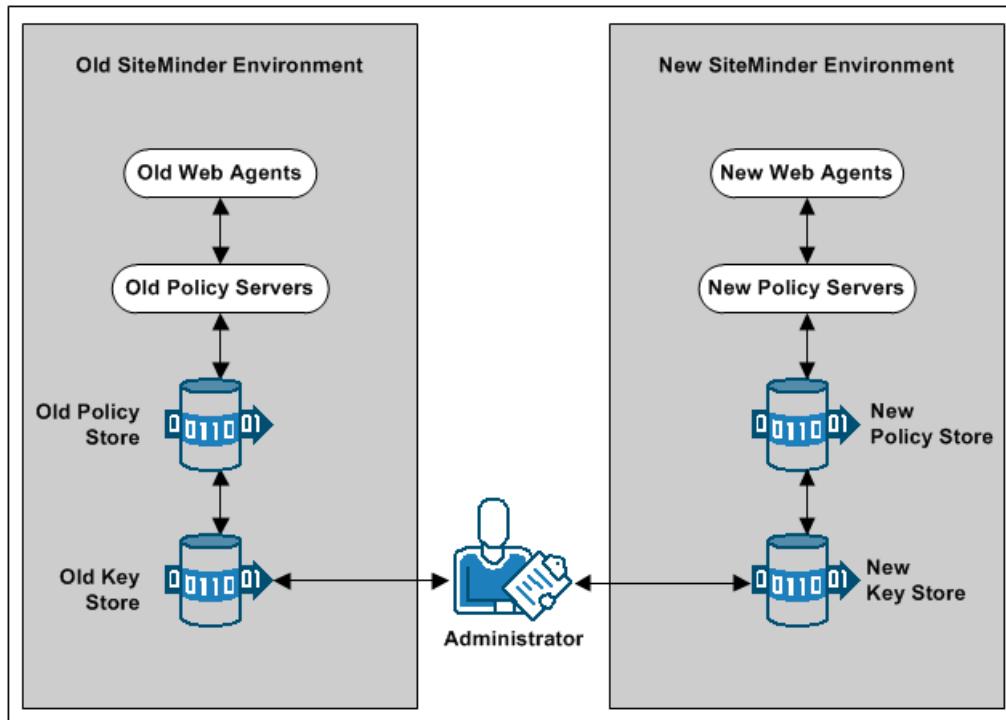
- r6.x Policy Servers connecting to an r6.x policy store.
- 12.52 Policy Servers connecting to an 12.52 policy store.
- r6.x Policy Servers connecting to an r6.x key store to retrieve new keys.
- 12.52 Policy Servers connecting to an 12.52 key store to retrieve new keys.
- A CA SiteMinder® administrator 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.
- 12.52 Web Agents polling their respective 12.52 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.

Figure 9: r6.x multiple key store deployment



Create the 12.52 Environment

You can configure an 12.52 environment independently of the existing environment. Install and configure the 12.52 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 12.52 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:
 - If the r6.x environment is configured with a separate key store, leave the key store version at r6.x. 12.52 Policy Servers can communicate with an r6.x key store, but r6.x Policy Servers cannot communicate with an 12.52 key store.
 - If the r6.x environment is configured with a collocated policy/key store, separate the r6.x keys in to a separate r6.x 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 12.52 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*.

How to Separate a Key Store from a Policy Store

Complete the following procedures to separate the key store from the policy store:

1. Install or locate a set-up Policy Server. A set-up Policy Server is a Policy Server that is not configured with the collocated policy/key store.
 - If a Policy Server is configured with the collocated store, you cannot use it to configure the new key store instance. The required CA SiteMinder® utilities available on the Policy Server host system are configured to manage the collocated store.
 - The set-up Policy Server makes available a separate set of the required utilities. The separate set lets you configure the key store without interfering with the collocated store.

2. Use the set-up Policy Server host system to create a separate r6.x key store instance. Consider the following items:
 - The key store only requires the default policy store schema. For more information about importing the default policy store schema, see the *r6.x Policy Server Installation Guide*.
 - The key store does not require that you:
 - Set the CA SiteMinder® superuser password.
 - Import the default policy store objects.
3. Disable dynamic agent key generation in the r6.x environment.

Note: If your environment uses static keys, this step is not required. However, be sure that a CA SiteMinder® administrator does not generate a random agent key after you export the keys from the policy store.
4. Export the agent keys from the r6.x policy/key store.
5. Import the agent keys in to the r6.x key store.
6. Configure all Policy Servers to use the separate key store.
7. If you disabled dynamic agent key generation, re-enable it.

Disable Dynamic Agent Key Generation

Before the key store separation is complete, the r6.x environment is operating with two key stores:

- Some Policy Servers use the agents keys in the collocated policy/key store.
- Some Policy Servers use the agent keys in the separate key store.

Disabling dynamic agent key generation prevents a Policy Server from generating keys after you export them for the separate store. Stopping the Policy Server from generating keys prevents single sign-on issues that can occur when the keys are not synchronized in all stores.

Follow these steps:

1. Log in to the r6.x Policy Server user interface.
2. Select Tools, Manage Keys.
3. Select the Use Static Agent Key option.
4. Click Apply.

The Policy Server is configured to use a static key. The Policy Server does not generate keys automatically.

Export the Agent Keys

You export the keys from the colocated policy/key store to make them available to the separate key store.

Follow these steps:

1. Log in to a r6.x Policy Server host system. Be sure that this Policy Server is configured with the colocated policy/key store.
2. Run the following command to export only the keys from the policy store:

```
smobjexport -ffile_name -x
```

Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

Note: For more information about these modes and arguments, see the r6.x *Policy Server Installation Guide*.

Example:

```
smobjexport -fagentkeys -x
```

The agent keys are exported from the colocated policy/key store.

3. Copy the file that contains the agent keys to the set-up Policy Server host system.

Import the Agent Keys

You import the keys from the colocated policy/key store to make them available to the separate key store.

Follow these steps:

1. Log in to the r6.x set-up Policy Server host system.
2. Run the following command to import the agent keys in to the separate key store:

```
smobjimport -ffile_name -k
```

Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

Note: For more information about these modes and arguments, see the r6.x *Policy Server Installation Guide*.

Example:

```
smobjimport -fagentkeys -k
```

The agent keys are imported in to the separate key store.

Configure all Policy Servers to use the Key Store

Configuring all Policy Servers in the parallel environment to use a common r6.x key store maintains single sign-on across both environments.

Follow these steps:

1. Identify the Policy Server that is nominated to generate agent keys dynamically. Configure this Policy Server with the key store last.
2. Complete the following procedure for all other Policy Servers in the environment:
 - a. Log in to the Policy Server host system.
 - b. Open the Policy Server Management Console.
 - c. Click the Data tab.
 - d. Select Key Store from the Database list and clear the Use Policy Store database option.
 - e. Select the key store type from the Storage list.
 - f. Do one of the following steps:
 - a. (LDAP) Enter the required connection information in the LDAP Key Store section.
 - b. (ODBC) Enter the data source information in the Data Source Information section.
 - g. Test the Connection.
 - h. Click OK.
 - i. Restart the Policy Server to configure the Policy Server to use the key store.
3. Configure the Policy Server that is nominated to generate agent keys to use the key store.

Re-enable Dynamic Agent Key Generation

If you disabled dynamic agent key generation, re-enable the functionality for the Policy Server that is nominated to generate agent keys. Complete this procedure only after all Policy Servers in the environment are configured to use the new key store.

Follow these steps:

1. Log in to the r6.x Policy Server user interface.
2. Select Tools, Manage Keys.
3. Select the Use Dynamic Agent Key option.

4. Click Apply.

The nominated Policy Server is enabled to generate keys dynamically.

You have completed the required tasks to separate the key store from the policy store.

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 CA 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 12.52 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 12.52 key stores.
Note: For more information about configuring a static Agent key and session ticket, see the *Policy Server Administration Guide*.

Migrate Keys and Certificates

If your environment contains one or more smkeydatabases, migrate their contents to the 12.52 certificate data store.

Follow these steps:

1. Be sure that all r6.x smkeydatabases are [synchronized](#) (see page 47).
2. Log in to an r6.x Policy Server host system and go to the following location:
`siteminder_home\config\properties`
`siteminder_home`
Specifies the Policy Server installation path.
3. Copy the following file:
`smkeydatabase.properties`

4. Log in to an 12.52 Policy Server host system and complete the following steps:

- a. Go to the following location:

siteminder_home\config\properties

- b. Rename the 12.52 version of the smkeydatabase properties file to the following value:

newsmkeydatabase.properties

- c. Add the r6.x version of the properties file to the directory.

- d. Open the 12.52 and r6.x properties file in a text editor.

- e. Edit the database location path in the r6.x version to match the path in the 12.52 version.

Example:

The r6.x file references the following path:

DBLocation=C\:/Program
Files/netegrity/siteminder/smkeydatabase

The 12.52 file references the following path:

DBLocation=C:/Program Files/CA/siteminder/smkeydatabase

Update the r6.x file to reference the following path:

DBLocation=C\:/Program Files/CA/siteminder/smkeydatabase

- f. Save the r6.x properties file and close the 12.52 properties file.

- g. Create the following directory at the root of the Policy Server installation:

smkeydatabase

Example:

C:\Program Files\CA\SiteMinder\smkeydatabase

5. Return to the r6.x Policy Server host system and copy the contents of the smkeydatabase directory.

Note: The default location of this directory is *siteminder_home*.

6. Return to the 12.52 Policy Server host system and complete the following steps:

- a. Add the contents of the r6.x smkeydatabase directory to the 12.52 smkeydatabase directory you created.

- b. Use the following migration utility to migrate the smkeydatabase to the certificate data store.

smmigratecds

- c. After a successful migration, remove the smkeydatabase properties file and the smkeydatabase directory.

The migration is complete.

More information:

[Migrate a CA SiteMinder® Key Database Manually](#) (see page 155)

Migrate the Assertion Issuer ID

If you are managing legacy federation (Federation Security Services) objects in your r12.x environment, migrate the assertion issuer ID from the r12.x Producer to the 12.52 Producer. Migrating the ID prevents SAML 1.1 transactions from failing on the Service Provider.

Follow these steps:

1. Log in to an r6.x Policy Server host system and go to the following location:

siteminder_home\config\properties

siteminder_home

Specifies the Policy Server installation path.

2. Copy the following file:

AMAssertionGenerator.properties

3. Log in to an 12.52 Policy Server host system and go to the following location:

siteminder_home\config\properties

4. Rename the 12.52 version of the assertion generator properties file to the following value:

newAMAssertionGenerator.properties

5. Add the r6.x version of the properties file to the directory.

The migration is complete.

Migrate the r6.x Policies

If you plan on using the 12.52 deployment to protect r6.x resources, we recommend migrating your policy store data to the 12.52 policy store.

You can avoid the possibility of conflicts that are associated with duplicate objects by migrating policy store data before you begin managing the 12.52 policy store.

Follow these steps:

1. Use the r6.x version of the smobjexport utility to export the r6.x policy store data.
Note: For more information about the r6.x version of the smobjexport utility, see the r6.x Policy Server Installation Guide.
2. Use the 12.52 version of the smobjimport utility to import the policy data into the 12.52 policy store.

When moving CA SiteMinder® policies from one environment to another, either as part of an upgrade or a policy migration, some objects that are environment-specific are included in the export file. Examples of these objects include:

- Trusted hosts
- HCO Policy Server settings
- Authentication scheme URLs
- Password services redirects
- Redirect responses

User Directory Single Sign-on Requirements

Be sure that the CA SiteMinder® user directory objects you create in both environments have the same names. If you use different names to point r6.x and 12.52 Policy Servers to the same user stores, single sign-on fails.

Chapter 3: Upgrading from r12.x

This section contains the following topics:

- [Migration Considerations](#) (see page 79)
- [How the r12.x Migration Works](#) (see page 82)
- [How to Migrate from r12.x](#) (see page 85)
- [How a Parallel Upgrade Works](#) (see page 105)
- [How to Configure a Parallel Environment](#) (see page 105)

Migration Considerations

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

Administrative UI Upgrade Paths

Review the following upgrade considerations:

- You cannot upgrade the Administrative UI on an existing application server from versions before 12.5 to 12.52. Instead, complete the following steps:
 - a. Uninstall the r12.x version of the Administrative UI.
 - b. Install an application server that CA SiteMinder® supports.
 - c. Install a new 12.52 Administrative UI.
- **Note:** For more information about installing the Administrative UI, see the *Policy Server Installation Guide*.
- You can upgrade the Administrative UI on an existing application server infrastructure only from version 12.5 to 12.52.
- You can upgrade the r12.x Administrative UI that uses the embedded version of JBoss to 12.52.

Note: For more information about upgrading the Administrative UI, read the instructions in [How to Migrate from r12.x](#) (see page 85) and [Upgrade an r12.x Administrative UI](#) (see page 99).

Administrative UI Protection with SiteMinder

You can protect an 12.52 Administrative UI with CA SiteMinder®. Protecting the Administrative UI requires that you complete the following steps:

1. Configure an agent to work with a reverse proxy server.

Note: For more information about configuring a reverse proxy server, see the *Web Agent Configuration Guide*.

2. Configure an external administrator store. You enable CA SiteMinder® authentication when you configure the store.

Note: For more information about configuring an external administrator store, see the *Policy Server Configuration Guide*.

If you have configured an r12.x Administrative UI with an external administrator store and you want to enable CA SiteMinder® authentication, complete the following steps:

1. Configure an agent to work with a reverse proxy server.
2. Reconfigure the external administrator store with the required agent settings.

Important! The Administrative UI does not retain the settings when you reconfigure the store. Before you reconfigure the connection, we recommend that you view the connection and record the settings.

Single Sign-on

You can maintain single sign-on during the migration to 12.52. Consider the following items:

- An 12.52 Policy Server can communicate with an r12.x policy store and an r12.x key store.
- An 12.52 Policy Server can communicate with an r12.x session store.

Certificate Data Management

The certificate data store is replacing the CA SiteMinder® key database (smkeydatabase). If you have one or more smkeydatabases deployed in your environment, consider the following items:

- The certificate data store is collocated with the 12.52 policy store. A single certificate data store replaces the need for an individual smkeydatabase instance on each Policy Server host system.
- As part of a Policy Server upgrade, all smkeydatabase content is automatically backed up and migrated to the certificate data store.

- A 12.52 Policy Server can only communicate with a certificate data store. A 12.52 Policy Server and the respective local smkeydatabase do not operate in compatibility mode. However, all Policy Servers that have not been upgraded continue to communicate with their local version of the smkeydatabase.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

- Synchronize all smkeydatabase instances before beginning the migration. Synchronizing all instances helps avoid data collisions. Data collisions prevent a successful migration.
- All Policy Servers that share a common view into the same policy store have access to the same keys, certificates, and certificate revocation lists (CRL).
- The purpose of the certificate data store remains unchanged from the purpose of the smkeydatabase. This store makes the following available to the CA SiteMinder® environment:
 - Certificate authority (CA) certificates
 - Public and private keys
 - Certificate revocation lists
- You can continue to use the CA SiteMinder® key tool to manage the certificate data store. However, several options are deprecated.

Note: For more information, see the *Policy Server Release Notes*.

- If a CRL is stored in an LDAP directory service, consider the following items:
 - CA SiteMinder® no longer requires that the issuer of the CRL is the same CA that issued the corresponding root certificate.
 - CA SiteMinder® no longer performs this check. This behavior is consistent with the requirements for a text-based CRL.

More information:

[Synchronize Key Database Instances](#) (see page 47)

Federation Integration

All Federation Security Services functionality available in an r12.x FSS Administrative UI has been moved to the Administrative UI. If you were managing a federated environment, this functionality is referred to as legacy federation.

The Administrative UI also includes partnership federation. This functionality is specific to the partnership-based federation that CA SiteMinder® Federation makes available.

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.

Advanced Password Services

If you have deployed Advanced Password Services, a Policy Server upgrade retains all LANG (translation), CFG (configuration), and mail files. The default 12.52 versions of the files are installed to *siteminder_home\samples*.

siteminder_home

Specifies the Policy Server installation path.

How the r12.x Migration Works

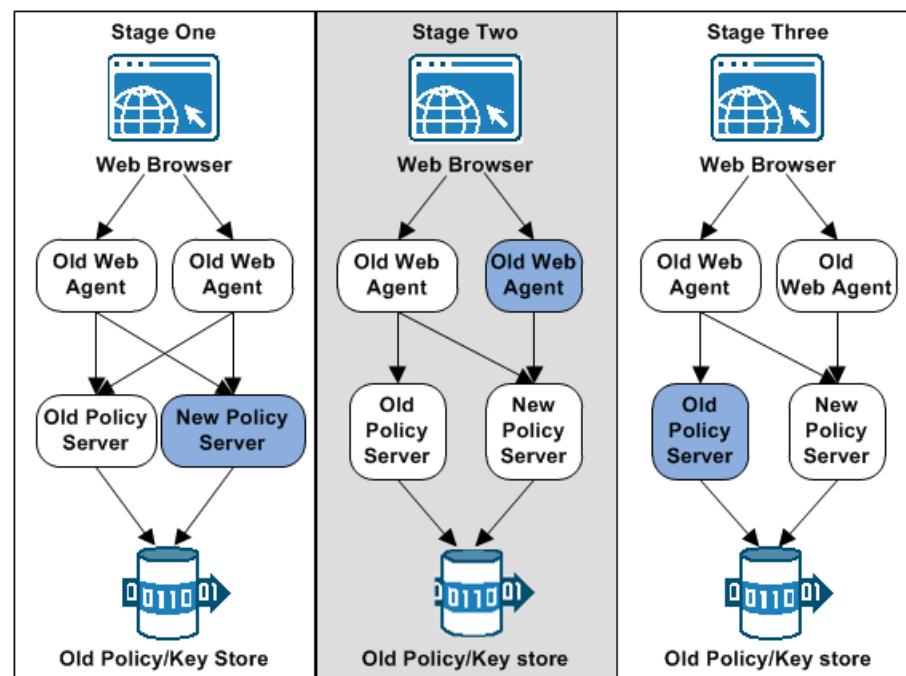
To migrate a CA SiteMinder® deployment with multiple Policy Servers and Web Agents, remove one of the Policy Servers and Web Agents from the CA SiteMinder® environment. While these components are being upgraded, the remaining Policy Servers and Web Agents continue to protect your resources.

Continue removing and upgrading CA SiteMinder® components until all components are upgraded or operating in mixed-mode compatibility.

The following figures illustrate a simple r12.x 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.

Figure 10: r12.x migration overview.

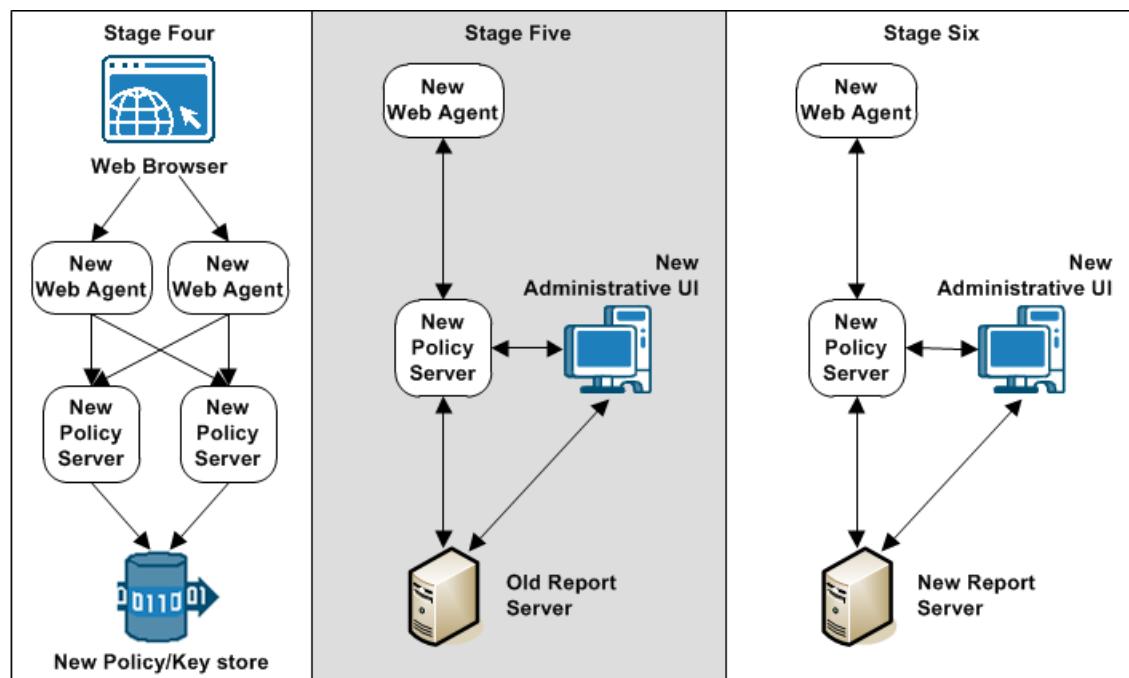


1. In stage one, an r12.x Policy Server is upgraded. The 12.52 Policy Server operates in compatibility mode. Consider the following items:
 - The r12.x Web Agents continue to communicate with the 12.52 Policy Server.
 - The 12.52 Policy Server continues to communicate with the r12.x policy and key store.
 - The r12.x Policy Server continues to communicate with the r12.x policy and key store.
 - If an r12.x Administrative UI is configured with the 12.52 Policy Server, the Administrative UI continues to communicate with the Policy Server to manage objects in the r12.x policy store.
 - If an r12.x Report Server is configured with the 12.52 Policy Server, the Report Server continues to create reports.

2. In stage two, an r12.x Web Agent is upgraded to 12.52.
 - The r12.x Web Agent continues to communicate with the r12.x and the 12.52 Policy Server.
 - The 12.52 Web Agent only communicates with the 12.52 Policy Server.

Note: You can configure a new 12.52 web agent with a 12.52 Policy Server during a migration. However, the 12.52 components only support features and functionality that are supported with the current version of your policy store.
3. In stage three, the remaining Policy Server is upgraded to 12.52. The 12.52 Policy Servers operate in compatibility mode with the r12.x policy and key store.

Figure 11: rr12.x migration overview.



4. In stage four, the r12.x policy and key store is upgraded to 12.52.
5. In stage five, the Administrative UI is upgraded.
6. In stage six, the r12.x Report Server is uninstalled. An 12.52 Report Server is installed, registered with the Policy Server, and connected to the Administrative UI.

Note: If you installed and configured an r12.0 SP3 cr4 or higher Report Server, this step is not required.

How to Migrate from r12.x

Complete the following procedures to migrate from r12.x to 12.52:

1. Review the installation and upgrade considerations in the *Policy Server Release Notes*.
2. (Optional) If your environment includes multiple instances of smkeydatabase, synchronize all instances. Part of the Policy Server upgrade includes migrating all content in the smkeydatabase to the certificate data store.
3. Review the sections in Before You Upgrade the Policy Server.
4. Upgrade an r12.x Policy Server to 12.52.
5. Upgrade an r12.x Web Agent to 12.52.
6. Upgrade the remaining r12.x Policy Servers and Web Agents to 12.52, respectively.
7. Upgrade the r12.x policy and key stores to 12.52.
8. Upgrade the r12.x Administrative UI.
9. If required, use the Administrative UI to save existing reports locally and remove the r12.x Report Server and report database from the environment. The simplest path to an 12.52 reporting environment is to install and configure a new Report Server and report database.

Synchronize Key Database Instances

Synchronize all smkeydatabase instances before beginning the migration to a new version.

Note: Use the smkeytool utility to synchronize the smkeydatabases and resolve all data inconsistencies between smkeydatabase instances. For more information about the smkeytool utility, see the *Policy Server Administration Guide*.

Previous versions of CA SiteMinder® used a local smkeydatabase to store certificate data. Each Policy Server required its own smkeydatabase. For version 12.52, a centralized certificate data store replaces the local smkeydatabases.

As part of a Policy Server upgrade, the installer automatically backs up the local smkeydatabase and tries to migrate all content to the certificate data store. This process includes a comparison of both stores before starting the migration.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

Use the following guidelines to identify and resolve data inconsistencies among your smkeydatabases:

- Verify that each certificate-authority certificate references certificate revocation lists consistently across instances.
Example: A certificate-authority certificate consistently references certificate revocation lists in an LDAP directory service.
- Verify that the defaultenterpriseprivatekey alias represents the same private key/certificate pair in all instances.
- Verify that the same alias maps to the same certificate or key/certificate pair.
- Verify that the same certificate-authority certificates map to the same certificate revocation lists.
- Verify that a revoked or expired certificate is not present.
- Verify that all CRL information is valid.

Important! After you resolve all data inconsistencies, we recommended that you do not modify a smkeydatabase until all migrations are complete.

Upgrade an r12.x Policy Server

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

Before You Upgrade

Before you upgrade a Policy Server, consider the following items:

- (Optional) If the environment contains multiple smkeydatabase instances, be sure to synchronize all content. Synchronizing resolves data inconsistencies that can prevent the Policy Server installer from automatically migrating content to the certificate data store.
- You upgrade the Policy Server using the installation media on the Technical Support site.
Note: For a list of installation media names, see the *Policy Server Release Notes*.
- (Linux) Be sure that the required Linux libraries are installed to the Policy Server host system. For more information, see Required Linux Libraries.
- Remove the Policy Server from the environment. Removing the Policy Server prevents CA SiteMinder® Agents from contacting the Policy Server during the upgrade.

- Shut down all instances of the Policy Server Management Console.
- (UNIX) The user account upgrading the Policy Server must have executable permissions on the directory that contains the installation media. If the user account does not have these permissions, run the following command:

```
chmod +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 Server using a root user.
- The CA SiteMinder® documentation is not installed with the Policy Server. We recommend that you locate the documentation before you upgrade.

Required Linux Libraries

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

```
java.lang.UnsatisfiedLinkError
```

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

Red Hat 5.x:

```
compat-gcc-34-c++-3.4.6-patch_version.i386  
libstdc++-4.x.x-x.el5.i686.rpm
```

Red Hat 6.x:

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

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

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

libXau-1.0.5-1.el6.i686.rpm

libxcb-1.5-1.el6.i686.rpm

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

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

libX11-1.3-2.el6.i686.rpm

libXrender-0.9.5-1.el6.i686.rpm

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

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

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

libICE-1.0.6-1.el6.i686.rpm

libuuid-2.17.2-12.7.el6.i686.rpm

libSM-1.1.0-7.1.el6.i686.rpm

libXext-1.1-3.el6.i686.rpm

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

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

libXi-1.3-3.el6.i686.rpm

libXtst-1.0.99.2-3.el6.i686.rpm

libXft-2.1.13-4.1.el6.i686.rpm

libXt-1.0.7-1.el6.i686.rpm

libXp-1.0.0-15.1.el6.i686.rpm

Disable XML Signature Wrapping Checks Before a Policy Server Upgrade

SAML 2.0 artifact transactions fail in CA SiteMinder® federation (legacy or partnership) deployments after you upgrade the Policy Server at the Service Provider.

The following conditions result in failed transactions:

- CA SiteMinder® federation is deployed is at the Service Provider site.
- SAML 2.0 HTTP-Artifact SSO is configured.
- Signature verification at the Service Provider is configured for the assertion or the artifact resolve response.
- The Policy Server setting that prevents XML signature wrapping attacks is enabled.

When the Policy Server tries to verify that the signature of the artifact response, the SSO transaction fails.

To prevent artifact SSO from failing, temporarily turn off the signature vulnerability check. Disable the check after you upgrade the Policy Server at the Service Provider site but before you put the Policy Server into service.

Follow these steps:

1. Navigate to the xsw.properties file. Locate the file in the following directory:
siteminder_install_dir\config\properties\xsw.properties
siteminder_install_dir is the location where you installed the Policy Server.
2. Open the file in a text editor, and set the DisableXSWCheck to true (DisableXSWCheck=true). Setting the value to true disables the vulnerability check.
3. After the entire deployment is at version 12.52, and the Policy Server is running, return the DisableXSWCheck setting to false (DisableXSWCheck=false). Setting the value to false enables the signature vulnerability check.

Verify That Existing Federated SAML Partnerships Do Not Have the Same Backchannel Username

Verify that no existing partnerships have incoming backchannel usernames (within the same protocol) that are the same before upgrading.

That is, no two SAML 2.0 partnerships can share an incoming backchannel username. Similarly, no two SAML 1.0 partnerships can share an incoming backchannel username. A SAML 1.0 and a SAML 2.0 partnership can share an incoming backchannel username but it is not recommended.

If you do have partnerships of the same protocol that share an incoming backchannel username, do the following steps before you upgrade:

1. Deactivate one of the partnerships.
2. Change the backchannel username that is defined in that partnership.
3. Inform the remote partner of the change.
4. Reactivate the partnership.

Upgrade a Policy Server on Windows

Follow these steps:

1. Review [Before You Upgrade](#) (see page 86).
2. Exit all applications that are running.
3. Navigate to the installation media.
4. 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, see the *Policy Server Release Notes*.

5. Considering the following items 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.
 - During the upgrade, leave the policy store check box on the configuration wizard cleared to preserve your existing policy store. However, the configuration wizard prompts you for the encryption key for the advanced authentication server. This key is stored on each Policy Server, but all Policy Servers require the same key.
 - If you are upgrading another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.
 - If the installer detects a smkeydatabase, it:
 - Backs up the smkeydatabase.
 - Attempts to migrate the content to the certificate data store.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

6. Review the installation settings and click **Install**.

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

More information:

[Troubleshoot a Policy Server Upgrade](#) (see page 57)

Upgrade a Policy Server Using a GUI on UNIX

Follow these steps:

1. Review [Before You Upgrade](#) (see page 86).
2. Exit all applications that are running.
3. Execute the following script in a ksh shell from the CA SiteMinder® installation directory:

`.../ca_ps_env.ksh`

Note: Be sure that there is a space between the periods.

4. Open a shell and navigate to the installation executable.
5. Enter the following command:

`./installation_media`

installation_media

Specifies the name of the Policy Server installer executable.

The Policy Server installer starts.

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

6. Considering the following items 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.
 - During the upgrade, leave the policy store check box on the configuration wizard cleared to preserve your existing policy store. You manually upgrade an existing policy store. However, the configuration wizard prompts you for the encryption key for the advanced authentication server. This key is stored on each Policy Server, but all Policy Servers require the same key. You manually upgrade an existing policy store.
 - If you are upgrading another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.

- If the installer detects a smkeydatabase, it:
 - Backs up the smkeydatabase.
 - Attempts to migrate the content to the certificate data store.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

7. Review the installation settings and click Install.

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

8. Click Done.

9. Execute the following script in a ksh shell from the CA SiteMinder® installation directory:

.../ca_ps_env.ksh

Note: Be sure that there is a space between the periods.

More information:

[Troubleshoot a Policy Server Upgrade](#) (see page 57)

Upgrade a Policy Server on UNIX Using a Console

Follow these steps:

1. Review [Before You Upgrade](#) (see page 86).
2. Exit all applications that are running.
3. Execute the following script in a ksh shell from the CA SiteMinder® installation directory:

.../ca_ps_env.ksh

Note: Be sure that there is a space between the periods.

4. Open a shell and navigate to the installation executable.
5. 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, see the *Policy Server Release Notes*.

6. Considering the following items when running the installer:

The installer prompts you to select CA 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.

■ Consider the following items when selecting components:

- Reconfigure components that had been previously configured for the environment. Be sure to select the respective components.
- During the upgrade, leave the policy store check box on the configuration wizard cleared to preserve your existing policy store. You manually upgrade an existing policy store. However, the configuration wizard prompts you for the encryption key for the advanced authentication server. This key is stored on each Policy Server, but all Policy Servers require the same key.
- If you are upgrading another (nth) Policy Server, use the same encryption key for the Advanced Authentication server that you used previously.

■ If the installer detects a smkeydatabase, it:

- Backs up the smkeydatabase.
- Attempts to migrate the content to the certificate data store.

Important! If the migration of the smkeydatabase fails, do not return the Policy Server to the environment. Returning the Policy Server after a failed migration causes all transactions that require the certificate data to fail.

7. Review the installation settings and press Enter.

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

8. Click Done.

9. Execute the following script in a ksh shell from the CA SiteMinder® installation directory:

.../ca_ps_env.ksh

Note: Be sure that there is a space between the periods.

More information:

[Troubleshoot a Policy Server Upgrade](#) (see page 57)

Policy Server Upgrade Creates a New JVMOptions File

During a Policy Server upgrade, the existing `JVMOptions.txt` file is renamed to `JVMOptions.txt.backup`. A new `JVMOptions.txt` file is created.

If the original file included customized parameters, be sure to modify the newly created file to include these customized parameters.

Custom Server-Side Code Requirements

Your Policy Server operating system determines whether recompiling custom server-side code is required. Use the following table to identify the requirement:

Operating System	Required?
Microsoft Windows and UNIX	No. Recompiling the custom code is optional.
Red Hat Linux	Yes. Upgrade the SDK and recompile the custom code using GCC 3.4.

Troubleshoot a Policy Server Upgrade

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.
- You can locate the smkeydatabase migration log (`smkeydatabaseMigration.log`) in `siteminder_home\log`.
Note: A Policy Server upgrade and a smkeydatabase migration are separate processes. If the smkeydatabase migration fails, the Policy Server upgrade does not fail.

Upgrade an r12.x Web Agent

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

CA SiteMinder® r12.x Web Agents can communicate with an 12.52 Policy Server. Therefore, upgrade a Policy Server to r12.5 before upgrading a Web Agent to 12.52.

Before You Upgrade an r12.x 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 CA 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.x Web Agent

Use the 12.52 web agent installer to upgrade a web agent.

- Agents that require option pack functionality must be upgraded to 12.52 before installing the 12.52 Web Agent Option Pack.

Note: For more information about upgrading a web agent, see the *Web Agent Installation Guide*. For more information about installing the 12.52 Web Agent Option Pack, see the *Web Agent Option Pack Guide*.

- If you have deployed Advanced Password Services, a web agent upgrade retains all LANG (translation) and CFG (configuration) files. The default 12.52 versions of the files are installed to `agent_home\samples`.

agent_home

Specifies the web agent installation path.

Custom Agent Requirements

To determine if you are required to recompile your custom agent, use the following table:

Agent Type	Required?
CA SiteMinder® agent	Operating system-specific. If the agent operating system has reached end-of-life, you must recompile the custom agent. Upgrade the CA SiteMinder® SDK and recompile the agent on a supported operating system.
Third-party agent	Vendor-specific. Contact your third-party vendor to determine whether the agent is supported.

How to Upgrade an r12.x Policy Store

Complete the following procedures to upgrade an r12.x policy store to 12.52:

1. Stop all Policy Servers that are communicating with the policy store.
2. Import the policy store data definitions.
3. Import the default policy store objects.
4. If you managed your r12.x legacy federation environment using the FSS Administrative UI, run the XPS sweeper utility to complete the migration of your legacy federation objects.
5. Start all Policy Servers that are communicating with the policy store.

Stop all Policy Servers

Stopping all of the Policy Servers that are communicating with the policy store helps to prevent policy store corruption during the upgrade.

Follow these steps:

1. Log in to the Policy Server host system.
2. Complete one of the following steps:
 - (Windows)
 - a. Open the Policy Server Management Console and click Stop.
 - b. Click OK to close the console.
 - (UNIX) Use the following supplied script:
install_path/siteminder/stop-all
install_path
Specifies the Policy Server installation path.
3. Repeat this procedure for each Policy Server that is communicating with the policy store.

Import the Policy Store Data Definitions

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

Follow these steps:

1. Open a command window and navigate to *siteminder_home\xps\dd*.
siteminder_home
Specifies the Policy Server installation path.
2. Run the following command:
XPSDDInstall SmMaster.xdd
XPSDDInstall
Imports the required data definitions.

Import the Default Policy Store Objects

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

Consider the following items:

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

siteminder_home

Specifies the Policy Server installation path.

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

Follow these steps:

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

2. Import one of the following files:

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

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

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

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

Note: You use either file to configure a new policy store and upgrade an existing store. When imported as part of an upgrade, the file does not overwrite existing default objects that were modified. Both files include the default policy store objects. These objects include the default security settings in the default Agent Configuration Object (ACO) templates. The secure file provides more restrictive security settings.

-npass

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

The default policy store objects are imported.

Run the XPS Sweeper Utility

If you managed your Federation Security Services (legacy federation) objects using the FSS Administrative UI, run the XPS sweeper utility (XPSSweeper) to complete the migration of these objects.

Follow these steps:

1. Log in to the Policy Server host system.
2. Run the following command to make available your legacy federation objects to the Administrative UI:

XPSSweeper

All legacy federation created using the FSS Administrative UI are available in the Administrative UI.

Start all Policy Servers

Starting all Policy Servers resumes communication between all of the Policy Servers and the upgraded policy store.

Follow these steps:

1. Log in to the Policy Server host system.
2. Complete one of the following steps:
 - (Windows)
 - a. Open the Policy Server Management Console and click Start.
 - b. Click OK to close the console.
 - (UNIX) Use the following supplied script:
install_path/siteminder/start-all
install_path
Specifies the Policy Server installation path.
3. Repeat this procedure for each Policy Server that is communicating with the policy store.

The policy store is upgraded.

Upgrade an r12.x Administrative UI

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

Before You Upgrade

Consider the following items before you upgrade the Administrative UI:

- **Important!** Review the [Administrative UI upgrade paths](#) (see page 79).
- Upgrade the Administrative UI using the installation media on the Technical Support site.

Note: For a list of installation media names, see the *Policy Server Release Notes*.
- (Embedded JBoss installations only) Extract the contents of the prerequisite installer into the same directory that you extracted the contents of the Administrative UI installer. The contents of each installer zip file must be in the same location as the layout.properties file. The layout.properties file, which is included with the Administrative UI installation zip, must always be co-located with both executables or the installation fails.
- (Windows) Run the installer from the Administrative UI host system. Do not run the installer from a mapped network share or UNC path.
- (Linux) Be sure that the required Linux libraries are installed to the Administrative UI host system. For more information, see Required Linux Libraries.
- **Important!** (UNIX) Depending on your permissions, run the following command to add executable permissions to the directory that contains the installation media:

```
chmod -R+x directory  
directory
```

Specifies the directory that contains the installation media.
- (UNIX) If you execute the Administrative UI installer across different subnets, it can crash. Run the Administrative UI installer directly on the host system.

Required Linux Libraries

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

```
java.lang.UnsatisfiedLinkError
```

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

Red Hat 5.x:

```
compat-gcc-34-c++-3.4.6-patch_version.i386  
libstdc++-4.x.x-x.el5.i686.rpm
```

Red Hat 6.x:

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

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

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

libXau-1.0.5-1.el6.i686.rpm

libxcb-1.5-1.el6.i686.rpm

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

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

libX11-1.3-2.el6.i686.rpm

libXrender-0.9.5-1.el6.i686.rpm

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

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

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

libICE-1.0.6-1.el6.i686.rpm

libuuid-2.17.2-12.7.el6.i686.rpm

libSM-1.1.0-7.1.el6.i686.rpm

libXext-1.1-3.el6.i686.rpm

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

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

libXi-1.3-3.el6.i686.rpm

libXtst-1.0.99.2-3.el6.i686.rpm

libXft-2.1.13-4.1.el6.i686.rpm

libXt-1.0.7-1.el6.i686.rpm

libXp-1.0.0-15.1.el6.i686.rpm

Upgrade the Administrative UI on Windows

Follow these steps:

1. (Embedded JBoss setups only). Verify that you extracted the prerequisite installer zip into the same directory that you extracted the Administrative UI installer zip. The layout.properties file, included with the Administrative UI installation zip, must be located in the same directory as both executables.

Note: If you move the prerequisite or Administrative UI installation executables after extracting the zips, move the layout.properties file to the same location.

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

Note: For information about stopping and starting the embedded JBoss application server, see the r12.x *Policy Server Installation Guide*. For information about stopping an existing application server, see the vendor-specific documentation.

4. For embedded JBoss installations only, run the following executable and follow the installer prompts. Otherwise, skip to the next step.

`adminui-pre-req-version-cr-win32.exe`

5. Run the following executable:

`ca-adminui-version-cr-win32.exe`

6. Follow the installer prompts and confirm upgrade of the Administrative UI.

7. Review the installation settings and click Install.

8. For existing application servers, restart the application server after the installation is complete.

Note: The embedded JBoss application server automatically restarts after the installation is complete.

The Administrative UI is upgraded.

Upgrade the Administrative UI on UNIX

You can install the Administrative UI on UNIX platforms in GUI or Console mode.

Follow these steps:

1. (Embedded JBoss setups only). Verify that you extracted the prerequisite installer zip into the same directory that you extracted the Administrative UI installer zip. The layout.properties file, included with the Administrative UI installation zip, must be located in the same directory as both executables.

Note: If you move the prerequisite or Administrative UI installation executables after extracting the zips, move the layout.properties file to the same location.

2. Exit all applications that are running.

3. Stop the application server that is hosting the Administrative UI.

Note: For information about stopping and starting the embedded JBoss application server, see the *r12.x Policy Server Installation Guide*. For information about stopping an existing application server, see the vendor-specific documentation.

4. For embedded JBoss installations only, run the prerequisite installer. Otherwise, skip to the next step.

- a. Open a shell and navigate to one of the following prerequisite installation executables:

```
adminui-pre-req-version-cr-linux.bin  
adminui-pre-req-version-cr-sol.bin
```

- b. Enter the command for the appropriate mode:

GUI Mode

```
./prerequisite_installation_media
```

Console Mode

```
./prerequisite_installation_media -i console
```

- c. Follow the prerequisite installer prompts.

5. Open a shell and navigate to one of the following installation executables:

```
ca-adminui-version-cr-linux.bin
```

```
ca-adminui-version-cr-sol.bin
```

6. Enter the command for the appropriate mode:

GUI Mode

```
./installation_media
```

Console Mode

```
./installation_media -i console
```

7. Follow the prompts and confirm the upgrade of the Administrative UI.

8. Review the installation settings and click Install.

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

Note: For information about stopping and starting the embedded JBoss application server, see the *r12.x Policy Server Installation Guide*. For information about stopping an existing application server, see the vendor-specific documentation.

The Administrative UI is upgraded.

Upgrade an r12.x Report Server

If you are using a Report Server version that is previous to r12.0 SP3 CR4, the simplest path to the 12.52 reporting environment is to uninstall the installed version, and then install and configure the 12.52 reporting components.

If you are using a Report Server r12.0 SP3 CR4 or higher, an upgrade is not required. However, if you want localized reports, you require the 12.52 reporting templates. So, run the 12.52 version of the Report Server Configuration Wizard for the reporting templates.

The Report Server uses data in the policy store and the CA SiteMinder® audit database to compile policy analysis and audit-based reports. The report database contains no information that these reports require. As a result, a migration from an r12.x report database to an 12.52 report database is not necessary.

Complete the following process to install and configure the 12.52 reporting components:

1. (Optional) Export existing reports.

Important! Existing reports are stored in the report database. If you require existing reports for historical purposes, 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*.

2. Delete the connection between Report Server and the Administrative UI.

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

3. Uninstall the r12.x Report Server.

Note: For more information, see the r12 SP2 *Policy Server Installation Guide*. Uninstalling the Report Server does not remove the tables in the report database. Access the report database and remove all tables manually.

4. Install and configure 12.52 reporting, which includes:

- a. Installing the Report Server.
- b. Installing the CA SiteMinder® report templates.
- c. Registering the Report Server.
- d. Configuring connectivity between the Report Server and a CA SiteMinder® audit database.

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

How a Parallel Upgrade Works

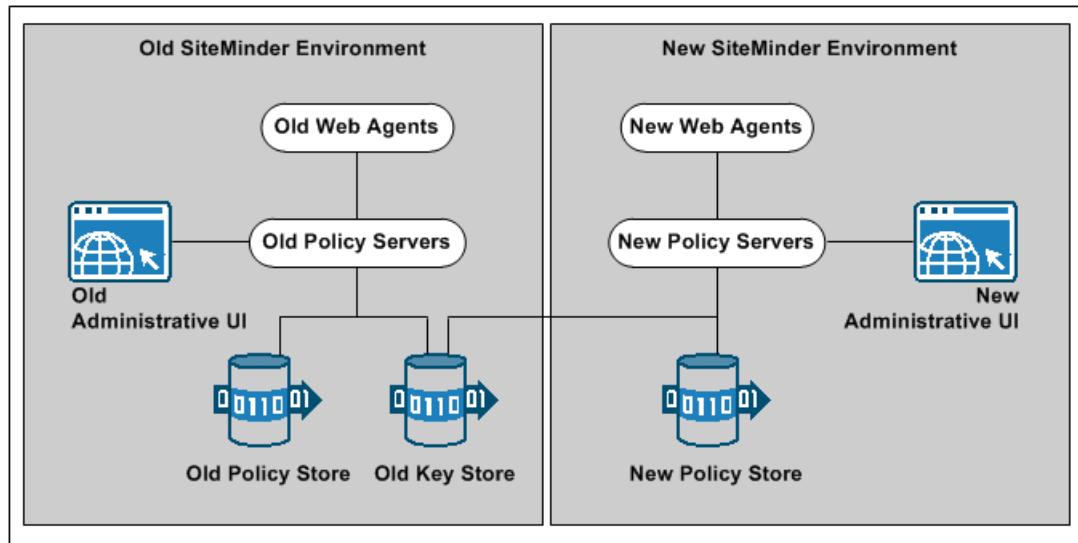
You do not have to migrate an existing r12.x environment to 12.52. Rather, you can configure a parallel 12.52 environment with an existing deployment.

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 CA SiteMinder® objects in the r12.x policy store.
- An 12.52 environment that protects new resources.
- An 12.52 Administrative UI that is used to manage CA SiteMinder® objects in the 12.52 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.

Figure 12: r12.x parallel upgrade overview



How to Configure a Parallel Environment

Complete the following 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 12.52 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. Migrate the r12.x policy store data. Use the 12.52 version of the XPSImport utility to import 12.52 default policy objects to the 12.x policy store using the following command

```
XPSImport smpolicy.xml -npass
```
5. If your r12.x environment contains smkeydatabases:
 - a. Synchronize all instances.
 - b. Migrate the content of a smkeydatabase to the 12.52 certificate data store.
6. If you are managing legacy federation (Federation Security Services) objects in your r12.x environment, migrate the assertion issuer ID.
7. Review the user directory single sign-on requirements.

More information:

[Certificate Data Management](#) (see page 29)
[Synchronize Key Database Instances](#) (see page 47)

Parallel Environment Key Management Options

Managing CA SiteMinder® keys to maintain single sign-on between the existing environment and 12.52 environment is critical to a successful parallel upgrade. Two CA 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.
- 12.52 Policy Servers connecting to an 12.52 policy store.

- A common r12.x key store maintaining key data for all Policy Servers. The common key store lets agents that are 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.

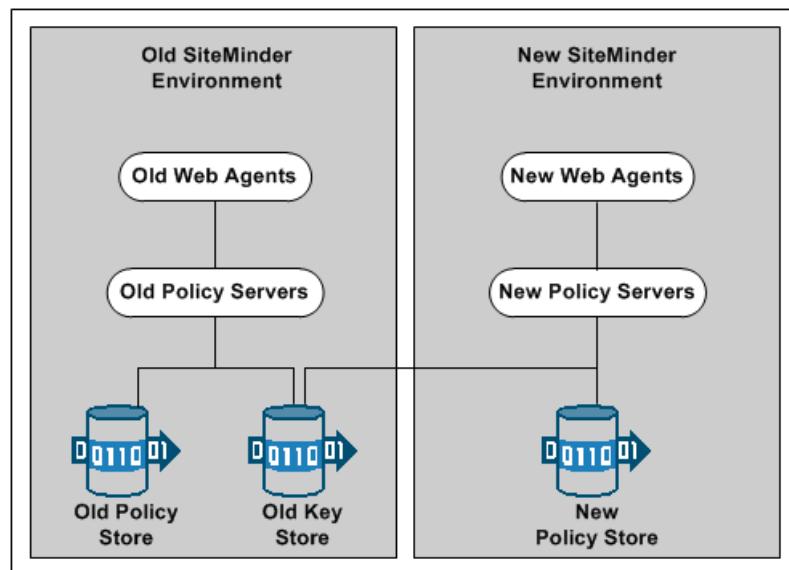
- All Policy Servers connecting to a common key store to retrieve new keys.

Important! The 12.52 Policy Servers must be configured with the r12.x key store. r12.x Policy Servers cannot communicate with an 12.52 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.

Figure 13: r12.x common key store deployment



Multiple Key Store Deployment

Existing r12.x Policy Servers can use an r12.x key store for key rollover, while 12.52 Policy Servers can use an 12.52 key store for key rollover. The following figure illustrates:

- r12.x Policy Servers connecting to an r12.x policy store.
- 12.52 Policy Servers connecting to an 12.52 policy store.
- r12.x Policy Servers connecting to an r12.x key store to retrieve new keys.

- 12.52 Policy Servers connecting to an 12.52 key store to retrieve new keys.
- A CA SiteMinder® administrator using the Administrative UI to configure static Agent and Session keys for each key store.

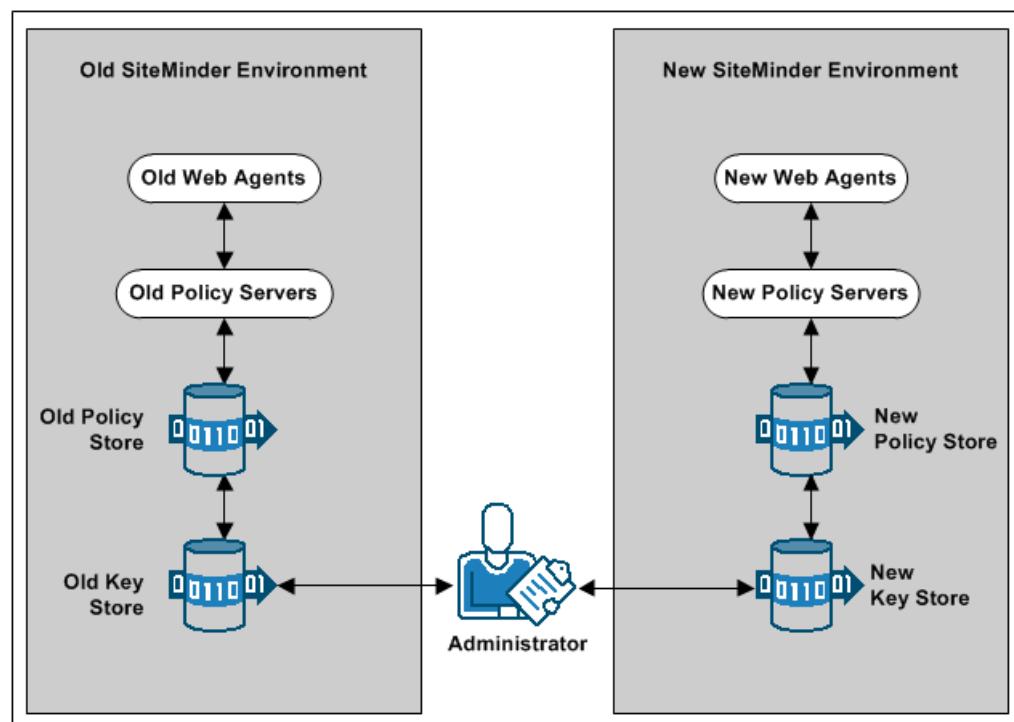
Important! If all key stores do not use the same Agent and Session keys, single sign-on fails.

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

- 12.52 Web Agents polling their respective 12.52 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.

Figure 14: r12.x multiple key store deployment



Create the 12.52 Environment

You can configure an 12.52 environment independently of the existing environment. Install and configure the 12.52 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 12.52 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:
 - If the r12.x environment is configured with a separate key store, leave the key store version at r12.x. 12.52 Policy Servers can communicate with an r12.x key store, but r12.x Policy Servers cannot communicate with an 12.52 key store.
 - If the r12.x environment is configured with a collocated policy/key store, separate the r12.x keys in to a separate r12.x key store.
- Leave the key store version at r12.x. 12.52 Policy Servers can communicate with an r12.x key store, but r12.x Policy Servers cannot communicate with an 12.52 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 12.52 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*.

How to Separate a Key Store from a Policy Store

Complete the following procedures to separate the key store from the policy store:

1. Install or locate a set-up Policy Server. A set-up Policy Server is a Policy Server that is not configured with the collocated policy/key store.
 - If a Policy Server is configured with the collocated store, you cannot use it to configure the new key store instance. The required CA SiteMinder® utilities available on the Policy Server host system are configured to manage the collocated store.
 - The set-up Policy Server makes available a separate set of the required utilities. The separate set lets you configure the key store without interfering with the collocated store.
2. Use the set-up Policy Server host system to create a separate r12.x key store instance. Consider the following items:
 - The key store only requires the default policy store schema. For more information about configuring a separate key store, see the *r12.0 SP3 Policy Server Installation Guide*.
 - The key store does not require that you:
 - Set the CA SiteMinder® superuser password.
 - Import the default policy store objects.
3. Disable dynamic agent key generation in the r12.x environment.

Note: If your environment uses static keys, this step is not required. However, be sure that a CA SiteMinder® administrator does not generate a random agent key after you export the keys from the policy store.
4. Export the agent keys from the r12.x policy/key store.
5. Import the agent keys in to the r12.x key store.
6. Configure all Policy Servers to use the separate key store.
7. If you disabled dynamic agent key generation, re-enable it.

Disable Dynamic Agent Key Generation

Before the key store separation is complete, the r12.x environment is operating with two key stores:

- Some Policy Servers use the agents keys in the collocated policy/key store.
- Some Policy Servers use the agent keys in the separate key store.

Disabling dynamic agent key generation prevents a Policy Server from generating keys after you export them for the separate store. Stopping the Policy Server from generating keys prevents single sign-on issues that can occur when the keys are not synchronized in all stores.

Follow these steps:

1. Log in to the r12.x Administrative UI.
2. Click Administration, Policy Server.
3. Click Key Management, Agent Key Management.
4. Select the Use Static Agent Key option.
5. Click Submit.

The Policy Server is configured to use a static key. The Policy Server does not generate keys automatically.

Export the Agent Keys

You export the keys from the collocated policy/key store to make them available to the separate key store.

Follow these steps:

1. Log in to a r12.x Policy Server host system. Be sure that this Policy Server is configured with the collocated policy/key store.
2. Run the following command to export only the keys from the policy store:

```
smkeyexport -dadministrator -wpassword -ofile_name
```

Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

Note: For more information about the utility, see the r12.x *Policy Server Administration Guide*.

Example:

```
smkeyexport -dsuperuser -wpassword -oagentkeys
```

The agent keys are exported from the collocated policy/key store.

3. Copy the file that contains the agent keys to the set-up Policy Server host system.

Import the Agent Keys

You import the keys from the collocated policy/key store to make them available to the separate key store.

Follow these steps:

1. Log in to the r12.x set-up Policy Server host system.
2. Run the following command to import the agent keys in to the separate key store:

```
smobjimport -ffile_name -k
```

Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

Note: For more information about these modes and arguments, see the *r12.x Policy Server Administration Guide*.

Example:

```
smobjimport -fagentkeys -k
```

The agent keys are imported in to the separate key store.

Configure all Policy Servers to use the Key Store

Configuring all Policy Servers in the parallel environment to use a common r12.x key store maintains single sign-on across both environments.

Follow these steps:

1. Identify the Policy Server that is nominated to generate agent keys dynamically. Configure this Policy Server with the key store last.
2. Complete the following steps for all other Policy Servers in the environment:
 - a. Log in to the Policy Server host system.
 - b. Open the Policy Server Management Console.
 - c. Click the Data tab.
 - d. Select Key Store from the Database list and clear the Use Policy Store database option.
 - e. Select the key store type from the Storage list.

- f. Complete one of the following steps:
 - (LDAP) Enter the required connection information in the LDAP Key Store section.
 - (ODBC) Enter the data source information in the Data Source Information section.
- g. Test the Connection.
- h. Click OK.
- i. Restart the Policy Server to configure the Policy Server to use the key store.

3. Configure the Policy Server that is nominated to generate agent keys to use the key store.

Re-enable Dynamic Agent Key Generation

If you disabled dynamic agent key generation, re-enable the functionality for the Policy Server that is nominated to generate agent keys. Complete this procedure only after all Policy Servers in the environment are configured to use the new key store.

Follow these steps:

1. Log in to the r12.x Administrative UI.
2. Click Administration, Policy Server.
3. Click Key Management, Agent Key Management.
4. Select the Use Dynamic Agent Key option.
5. Click Submit.

The nominated Policy Server is enabled to generate keys dynamically.

You have completed the required tasks to separate the key store from the policy store.

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 CA 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 12.52 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 12.52 key stores.

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

Migrate Keys and Certificates

If your environment contains one or more smkeydatabases, migrate their contents to the 12.52 certificate data store.

Follow these steps:

1. Be sure that all r12.x smkeydatabases are [synchronized](#) (see page 47).
2. Log in to an r12.x Policy Server host system and go to the following location:
`siteminder_home\config\properties`
`siteminder_home`
Specifies the Policy Server installation path.
3. Copy the following file
`smkeydatabase.properties`
4. Log in to an 12.52 Policy Server host system and complete the following steps:
 - a. Go to the following location:
`siteminder_home\config\properties`
 - b. Rename the 12.52 version of the smkeydatabase properties file to the following value:
`newsmkeydatabase.properties`
 - c. Add the r12.x version of the properties file to the directory.
 - d. Open the 12.52 and r12.x properties file in a text editor.

- e. Edit the database location path in the r12.x version to match the path in the 12.52 version.

Example:

The r12.x file references the following path:

```
DBLocation=C\:/Program  
Files/netegrity/siteminder/smkeydatabase
```

The 12.52 file references the following path:

```
DBLocation=C:/Program Files/CA/siteminder/smkeydatabase
```

Update the r12.x file to reference the following path:

```
DBLocation=C\:/Program Files/CA/siteminder/smkeydatabase
```

- f. Save the r12.x properties file and close the 12.52 properties file.
- g. Create the following directory at the root of the Policy Server installation:
smkeydatabase

Example:

```
C:\Program Files\CA\SiteMinder\smkeydatabase
```

5. Return to the r12.x Policy Server host system and copy the contents of the smkeydatabase directory.

Note: The default location of this directory is *siteminder_home*.

6. Return to the 12.52 Policy Server host system and complete the following steps:

- a. Add the contents of the r12.x smkeydatabase directory to the 12.52 smkeydatabase directory you created.
- b. Use the following migration utility to migrate the smkeydatabase to the certificate data store:
`smmigratecds`
- c. After a successful migration, remove the smkeydatabase properties file and the smkeydatabase directory.

The migration is complete.

More information:

[Migrate a CA SiteMinder® Key Database Manually](#) (see page 155)

Migrate the Assertion Issuer ID

If you are managing legacy federation (Federation Security Services) objects in your r12.x environment, migrate the assertion issuer ID from the r12.x Producer to the 12.52 Producer. Migrating the ID prevents SAML 1.1 transactions from failing on the Service Provider.

Follow these steps:

1. Log in to an r12.x Policy Server host system and go to the following location:
siteminder_home\config\properties
siteminder_home
Specifies the Policy Server installation path.
2. Copy the following file:
AMAssertionGenerator.properties
3. Log in to an 12.52 Policy Server host system and go to the following location:
siteminder_home\config\properties
4. Rename the 12.52 version of the assertion generator properties file to the following value:
newAMAssertionGenerator.properties
5. Add the r12.x version of the properties file to the directory.

The migration is complete.

Migrate the r12.x Policies

If you plan on using the 12.52 deployment to protect r12.x resources, we recommend migrating your policy store data to the 12.52 policy store.

Although not required, if you migrate the policy store data before you begin managing the 12.52 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. For more information about the r12.x version of XPSExport, see the *r12.x Policy Server Administration Guide*.
2. Use the 12.52 version of the XPSImport utility to import the policy data into the 12.52 policy store. For more information about the 12.52 version of XPSImport, see the *Policy Server Administration Guide*.

When moving CA SiteMinder® policies from one environment to another, either as part of an upgrade or a policy migration, some objects that are environment-specific are included in the export file. Examples of these objects include:

- Trusted hosts
- HCO Policy Server settings
- Authentication scheme URLs
- Password services redirects
- Redirect responses

Depending on the mode you select when using XPSExport, these objects may be added to the new environment or can overwrite existing settings. Be sure that you do not adversely affect environment settings when importing the objects.

Note: For more information about the XPSExport modes of export, see the *Policy Server Administration Guide*.

User Directory Single Sign on Requirements

Be sure that the CA SiteMinder® user directory objects you create in both environments have the same names. If you use different names to point r12.x and 12.52 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](#) (see page 119)
- [FIPS 140-2 Migration Requirements](#) (see page 120)
- [Migration Roadmap—Re-Encrypt Sensitive Data](#) (see page 120)
- [How to Re-Encrypt Existing Sensitive Data](#) (see page 122)
- [Migration Roadmap—Configure FIPS-Only Mode](#) (see page 135)
- [How to Configure FIPS-only Mode](#) (see page 136)

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 that is used to accredit cryptographic modules that meet the Advanced Encryption Standard (AES). These libraries provide a FIPS mode of operation when a CA SiteMinder® environment only uses FIPS-compliant algorithms to encrypt sensitive data. A CA SiteMinder® environment can operate in one of the following FIPS modes of operation:

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

By default, an environment that is upgraded to 12.52 is operating in FIPS-compatibility mode. In FIPS-compatibility mode, the environment uses algorithms existing in previous versions of CA SiteMinder® to encrypt sensitive data and is compatible with previous versions CA SiteMinder®. If your organization does not require the use of FIPS-compliant algorithms, the environment 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 a 12.52 environment running in FIPS-compatibility mode to FIPS-only mode. In FIPS-migration mode, the 12.52 environment continues to use existing CA 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 versions of CA SiteMinder® before 12.x, including:

- All agents
- Custom software using older versions of the Agent API
- Custom software using PM APIs or any other API that the Policy Server exposes

Re-link all such software with the 12.52 versions of the respective SDKs to achieve the required support for FIPS-only mode.

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 CA SiteMinder® environment, including the SDK, is upgraded to 12.52.
- 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.

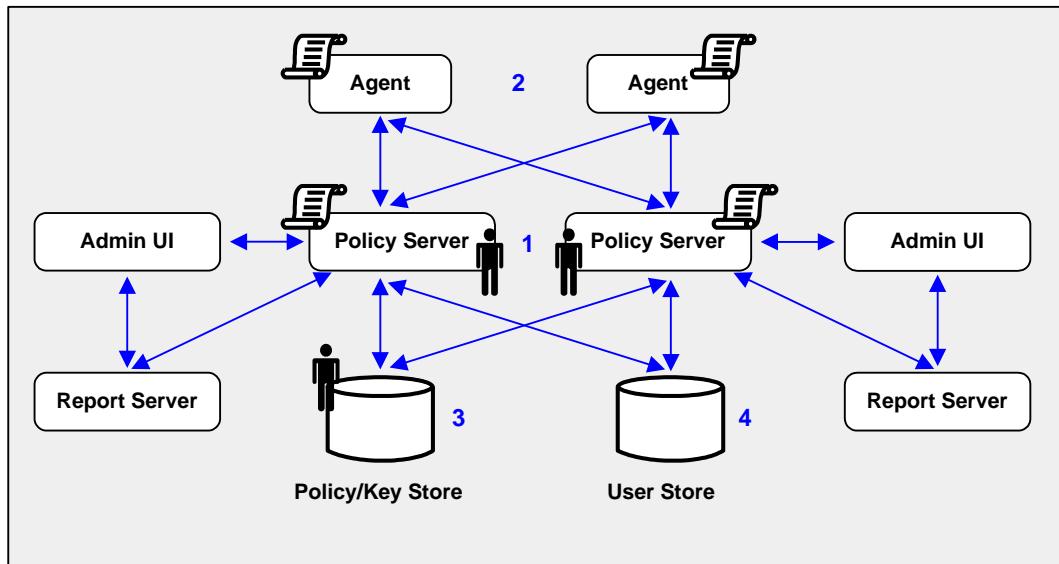
Migration Roadmap—Re-Encrypt Sensitive Data

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 12.52 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 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 key is located in the EncryptionKey.txt file.
 - 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 store, these passwords are encrypted using algorithms that are not FIPS-compliant. Re-encrypt these passwords before configuring the environment for FIPS-only mode.

 - The CA SiteMinder® superuser password is encrypted using algorithms that are not FIPS-compliant. Re-encrypt the password before configuring the environment for FIPS-only mode.

Note: The password is for the default CA SiteMinder® administrator account. The account is used for all administrative tasks that do not require direct access to the Administrative UI. The password is not the password for the Administrative UI administrator account with superuser privileges.

2. Each CA SiteMinder® 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 can 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 to log in or to 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 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 CA 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.

- **CA SiteMinder® Super User account name and password**— Identify the CA SiteMinder® Super User account name and password. CA 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.

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 CA SiteMinder® encryption algorithms as you re-encrypt existing sensitive data using FIPS-compliant algorithms.

Follow these steps:

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

```
setFIPSmigration
```

MIGRATION appears in the command window.

2. Stop the Policy Server.

Note: For more information about stopping and starting the Policy Server, see the *Policy Server Administration Guide*.

3. Complete one of the following steps:

- If the Policy Server is installed on a Windows system, reboot the system.
- If the Policy Server is installed on a UNIX system, complete the following steps:
 - a. Log in as the user that is used to start the Policy Server.
 - b. Open a command prompt.
 - c. Navigate to *policy_server_home*.
 - d. Run the following command:

```
./ca_ps_env.ksh
```

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 can 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 be sure that the data is encrypted using FIPS-compliant algorithms.

Follow these steps:

1. Start the Policy Server Management Console, and click the Data tab.
Note: For more information about starting the Policy Server Management Console, see the *Policy Server Administration Guide*.
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 stores, re-encrypt the administrator password for each:
 - key store
 - audit logs
 - token data
 - session store

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 can now re-encrypt the CA SiteMinder® superuser password.

Re-encrypt the CA SiteMinder® Super User Password

You re-encrypt the CA 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 CA 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 CA 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 CA 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 host 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 CA 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 CA 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 12.52 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 12.52 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 a 12.52 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 -dadmin_name -wadmin_password -ooutput_file_name -l -v -t -cf  
-dadmin_name
```

Specifies the name of the CA SiteMinder® administrator account.

-wadmin_password

Specifies the password for the CA SiteMinder® administrator account.

-ooutput_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 -dadmin_name -wadmin_password -l -v -t -cf  
-i
```

Specifies the name of the file output file you created.

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

-dadmin_name

Specifies the name of the CA SiteMinder® administrator account.

-wadmin_password

Specifies the password for the CA 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 -xe -xp -pass <passphrase> -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

-xe

Exports the object types that are related to the execution environment.

-xp

Exports the object types that are related to the policies.

-pass <passphrase>

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 -pass <passphrase> -vT -vI -vW -vE -vF -l log_path  
input_file
```

Specifies the input XML file.

-pass <passphrase>

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 uses 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.

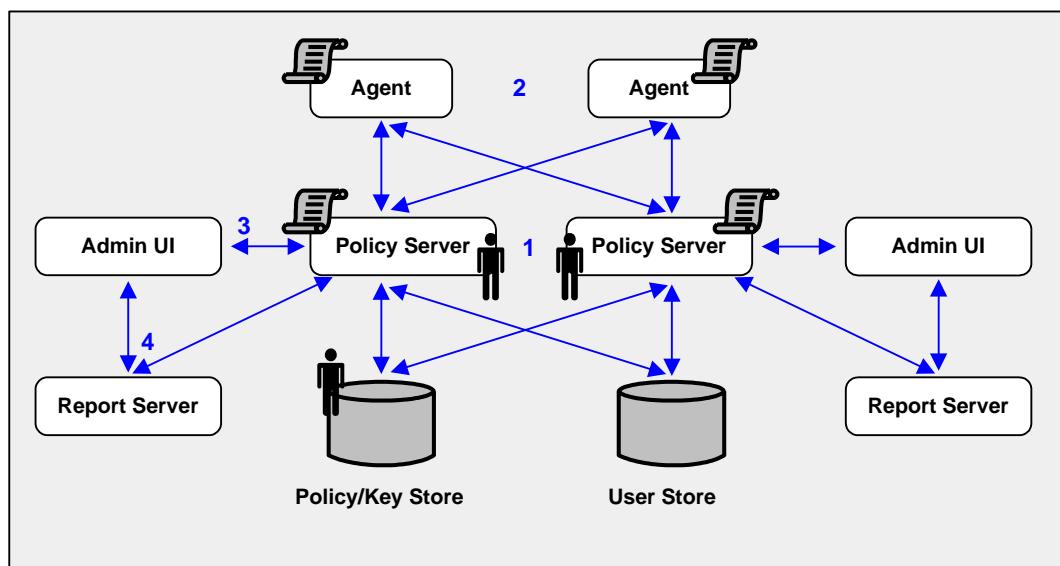
Migration Roadmap—Configure FIPS-Only Mode

The following diagram illustrates a sample 12.52 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 CA 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 CA 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 its 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 CA 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 read and write encrypted information using FIPS-compliant algorithms only.

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: For more information about identifying Password Blobs that are not re-encrypted, see [Verify that Password Blobs are Re-encrypted](#) (see page 134).

Follow these steps:

1. Open a command prompt from the Policy Server host system and run the following command:

```
setFIPSOnly
```

ONLY appears in the command window.

2. Stop the Policy Server.

Note: For more information about stopping and starting the Policy Server, see the *Policy Server Administration Guide*.

3. Do one of the following steps:
 - If the Policy Server is installed on a Windows system, reboot the system.
 - If the Policy Server is installed on a UNIX system, do the following steps:
 - a. Log in as the user that is used to start the Policy Server.
 - b. Open a command prompt.
 - c. Navigate to *policy_server_home*.
 - d. Run the following command:
`./ca_ps_env.ksh`
4. Start the Policy Server.
5. Open the *smpls.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 can now re-register each Administrative UI with its respective Policy Server.

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

Existing CA 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 CA 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 -retries -c comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

siteminder_administrator

Specifies a CA SiteMinder® administrator with super user permissions.

Note: If a super user account is not available, use the smreg utility to create the default CA SiteMinder® account.

passphrase

Specifies the password for the CA 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: 240 (4 hours)

Minimum limit: 1

Maximum limit: 1440 (24 hours)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you are registering the Administrative UI. A failed attempt can result from submitting incorrect CA SiteMinder® administrator credentials when logging 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 CA 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 CA 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 CA 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\CommonReporting3

Default: (UNIX) /opt/CA/SharedComponents/CommonReporting3

2. Run one of the following commands:

- (Windows)

```
regreportserver.bat -pshost host_name -client client_name -passphrase  
passphrase  
-psport portnum -fipsmode 0|1
```

Important! Before running a CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

- (UNIX)

```
regreportserver.sh -pshost host_name -client client_name -passphrase  
passphrase  
-psport portnum -fipsmode 0|1
```

-pshost *host_name*

Specifies the IP address or name of the Policy Server host system to which you are registering the Report Server.

-client *client_name*

Specifies the client name. The client name identifies the Report Server 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 CA SiteMinder® when using the XPSRegClient utility, enter CA SiteMinder®.

-psport *portnum*

(optional) Specifies the port on which the Policy Server is listening for the registration request.

fipsmode

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.

Chapter 5: Troubleshoot a SiteMinder Key Database Migration

Status of CA SiteMinder® Key Database Migration Unknown

Symptom:

I know that a Policy Server was upgraded. However, I am not sure that the smkeydatabase migration to the certificate data store was successful.

Solution:

Use the smkeydatabase migration utility (smmigratecds) to verify that the migration was successful.

Note: The default location of this utility is *siteminder_home\bin*.

siteminder_home

Specifies the Policy Server installation path.

Follow these steps:

1. Log in to the Policy Server host system on which the smkeydatabase is collocated.
2. Do one of the following steps:

- (Windows) Open a command prompt and run the following command:

`smmigratecds.bat -isComplete`

`-isComplete`

Verifies that a previous migration succeeded.

- (UNIX) Open a shell and run the following command:

`smmigratecds.sh -isComplete`

If the migration was successful, a message states that the system has already been migrated. If the migration failed, a message states that the system must be migrated.

Certificate Data Store Error Appears

Symptom:

I received a message stating that the certificate data store is not configured.

Solution:

Follow these steps:

1. If you are upgrading from r6.x, [extend the policy store schema](#) (see page 35).
2. Log in to the Policy Server host system.
3. Run the following command:

```
XPSDDInstall CDSObjects.xdd
```

The policy store schema is extended to support the certificate data store.

4. Do one of the following steps:
 - (Windows) Open a command prompt and run the following command:
`smmigratecds.bat -validateInstall`
validateInstall
Verifies if the certificate data store is installed correctly.
 - (UNIX) Open a shell and run the following command:
`smmigratecds.sh -validateInstall`
If the certificate data store is configured correctly, a message states that the installation is valid. If the certificate data store installation failed, a message states that the installation is not valid.
5. Migrate the CA SiteMinder® key database manually.

More information:

[Migrate a CA SiteMinder® Key Database Manually](#) (see page 155)

Migration Failed Error Appears

Symptom:

I received a message stating that the smkeydatabase migration failed.

Solution:

The migration utility (smmigratecds) compared the contents of the smkeydatabase to the certificate data store and identified one or more data inconsistencies. An example of a data inconsistency is the same alias mapping to different certificates.

These inconsistencies prevented a successful migration.

Follow these steps:

1. Use the smkeydatabase migration log (smkeydatabaseMigration.log) to identify the problem.

The log is located in *siteminder_home\log*.

siteminder_home

Specifies the Policy Server installation path.

2. Access the smkeydatabase using the smkeytool utility with the access legacy key store flag (-accessLegacyKS).
3. Resolve the data inconsistencies that resulted in the failure.

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

4. Migrate the smkeydatabase manually.

Migrate a CA SiteMinder® Key Database Manually

Symptom:

I want to migrate smkeydatabase certificate data to the certificate data store manually.

Solution:

Use the smkeydatabase migration utility (smmigratecds).

Follow these steps:

1. Be sure that all smkeydatabase instances are [synchronized](#) (see page 47).
2. Log in to the Policy Server host system on which the smkeydatabase is collocated.

3. Do one of the following steps to verify that the certificate data store is configured correctly:

- (Windows) Open a command prompt and run the following command:

```
smmigratecds.bat -validateInstall
```

-validateInstall

Verifies that the certificate data store is installed correctly.

- (UNIX) Open a shell and run the following command:

```
smmigratecds.sh -validateInstall
```

4. Do one of the following steps to compare the contents of the smkeydatabase to the certificate data store. Comparing the contents identifies data inconsistencies that can prevent a successful migration:

- (Windows) Run the following command:

```
smmigratecds.bat -validate -log log_file
```

-validate

Compares the contents of the smkeydatabase to the certificate data store.

-log

Sends the validation results to a log.

log_file

Specifies the name of the log file and the location to which the utility sends it.

Example: -log "C:\Program Files\Sample\Logs"

- (UNIX) Run the following command:

```
smmigratecds.sh -validate -log log_file
```

5. (Optional) If data inconsistencies exist, use the log file to identify the problem.

6. Do one of the following steps to begin the migration:

- (Windows) Run the following command:

```
smmigratecds.bat -migrate -log log_file
```

-migrate

Migrates the smkeydatabase to the certificate data store.

-log

Sends the migration results to a log.

log_file

Specifies the name of the log file and the location to which the utility sends it.

Example: -log "C:\Program Files\Sample\Logs"

- (UNIX) Run the following command:

```
smmigratecds.sh -migrate -log log_file
```

7. (Optional) If the migration fails, use the log file to identify the cause.

Index

6

6.x Mixed Mode Support • 18

A

Administrative UI Protection with SiteMinder • 80
Administrative UI Upgrade Paths • 79
Administrator Authentication • 28
Advanced Password Services • 30, 82
After You Upgrade the Policy Server • 58
Analyze Your SiteMinder Environment • 13
Avoid Policy Store Corruption • 30, 82

B

Before You Upgrade • 48, 86, 100
Before You Upgrade an r12.x Web Agent • 95
Before You Upgrade r6.x Web Agents • 58

C

CA Technologies Product References • 3
Certificate Data Management • 29, 80
Certificate Data Store Error Appears • 154
Clustered Environment • 23
Common CA SiteMinder® Environments • 22
Common Key Store Deployment • 68, 106
Common Key Store Single Sign-on Requirements • 71, 109
Component Versions in this Guide • 9
Configure all Policy Servers to use the Key Store • 74, 112
Configure the Connection to the Policy Server • 146
Contact CA Technologies • 3
Create a Client Name and Passphrase • 148
Create the 12.52 Environment • 70, 109
Crystal Reports in 12.x • 27
Custom Agent Requirements • 60, 96
Custom Server-Side Code Requirements • 57, 94

D

Delete an Administrative UI Connection to the Policy Server • 143
Delete the Administrative UI Data Directory • 139
Delete the Previous Trusted Host • 147
Determine the Upgrade Path • 16

Disable Dynamic Agent Key Generation • 72, 111
Disable XML Signature Wrapping Checks Before a Policy Server Upgrade • 89
Documentation Changes • 4
Download the Policy Store Schema Files • 34

E

Enable the Advanced Authentication Server • 55
Ensure the Policy Server is Configured • 59, 95
Export the Agent Keys • 73, 111
Extend Policy Store Schema for Your Active Directory LDS Server • 36
Extend Policy Store Schema for Your CA Directory Server • 37
Extend the Policy Store Schema • 35
Extend the Policy Store Schema for Your Active Directory Server • 36
Extend the Policy Store Schema for Your IBM DB2 Server • 39
Extend the Policy Store Schema for Your IBM Tivoli Directory Server • 39
Extend the Policy Store Schema for Your Microsoft SQL Server • 45
Extend the Policy Store Schema for Your MySQL Server • 46
Extend the Policy Store Schema for Your Novell eDirectory Server • 40
Extend the Policy Store Schema for Your OpenLDAP Server • 41
Extend the Policy Store Schema for Your Oracle Internet Directory Server • 41
Extend the Policy Store Schema for Your Oracle Server • 46
Extend the Policy Store Schema for Your Red Hat Directory Server • 43
Extend the Policy Store Schema for Your Siemens DirX Server • 44
Extend the Policy Store Schema for Your Sun Java System Directory Server • 45

F

Federation Integration • 30, 81
FIPS 140-2 Migration Overview • 119
FIPS 140-2 Migration Requirements • 120

G

Gather Environment Information • 123
Gather Registration Information • 146, 151

H

How a Parallel Upgrade Works • 66, 105
How the r12.x Migration Works • 82
How the r6.x Migration Works • 31
How to Configure a Parallel Environment • 67, 105
How to Configure FIPS-only Mode • 136
How to Migrate from r12.x • 85
How to Migrate from r6.x • 34
How to Plan a Migration • 12
How to Plan a Parallel Upgrade • 20
How to Re-Encrypt Existing Sensitive Data • 122
How to Re-Register an Administrative UI Configured for External Authentication • 143
How to Re-Register an Administrative UI Configured for Internal Authentication • 138
How to Re-Register the Report Server Connection • 148
How to Separate a Key Store from a Policy Store • 71, 110
How to Upgrade an r12.x Policy Store • 96
How to Upgrade an r6.x Policy Store • 61
How to Upgrade Simple Test Environments • 21

I

Identify the Required Administrator and Policy Server Object Names • 59, 95
Identify the Web Agent Requirements • 59, 95
Import the Agent Keys • 73, 112
Import the Default Policy Store Objects • 63, 98
Import the Policy Store Data Definitions • 62, 97
Install the Administrative User Interface • 65

K

Korn Shell (ksh) Package Required on Linux • 51

L

Limitations of a 6.x Mixed Environment • 19
Limitations of an r12.x Mixed Environment • 20

M

Make the legacy federation Objects Available in the Administrative UI • 64

Migrate a CA SiteMinder® Key Database Manually • 155

Migrate Keys and Certificates • 75, 114

Migrate the Assertion Issuer ID • 77, 116

Migrate the r12.x Policies • 116

Migrate the r6.x Policies • 78

Migration • 10

Migration Considerations • 27, 79

Migration Failed Error Appears • 155

Migration Roadmap—Configure FIPS-Only Mode • 135

Migration Roadmap—Re-Encrypt Sensitive Data • 120

Mixed SiteMinder Environments • 17

Multiple Key Store Deployment • 69, 107

Multiple Key Store Single Sign-on Requirements • 75, 114

O

Options for Re-encrypting Policy and Key Store Data • 129

Options for Upgrading a Key Store • 61

Options for Upgrading a Policy Store • 60

P

Parallel Environment Key Management Options • 67, 106

Parallel Upgrade • 11

Plan a Recovery Strategy • 15

Planning an Upgrade • 9

Policy Server Option Pack Support • 27

Policy Server Upgrade Creates a New JVMOptions File • 94

Policy Server Upgrade Creates New Files • 56

R

r12.x Mixed Mode Support • 19

Re-enable Dynamic Agent Key Generation • 74, 113

Re-encrypt a Policy Store Key • 125

Re-encrypt Client Shared Secrets • 127

Re-encrypt Keys Stored in the Policy or Key Store • 130

Re-encrypt Policy and Key Store Data • 129

Re-encrypt the CA SiteMinder® Super User Password • 126

Re-Encrypt the Policy Store Administrator Password • 126

Re-encrypt the Policy Store Data • 132

Register the Administrative UI • 142
Register the Report Server with the Policy Server • 151
Required Linux Libraries • 49, 87, 100
Reset the Administrative UI Registration Window • 140
Review the Policy Server Release Notes • 13
Run the Registration Tool • 143
Run the XPS Sweeper Utility • 99

S

Set a Policy Server to FIPS-Migration Mode • 123
Set an Agent to FIPS-Migration Mode • 127
Set an Agent to FIPS-only Mode • 137
Set the Policy Server to FIPS-only Mode • 137
Shared User Directory Environment • 24
Single Policy Store, Multiple Policy Servers and Web Agents • 22
Single Sign-on • 30, 80
Start all Policy Servers • 64, 99
Start the Application Server • 142
Status of CA SiteMinder® Key Database Migration Unknown • 153
Stop all Policy Servers • 62, 97
Stop the Application Server • 139
Synchronize Key Database Instances • 47, 85

T

Troubleshoot a Policy Server Upgrade • 57, 94
Troubleshoot a SiteMinder Key Database Migration • 153

U

UNIX Console • 54
UNIX GUI • 52
Upgrade a Policy Server on UNIX Using a Console • 92
Upgrade a Policy Server on Windows • 90
Upgrade a Policy Server Using a GUI on UNIX • 91
Upgrade an r12.x Administrative UI • 99
Upgrade an r12.x Policy Server • 86
Upgrade an r12.x Report Server • 104
Upgrade an r12.x Web Agent • 94, 95
Upgrade an r6.x Audit Log Database • 65
Upgrade an r6.x Policy Server • 48
Upgrade an r6.x Policy Store • 60
Upgrade an r6.x Session Store • 65
Upgrade an r6.x Web Agent • 58, 59

Upgrade Paths • 10
Upgrade the Administrative UI on UNIX • 102
Upgrade the Administrative UI on Windows • 102
Upgrading from r12.x • 79
Upgrading from r6.x • 27
Use Mixed-Mode Support • 18
Use smreghost to Re-encrypt a Shared Secret • 128
Use the Administrative UI to Re-encrypt a Shared Secret • 128
User Directory Single Sign on Requirements • 117
User Directory Single Sign-on Requirements • 78
Using FIPS-Compliant Algorithms • 119

V

Verify That Existing Federated SAML Partnerships Do Not Have the Same Backchannel Username • 89
Verify that Password Blobs are Re-encrypted • 134

W

Windows • 51