# CA SOA Security Manager

## Upgrade Guide

r12.1

# CA Product References

This document references the following CA products:

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

# Contact CA

**Contact Technical Support**

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

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

**Provide Feedback**

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

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

# Contents

# Chapter 1: Planning Migration and Upgrades

This section contains the following topics:



## How to Distinguish Between Migration and Upgrade

There are differences between an upgrade and a migration of a SOA Security Manager environment. An upgrade typically consists of a step-by-step operation that you perform on individual SOA Security Manager components, such as Policy Servers or SOA Agents. During an upgrade, you must take the component you are upgrading offline, perform the upgrade, then bring it back online again. The component is unavailable to the others during an upgrade.

A migration is a sequence of upgrades that you perform over an extended period of time, while maintaining overall system availability. The key to migration is proper planning. To minimize problems, develop a migration plan before starting a migration.

The migration plan should include the following:

- List the order that you plan to upgrade each SOA Security Manager component (Policy Servers, SOA Agents, and SOA Security Gateways).
- Identify the Windows or UNIX systems hardware where you plan to install each SOA Security Manager component.
- Implement a recovery plan that lets you return to your original configuration if the upgrade fails since you cannot undo a migration or upgrade. Thus, you must back up your entire environment before beginning the migration.
- Decide where you will store exported policy store data files for safekeeping and avoid overwriting or misplacing these files.
- Decide where you will import old policy store data.

- Create a non-production environment where you can perform a test migration to become familiar with the steps necessary to later migrate a production environment. Migrating a non-production environment allows you to troubleshoot any migration issues so you do not have to bring down mission-critical resources.
- Develop a strategy to test the performance of each SOA Security Manager component.

## Policy Server and Policy Store Versions in this Guide

This guide details the considerations and migration paths for upgrading your Policy Server and policy store from SOA Security Manager r12 to r12.1.

**Note:** The SOA Security Manager r12 Policy Server is an extended version of the SiteMinder 6.0 SP5 Policy Server. The SOA Security Manager r12.1 Policy Server is an extended version of the SiteMinder r12 SP1 Policy Server.

## How to Plan a Migration Strategy

In a complex SOA Security Manager environment, migrating to r12.1 can involve many upgrades before the migration is complete. Implementing a migration strategy is critical so that upgrades are completed efficiently, without exposing sensitive resources to security risks or down–time.

Consider the following when planning a migration strategy:

- Site analysis
  - What is the current state of your SOA Security Manager environment and when is the best time to upgrade each site in your environment?
  - Does SOA Security Manager r12.1 support the operating systems, directory servers, and databases in your SOA Security Manager environment?
- Recovery plan

  Have you created a back–up of your SOA Security Manager environment in case there are upgrade problems?
- Upgrade plan

  Have you determined the order in which to upgrade components?

## Analyze Your SOA Security Manager Environment

Analyze your SOA Security Manager environment to determine the complexity of your upgrade. Do this by answering the following questions:

| Question | Recommendation |
|---|---|
| How many Policy Server and Agents are in your environment? | Use the Policy Server audit logs to determine the number. |
| Which Policy Servers are communicating with which SOA 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 and application server logs and the Policy Server audit logs. |
| What third party software do you use that may require upgrading to work with SOA Security Manager r12.1, such as operating systems, database software, directory servers? | Go to the Technical Support site and search for the SOA Security Manager Platform Matrix for r12.1. |
| Do you have SOA Security Manager software customized by Professional Services? | Contact Customer Support for instructions. |
| Do you have access to SOA Security Manager r12 user documentation? You may need to refer to procedures in these documents. | Go to the Technical Support site and locate the SOA Security Manager documentation. |
| Do you have any customized files that may be overwritten by the upgrade? | Back up configured files, such as Host configuration files before upgrading. |

**To locate the support matrix from the Support site**

1. Click Technical Support.
2. Click Support By Product or Solution.
3. Select CA SOA Security Manager from the Select a Product or Solution Page list.

Click Platform Support Matrices in the Product Status group box.

## Plan a Recovery Strategy

You should implement a recovery plan that lets you return to your original configuration if the upgrade fails. You cannot undo a migration or upgrade and should back up your entire environment before beginning a migration.

**Important!** The most complete recovery plan is to back up each machine's entire image, which includes Policy Servers and SOA Agents. We recommend this method.

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

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

  If you intend to manage Agents centrally from a r12.1 Policy Server, you need to supply the Agent configuration file to the Policy Server administrator. The Administrator will need this file to create an Agent Configuration Object, which defines the Agent's configuration at the Policy Server.

  **Note:** More information on centrally managing SOA Agents exists in the *Policy Configuration Guide*.
- Export the policy store in clear-text to a file using the smobjexport tool.

  Exporting the policy store in clear-text provides you with a record of encrypted information, such as shared secrets. This information may also be used to troubleshoot problems. If your key store resides in the policy store, use the -k option with smobjexport since to ensure keys are included with the exported information.

  **Note:** If the r12.1 Policy Server uses the same encryption key as the SOA Security Manager R12 Policy Server, you do not need to export the data stores in clear-text. Using clear-text is necessary only if the old and new Policy Servers use different encryption keys.

  **Important!** Ensure you are using the appropriate SiteMinder 6.0 SP5 version of smobjexport when exporting policy store data.
- Copy the r12.0 installation scripts, hot fixes, and service packs so you can re-install if necessary. You can download copies from the Technical Support site.

# 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.

A test environment may not require the latter, in which case the most efficient way to upgrade is:

1. Install a r12.1 Policy Server.

   **Note:** Ensure that you install a new Policy Server and do not upgrade the existing Policy Server. More information on installing a Policy Server exists in the *Policy Server Installation Guide*.

2. Export the r12.0 policy store using the SiteMinder r6.0 SP5 version of smobjexport.

   **Note:** More information on using the SiteMinder version of smobjexport exists the respective version of the *Policy Server Installation Guide*.

3. Import the policy store data into a r12.1 policy store.

   **Note:** More information on creating a r12.1 policy store exists in the *Policy Server Installation Guide*.

4. Uninstall SOA Security Manager r12.

# Chapter 2: Upgrading from r12

This section contains the following topics:



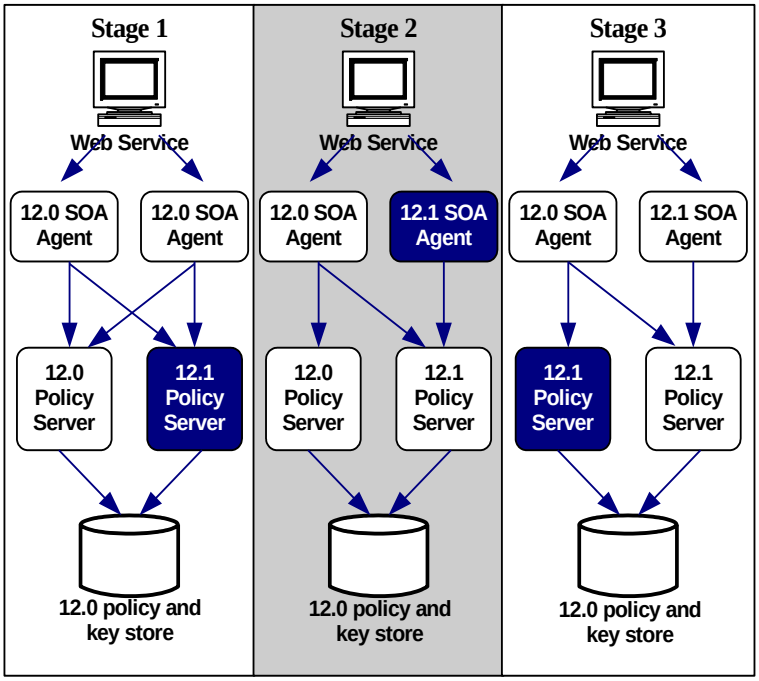
## Important Considerations

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

# How the Migration Works

The following figures represent an r12.0 environment and detail the order in which each component is upgraded to r12.1. The first figure represents stages one, two, and three of the migration. The second figure represents stages four and five of the migration.

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



1. In stage one, some of the r12.0 Policy Servers are upgraded to r12.1. The r12.1 Policy Server operates in compatibility mode.

   **Important!** The Policy Server installer replaces the Policy Server User Interface with the Federation Security Services Administrative UI during the upgrade. The r12.1 Policy Server continues to provide access control and generates log files that contain auditing information. However, you cannot administer the r12.1 Policy Server to record policy configuration information in the policy store until the Administrative UI is installed.

   **Note:** The Federation Security Services Administrative UI is for managing Federation Security Services and is required only if you use WS-Security SAML tokens. Although installed with the Policy Server, the Federation Security Services must be registered with the Policy Server before it may be used. You use the Administrative UI to register the Federation Security Services Administrative UI.

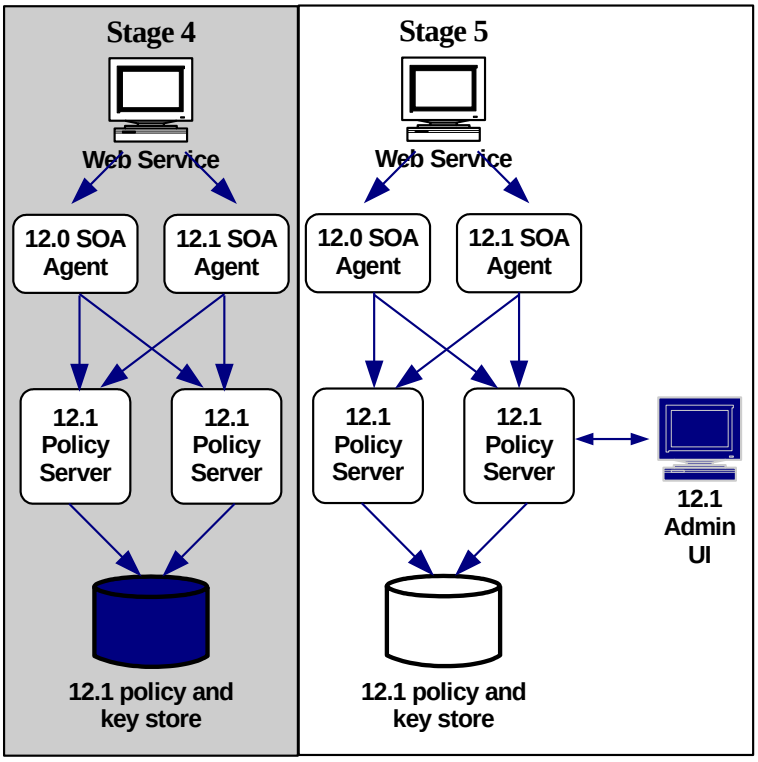
   - The r12.0 SOA Agents continue to communicate with the r12.1 Policy Server.
   - The r12.1 Policy Server continues to communicate with the r12.0 policy and key store.
   - The r12.0 Policy Server continues to communicate with the r12.0 policy and key store. You can continue to administer the r12.0 Policy Server to record policy configuration information using the r12.0 Policy Server User Interface.

   **Important!** If you are using WS-Security SAML tokens, the existing SOA Security Manager key database (smkeydatabase) must be upgraded to r12.1 or the existing keys and certificates must be migrated to an r12.1 SOA Security Manager key database. A r12.1 Policy Server can only communicate with a r12.1 key database. The SOA Security Manager installer lets you upgrade an existing key database to r12.1 or create a r12.1 key database during the Policy Server upgrade.

2. In stage two, some of the r12.0 SOA Agents are upgraded to r12.1.
   - The r12.0 SOA Agent continues to communicate with the r12.0 and the r12.1 Policy Servers.
   - The r12.1 SOA Agent only communicates with the r12.1 Policy Server.

3. In stage three, the remaining Policy Server is upgraded to r12.1. The r12.1 Policy Servers operate in compatibility mode with the r12.0 policy and key store.

   **Important!** Although the Policy Servers continue to protect resources and you have access to the Policy Server Management Console, you cannot administer the Policy Servers. The Policy Server installer replaced the Policy Server User Interface with the Federation Security Services Administrative UI during the upgrade. You cannot record policy information in the policy store until you have installed the r12.1 Administrative UI. Account for this time as you plan your migration.




4. In stage four, the r12.0 policy and key store is upgraded to r12.1.

5. In stage five, the Administrative UI is installed and configured with one or more Policy Servers. Consider the following:
   - You can install the Administrative UI before upgrading the policy store. However, you cannot register the Administrative UI until the policy store is upgraded. Installing the Administrative UI before the policy store upgrade minimizes the amount of time the Administrative UI is unavailable to the policy store.
   - Stage 5 contains r12.0 components to illustrate mixed-mode compatibility. You may upgrade remaining r12.0 components at this time.
6. The final step, which is not illustrated, is to register each Federation Security Services Administrative UI with its respective Policy Server, if required. The Federation Security Services Administrative UI is registered using the Administrative UI.

# How to Migrate from r12.0

Migrating from r12.0 to r12.1 requires that you complete the following procedures:

1. Review the sections in Before You Upgrade the Policy Server.
2. Upgrade an r12.0 Policy Server to r12.1. If you have one or more SOA Security Gateways, upgrade the Policy Server that hosts the SOA Security Gateway Configuration Manager first.

   **Note:** The Policy Server installer replaces the Policy Server User Interface with the Federation Security Services Administrative UI during the upgrade. The r12.1 Policy Server continues to provide access control and generates log files that contain auditing information. However, you cannot administer the r12.1 Policy Server to record policy configuration information in the policy store until the Administrative UI is installed.

   **Important!** If you are using WS-Security SAML tokens, the existing SOA Security Manager key database (smkeydatabase) must be upgraded to r12.1 or the existing keys and certificates must be migrated to an r12.1 SOA Security Manager key database. A r12.1 Policy Server can only communicate with a r12.1 key database. The SOA Security Manager installer lets you upgrade an existing key database to r12.1 or create a r12.1 key database during the Policy Server upgrade.
3. Review After You Upgrade the Policy Server (see page 27).
4. Upgrade an r12.0 SOA Agent or SOA Security Gateway to r12.1.

5. Upgrade the remaining r12.0 Policy Servers, SOA Agents, and SOA Security Gateways to r12.1, respectively.

   **Important!** Although the Policy Servers continue to protect resources and you have access to the Policy Server Management Console, you cannot administer the Policy Servers. The Policy Server installer replaced the Policy Server User Interface with the Federation Security Services Administrative UI during the upgrade. You cannot record policy information in the policy store until you have installed the r12.1 Administrative UI. Account for this time as you plan your migration.

6. Upgrade the r12.0 policy and key stores to r12.1
7. Install the r12.1 Administrative UI.
8. (Optional) If required, register each Federation Security Services Administrative UI with its respective Policy Server.

## Upgrade an r12.0 Policy Server

Upgrading an r12.0 Policy Server in the environment is the first step in the migration process.

### Before You Upgrade the Policy Server

Consider the following before you upgrade a Policy Server:

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

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

- Uninstall the Data Direct drivers.

  **Note:** This step only applies if your SOA Security Manager environment contains an RDB data store.

- Record Oracle/SQL data sources and recreate them.
- Remove the Policy Server being upgraded from your environment.
- Install the documentation.

### Uninstall the Data Direct Drivers

If your SOA Security Manager environment contains an ODBC data store, uninstall the Data Direct drivers.

**Note:** The Policy Server installer installs the latest version of the Data Direct drivers.

## Keep Track of Oracle/SQL Data Sources Then Recreate Them

This section only applies if the policy store you are upgrading resides in an Oracle or SQL Server database.

**Windows Systems**

The r12.1 Policy Server upgrade program deletes existing SOA Security Manager SQL Server/Oracle drivers and install new ones, which means you need to keep track of your existing SOA Security Manager data source connection settings before deleting the old data sources.

After upgrading, manually create new r12.1 SOA Security Manager data sources with these settings using the ODBC Data Source Administrator dialog box.

**Note:** For more information on creating new SOA Security Manager r12.1 data sources, see the *Policy Server Installation Guide*.

**Important!** If you do not delete the existing data sources prior to installing the r12.1 Policy Server, you cannot remove them after you upgrade because the upgrade program deletes the existing drivers. Thus, the Policy Server will then not be able to find the data sources.

**To keep track of the older data source settings and then delete the data sources**

1. Open the ODBC Data Source Administrator dialog box by selecting Programs, Administrative Tools, Data Sources (ODBC).
2. Click the System DN tab.
3. Make a note of the data source connection settings for all the SOA Security Manager data sources by doing the following:
    a. Select a data source, for example, SOA Security Manager Data Source.
    b. Click Configure.
    c. Write down all the data source connection settings as you will need them to create a new r12.1 data source after upgrading.
    d. Click Cancel.
    e. Repeat these steps for every SOA Security Manager data source. For example, you may have the following data sources:
        - SOA Security Manager Data Source
        - SOA Security Manager Logs Data Source
        - SOA Security Manager Reports Data Source
        - SOA Security Manager Tokens Data Source

- SOA Security Manager Key Data Source
- SOA Security Manager Session Server Data Source

4. Delete all the SOA Security Manager data sources by selecting the source and clicking Remove.

After you delete the data source, install the r12.1 Policy Server and create a new data source.

**Note:** For instructions on creating a new data source, see the *Policy Server Installation Guide*.

**UNIX Systems**

The system_odbc.ini file contains ODBC data source information for SOA Security Manager data stores in Oracle or SQL Server. When upgrading the Policy Server to r12.1, the upgrade program backs up your existing system_odbc.ini file by renaming it to system_odbc.ini<*PID_of_Upgrade*>.

**PID_of_Upgrade**

Defines the upgrade program's process ID.

**Example**: system_odbc.ini8957

After installing the Policy Server, you need to configure a new ODBC data source.

**To configure a new UNIX data source**

1. Go to *NETE_PS_ROOT*/db.

   **NETE_PS_ROOT**

   Defines the SOA Security Manager installation directory.

   **Example**: /export/smuser/siteminder

2. Create a new system_odbc.ini file by renaming oraclewire.ini or sqlserverwire.ini to system_odbc.ini.
3. Replace all occurrences of the string "nete_ps_root" with the explicit path of the SOA Security Manager installation directory.

4. For SQL Server, change the following values. These values need to be changed for all the data source names (SOA Security Manager Tokens Data Source, SOA Security Manager Logs Data Source, SOA Security Manager Session Data Source, etc.)

   [SiteMinder Data Source]
   Driver=nete_ps_root/odbc/lib/NSmsss19.so
   Description=DataDirect 4.2 SQL Server Wire Protocol
   Database=Siteminder Data
   Address=myhost, 1433
   QuotedId=No
   AnsiNPW=No

5. Save the file.

**Note:** For more information on creating a data source, see the *Policy Server Installation Guide*.

## Remove the Policy Server Being Upgraded from Your Environment

To prevent SOA Agents from contacting a Policy Server being upgraded, remove the Policy Server from your SOA Security Manager environment.

In addition, before running the Policy Server upgrade program, shut down all instances of the Policy Server Management Console.

## Upgrade an 12.0 Policy Server on Windows

You run the SOA Security Manager installer (ca-soasm-12.1-cr001-win32.exe) to upgrade the Policy Server. The executable can be downloaded from the Technical Support site.

**To locate installation kits on the Support site**

1. Click Technical Support.
2. Log into CA Support Online.
3. Click Download Center.

Search the Download Center for the installation kit you need.

**Note:** Before installing the Policy Server, ensure that the system meets the windows requirements.

**To upgrade the Policy Server**

1. Exit all applications that are running.
2. Navigate to where the installation executable is located.

3. Double-click ca-soasm-12.1-cr001-win32.exe.

   The SOA Security Manager installation wizard starts.

4. Considering the following when running the installer:

   - When prompted to select features to install, select CA SOA Security Manager Policy Server.
   - When prompted to select the components you want configured:
     - You must reconfigure components that had been previously configured for the environment. Ensure the respective check boxes are selected.
     - If you do not intend on configuring a new policy store, clear the Policy Store check box. You do not have to reconfigure existing policy store settings. The upgraded Policy Server retains the policy store settings. You manually upgrade an existing policy store.
     - If you plan on using WS-Security SAML tokens, ensure that the Create SM Key Database/Change SM Key Database Password option is selected.
   - If you selected the Create SM Key Database/Change SM Key Database Password check box:
     - Create a r12.1 smkeydatabase if you intend on migrating your existing smkeydatabase data into this repository.
     - Change the password if you intend on upgrading an existing smkeydatabase. Changing the password re-encrypts the database password and existing encrypted data using FIPS-compliant algorithms.
   - If you cut and paste path information into the wizard, you must also enter a character before the Next button is enabled.

5. Review the installation settings and click Install.

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

   **Note:** The Federation Security Services Administrative UI is installed during the Policy Server upgrade. The Federation Security Services Administrative UI is for managing Federation Security Services and is required only if using WS-Security SAML tokens. If you need it, register the Federation Security Services Administrative UI with the Policy Sever after upgrading the policy store. More information on registering the Federation Security Services Administrative UI exists the in *Policy Server Installation Guide*.

If you experience problems during the installation, you can locate the CA_SOA_Security_Manager_r12.1_InstallLog.log file in *soa_home*\install_config_info

You can also use the ca-ps-details.log file located in *soa_home*\siteminder\install_config_info to check the status of the installer's auto-configuration of an ADAM or Sun Java System Directory Server policy store.

***soa_home***

Specifies the path to where the SOA Security Manager is installed.

## Upgrade an r12.0 Policy Server on UNIX

You run the respective UNIX Policy Server installation executable to upgrade the Policy Server. The installation executables are in the SOA Security Manager kit available on the Technical Support site. They are the following:

- **Solaris**—ca-soasm-12.1-cr001-sol.bin
- **Red Hat Linux**—ca-soasm-12.1-cr001-linux.bin

**To locate installation kits on the Support site**

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

**Note:** Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

If you do not have sufficient rights, add executable permission to the install file by running the following command:

chmod+x ca-soasm-12.1-cr001-*os_version*.bin

***os_version***

Specifies sol or linux.

**Important!** If you execute the SOA Security Manager installer across different subnets it can crash. To avoid this problem, install the Policy Server directly on the host system.

**To locate installation kits on the Support site**

1. Click Technical Support.
2. Log into CA Support Online.

3. Click Download Center.
4. Search the Download Center for the installation kit you need.

**To upgrade the Policy Server**

1. Exit all applications that are running.
2. Execute the following script in a ksh shell from the *soa_home*/siteminder directory:

   ../ca_ps_env.ksh

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

   ***soa_home***

   Specifies the path to where the SOA Security Manager is installed.
3. Open a command window and navigate to where the install program is located.
4. Enter the following command:
5. Enter the following command in a UNIX shell:

   sh ./ca-soasm-12.1-cr001-*os_version*.bin

   **Example:** sh ./ca-soasm-12.1-cr001-sol.bin

   The SOA Security Manager installation wizard starts.

6. Consider the following when running the installer:
   - When prompted to select features to install, select CA SOA Security Manager Policy Server.
   - When prompted to select the components you want configured:
     - You must reconfigure components that had been previously configured for the environment. Ensure the respective check boxes are selected.
     - If you plan on using WS-Security SAML tokens, ensure that the Create SM Key Database/Change SM Key Database Password option is selected.
     - If you do not intend on configuring a new policy store, clear the Policy Store check box. You do not have to reconfigure existing policy store settings. The upgraded Policy Server retains the policy store settings. You manually upgrade an existing policy store.
   - If you selected the Create SM Key Database/Change SM Key Database Password check box:
     - Create a r12.1 smkeydatabase if you intend on migrating your existing smkeydatabase data into this repository.
     - Change the password if you intend on upgrading an existing smkeydatabase. Changing the password re-encrypts the database password and existing encrypted data using FIPS-compliant algorithms.
   - If you cut and paste path information into the wizard, you must also enter a character before the Next button is enabled.
7. Review the installation settings and click Install.

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

   **Note:** This may take several minutes.
8. Click Done and reboot the system.

   The Policy Server is upgraded.

   **Note:** The Federation Security Services Administrative UI is installed during the Policy Server upgrade. The Federation Security Services Administrative UI is for managing Federation Security Services and is required only if using WS-Security SAML tokens. If you need it, register the Federation Security Services Administrative UI with the Policy Sever after upgrading the policy store. More information on registering the Federation Security Services Administrative UI exists the in *Policy Server Installation Guide*.

If you experience problems during an installation or upgrade, you can locate the CA_SOA_Security_Manager_r12.1_InstallLog.log file in *soa_home*/install_config_info/

You can also refer to the ca-ps-details.log file located in *soa_home*/siteminder/install_config_info to check the status of the installer's auto-configuration of an ADAM or Sun Java System Directory Server policy store.

***soa_home***

Specifies the path to where SOA Security Manager is installed.

## Run the SOA Security Gateway Configuration Upgrade Utility on Windows

The SOA Security Gateway configuration upgrade utility takes an existing r12.0 Entity Store configuration file (entities.xml) and upgrades it for use with the r12.1 SOA Security Gateway.

**To run the Configuration Upgrade Utility on Windows**

1. Start the r12.0 SOA Security Gateway Configuration Manager and SOA Security Gateway (in that order) from their renamed install directories:
   a. Open a command prompt window.
   b. Navigate to the renamed r12.0 SOA Security Gateway Configuration Manager bin directory, *SOA_HOME*\SOASecurityGatewayCM.backup\win32\bin.
   c. Run the Configuration Manager startup script:

      soagatewayconfigmanager.bat

   d. Open another command prompt window.
   e. Navigate to the renamed r12.0 SOA Security Gateway bin directory, *SOA_HOME*\SOASecurityGateway.backup\win32\bin.
   f. Run the SOA Security Gateway startup script:

      soagateway.bat

2. Open a command prompt window and navigate to *SOA_HOME*\SOASecurityGateway\upgrade\win32.
3. Run the configuration upgrade utility:

   upgradeconfig.bat

4. When prompted to enter the location of the installation to upgrade, hit Enter to search for the renamed r12.0 SOA Security Gateway.

   The Update Utility searches for and displays a numbered list of possible r12.0 install directories.

5. When prompted to select the install to upgrade, type the numerical entry corresponding to the renamed r12.0 SOA Security Gateway install directory and hit Enter. For example, if the backup directory for the r12.0 SOA Security Gateway (C:\Program Files\CA\SOA Security Manager\SOASecurityGateway.backup by default) is listed as the second entry, type "2".
6. When asked whether you want to upgrade the configuration at http:localhost:8090/configuration/policies, type "y" and hit Enter.
7. When asked whether you want to push the configuration back to the originating SOA Security Gateway Configuration Manager, type "n" and hit Enter.
8. When prompted to enter a location for the newly upgraded entities-upgraded.xml file, hit Enter to accept the default (SOA_HOME\SOASecurityGateway\upgrade\win32).
9. When prompted to enter the host name, hit Enter to accept the default (localhost).
10. When prompted to enter the process name, hit Enter to accept the default value (SOA Security Gateway).
11. When prompted to enter the configuration service host name, hit Enter to accept the default value (locallhost).
12. When Prompted to enter the configuration service process name, hit Enter to accept the default value (SOA Security Gateway Configuration Manager).

    The upgrade proceeds. If successful, the upgraded Entity Store configuration file (entities-upgraded.xml) is created in the current directory.
13. Stop the r12.0 SOA Security Gateway and SOA Security Gateway Configuration Manager.

## 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 r12.0 SOA Agents and SOA Security Gateways

Upgrading the SOA Agents and SOA Security Gateways in the environment is the second step in the migration process. You can upgrade the SOA Agents and SOA Security Gateways in your environment in any order.

**Note:** SOA Security Manager r12 SOA Agents and SOA Security Gateways can communicate with a r12.1 Policy Server. Therefore, you can upgrade your Policy Server to r12.1 before upgrading SOA agents and SOA Security Gateways while continuing to protect resources.

## How to Prepare for a SOA Agent for Web Servers Upgrade

**Note:** Because the SOA Agent for Web Servers is an XML-enabled version of the CA SiteMinder Web Agent, you must perform all the procedures that are required to prepare for a Web Agent installation or upgrade before installing or upgrading the SOA Agent software.

You can prepare for upgrading a SOA Agent for Web Servers using the following process:

- Back up the Web Agent Option Pack (WAOP) configuration files and uninstall the WAOP.

  **Note:** More information on uninstalling the WAOP exists in the *Web Agent Option Pack Guide*.Back up any customized files on your web server.
- Ensure the Policy Server is Configured
- Identify the Required Administrator and Policy Server Object Names
- Review the changes to the various Web Agent configuration files that occur when you run the Web Agent Configuration wizard *after* an upgrade.
- Set the LD_PRELOAD variable to avoid conflicts with existing Web Agents.
- Replace existing read-only files during the upgrade (if prompted).

**Note:** If you have upgraded the web server itself since you last installed the Web Agent, the Agent upgrade may not work. The upgrade is ensured only if the web server version has remained the same since the last Web Agent installation.

## 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 SOA Security Manager Administrator allowed to register hosts.
- Name of the Host Configuration Object.
- Name of the Agent Configuration Object.

### Back Up Customized Files

Customized files may be overwritten by the upgrade. Back up configured files, such as Agent and Host configuration files *before* upgrading.

### Ensure LD_PRELOAD Variable Does Not Conflict with Existing Agent

If you are upgrading or reinstalling a Web Agent on a Linux system, from the shell, set the LD_PRELOAD variable so that it points to a different location from any existing Web Agent installation directory. For example, if an existing LD_PRELOAD entry is set to:

LD_PRELOAD=*web_agent_home*/bin/libbtunicode.so

Before you reinstall or upgrade, set the variable to:

export LD_PRELOAD=

This entry sets the variable to a blank value.

### Replace Existing Read-only Files

When you upgrade a Web Agent, you may see messages asking whether you want to replace read-only files. Select Yes to all.

### Upgrade a SOA Agent to r12.1 on Windows

The SOA Security Manager installer can upgrade existing SOA Agents to r12.1. The kit that contains the installer can be downloaded from the Technical Support site.

**To locate installation kits on the Support site**

1. Click Technical Support.
2. Log into CA Support Online.

3. Click Download Center.

Search the Download Center for the installation kit you need.

**Note:** Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

Consider the following:

- If the installation program detects any locked Agent files, it prompts you to restart your system instead of reconfiguring it. Select whether to restart the system immediately or later.
- If you are installing an Agent on an Sun Java System web server, you may see an error message stating that the httpd.exe service is unable to locate the smconapi.dll. If this message appears, reboot your system before launching the Web Agent Configuration Wizard.

**To upgrade SOA Agents on Windows**

1. Exit all applications that are running and stop the web server.
2. Navigate to where the installation executable is located.
3. Double-click ca-soasm-12.1-cr001-win32.exe.

   The SOA Security Manager installation wizard starts.
4. Proceed through the wizard to upgrade the SOA Agent. Consider the following when running the installer:
   - When prompted to select features to install, select CA SOA Security Manager Agents and then specify the SOA Agent type you want to upgrade.
   - When the wizard prompts you to confirm the upgrade, select one of the following options:
     - Continue with the upgrade—upgrades the SOA Agent to r12.1.
     - Abort the upgrade—exits the upgrade procedure without upgrading the SOA Agent.
   - If the installation program detect that newer versions of certain system .dlls are installed on your system and prompts you to overwrite these newer files with older files, select the No To All option.

   The new SOA Agent files are copied to the specified location.
5. Choose whether to restart your system immediately or later.
6. Re-configure the upgraded SOA Agent with the SOA Security Manager Configuration Wizard.

   **Note:** You do not need to re-register your trusted host.

## Upgrade a SOA Agent to r12.1 on UNIX

The SOA Security Manager installer can upgrade existing SOA Agents to r12.1. The kit that contains the installer can be downloaded from the Technical Support site.

**Note:** if you have upgraded the web server associated with a SOA Agent for Web Servers since you last installed the SOA Agent, the Agent upgrade may not work. The upgrade is ensured only if the web server version has remained the same since the last SOA Agent installation. However, you can upgrade if you have applied a hotfix.

The installation executables are in the SOA Security Manager kit available on the Technical Support site. They are the following:

- **Solaris**—ca-soasm-12.1-cr001-sol.bin
- **Red Hat Linux**—ca-soasm-12.1-cr001-linux.bin

**To locate installation kits on the Support site**

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

**Note:** Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

If you do not have sufficient rights, add executable permission to the install file by running the following command:

chmod+x ca-soasm-12.1-cr001-*os_version*.bin

***os_version***

Specifies sol or linux.

**Important!** If you execute the SOA Security Manager installer across different subnets it can crash. To avoid this problem, install the Policy Server directly on the host system.

**Important!** Remove any 5.x Web Agent Option Packs before upgrading to r12.1. 6.x Web Agent Option Packs do not need to be removed before upgrading to r12.1. For more information about removing and reinstalling Web Agent Option Packs, see the SOA Security Manager Web Agent Option Pack Guide.

Consider the following:

- **I**f you have upgraded the web server associated with a SOA Agent for Web Servers since you last installed the SOA Agent, the Agent upgrade may not work. The upgrade is ensured only if the web server version has remained the same since the last SOA Agent installation. However, you can upgrade if you have applied a hotfix.
- If the installation program detects any locked Agent files, it prompts you to restart your system instead of reconfiguring it. Select whether to restart the system immediately or later.
- If you are upgrading an Agent on an Sun Java System web server, you may see an error message stating that the httpd.exe service is unable to locate the smconapi.dll. If this message appears, reboot your system before launching the Web Agent Configuration Wizard.

**To upgrade a SOA Agent on UNIX systems**

1. Exit all applications that are running and stop the web server.
2. Open a command window and navigate to where the install program is located.

3. Enter one of the following commands:

   **GUI mode**: sh./ca-soasm-12.1-cr001-*os_version*.bin

   **Console mode**: sh./ca-soasm-12.1-cr001-*os_version*.bin -i

   The SOA Security Manager installation wizard starts.

4. Proceed through the wizard to upgrade the SOA Agent. Consider the following when running the installer:

   - When prompted to select features to install, select CA SOA Security Manager Agents and then specify the SOA Agent types you want to upgrade.
   - When the wizard prompts you to confirm the upgrade, select one of the following option:
     - Continue with the upgrade—upgrades the SOA Agent to r12.1.
     - Abort the upgrade—exits the upgrade procedure without upgrading the SOA Agent.
   - If the installation program detect that newer versions of certain system .dlls are installed on your system and prompts you to overwrite these newer files with older files, select the No To All option.

   The new SOA Agent files are copied to the specified location.

5. Choose whether to restart your system immediately or later.
6. Re-configure the upgraded SOA agent with the SOA Security Manager Configuration Wizard.

   Note: You do not need to re-register your trusted host.

## Upgrade a SOA Security Gateway to r12.1 on Windows

In the SOA Security Manager r12.0 release, the SOA Security Gateway comprised the following three separately installable components:

- SOA Security Gateway
- SOA Security Gateway Configuration Manager
- SOA Security Gateway Management Console

In r12.1, the SOA Security Gateway installation comprises the following two components, which are installed together:

- SOA Security Gateway
- SOA Security Gateway Management Console

Because of this new component structure and a change to the Entity Store configuration, a number of steps are required to upgrade an existing SOA Security Gateway to r12.1.

**To upgrade an r12.0 SOA Security Gateway to r12.1 on Windows**

1. Stop r12.0 components and install the r12.1 SOA Security Gateway (see page 35)
2. Run the SOA Security Gateway configuration upgrade utility (see page 26)
3. Replace the r12.1 Entity Store configuration file with the upgraded r12.0 file produced by the configuration upgrade utility (see page 38)
4. Uninstall all r12.0 SOA Security Manager components (see page 38)

## Run the Installer to Install the r12.1 SOA Security Gateway

You run the SOA Security Manager installer (ca-soasm-12.1-cr001-win32.exe) to install the r12.1 SOA Security Gateway software. The kit that contains the installer can be downloaded from the Technical Support site.

**To locate installation kits on the Support site**

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

**Note:** Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

**To run the SOA Security Manager installer to install a SOA Security Gateway**

1. Stop all r12.0 SOA Security Gateway components and any other applications that are running.
2. Navigate to where the installation executable is located.
3. Double-click ca-soasm-12.1-cr001-win32.exe.

   The SOA Security Manager installation wizard starts.

4. Use gathered system and component information to install the SOA Security Gateway.Consider the following when running the installer:
   - When prompted to select features to install, select CA SOA Security Manager Agents and then specify the SOA Security Gateway as the agent type you require.
   - If you cut and paste path information into the wizard, you must also enter a character before the Next button is enabled.
5. Review the information on the Pre-Installation Summary page, then click Install.

   **Note:** The installation program may detect that newer versions of certain system dlls are installed on your system. It asks if you want to overwrite these newer files with older files. Select No To All if you see this message.

   The SOA Security Gateway r12.1 files are copied to the installed location of the r12.0 SOA Security Gateway. The original directories for each installed component are renamed with a ".backup" extension such that the installation directories for the three r12 SOA Security Gateway become SOASecurityGateway.backup, SOASecurityGatewayCM.backup, and SOASecurityGatewayMMC.backup, respectively.
6. Re-configure the upgraded SOA Security Gateway with the SOA Security Manager Configuration Wizard.

   **Note:** You do not need to re-register your trusted host.

After installation, you can review the installation log file in *SOA_HOME*\install_config_info. The file name is: CA_SOA_Security_Manager_r12.1_InstallLog.log

***soa_home***

Specifies the path to where SOA Security Manager is installed.

Default: C:\Program Files\CA\SOA Security Manager

## Run the SOA Security Gateway Configuration Upgrade Utility on Windows

The SOA Security Gateway configuration upgrade utility takes an existing r12.0 Entity Store configuration file (entities.xml) and upgrades it for use with the r12.1 SOA Security Gateway.

**To run the Configuration Upgrade Utility on Windows**

1. Start the r12.0 SOA Security Gateway Configuration Manager and SOA Security Gateway (in that order) from their renamed install directories:
   a. Open a command prompt window.
   b. Navigate to the renamed r12.0 SOA Security Gateway Configuration Manager bin directory, *SOA_HOME*\SOASecurityGatewayCM.backup\win32\bin.

c. Run the Configuration Manager startup script:

soagatewayconfigmanager.bat

d. Open another command prompt window.

e. Navigate to the renamed r12.0 SOA Security Gateway bin directory, *SOA_HOME*\SOASecurityGateway.backup\win32\bin.

f. Run the SOA Security Gateway startup script:

soagateway.bat

2. Open a command prompt window and navigate to *SOA_HOME*\SOASecurityGateway\upgrade\win32.
3. Run the configuration upgrade utility:

upgradeconfig.bat

4. When prompted to enter the location of the installation to upgrade, hit Enter to search for the renamed r12.0 SOA Security Gateway.

   The Update Utility searches for and displays a numbered list of possible r12.0 install directories.

5. When prompted to select the install to upgrade, type the numerical entry corresponding to the renamed r12.0 SOA Security Gateway install directory and hit Enter. For example, if the backup directory for the r12.0 SOA Security Gateway (C:\Program Files\CA\SOA Security Manager\SOASecurityGateway.backup by default) is listed as the second entry, type "2".
6. When asked whether you want to upgrade the configuration at http:localhost:8090/configuration/policies, type "y" and hit Enter.
7. When asked whether you want to push the configuration back to the originating SOA Security Gateway Configuration Manager, type "n" and hit Enter.
8. When prompted to enter a location for the newly upgraded entities-upgraded.xml file, hit Enter to accept the default (SOA_HOME\SOASecurityGateway\upgrade\win32).
9. When prompted to enter the host name, hit Enter to accept the default (localhost).
10. When prompted to enter the process name, hit Enter to accept the default value (SOA Security Gateway).
11. When prompted to enter the configuration service host name, hit Enter to accept the default value (locallhost).

12. When Prompted to enter the configuration service process name, hit Enter to accept the default value (SOA Security Gateway Configuration Manager).

    The upgrade proceeds. If successful, the upgraded Entity Store configuration file (entities-upgraded.xml) is created in the current directory.

13. Stop the r12.0 SOA Security Gateway and SOA Security Gateway Configuration Manager.

## Replace the r12.1 Entity Store Configuration File With the Upgraded r12.0 File

To configure the r12.1 SOA Security Gateway to use the upgraded r12.0 Entity Store configuration file created by the upgrade utility, you must rename and move it to replace the default r12.1 file.

**To replace the r12.1 Entity Store configuration file with the upgraded r12.0 file**

1. Navigate to *SOA_HOME*\SOASecurityGateway\conf
2. Rename the r12.1 entities.xml file to entities.backup (or similar) to preserve it in case of problems.
3. Copy the entities-upgraded.xml file created by the upgrade utility from *SOA_HOME*\SOASecurityGateway\upgrade\upgrade\win32 to *SOA_HOME*\SOASecurityGateway\conf.
4. Rename entities-upgraded.xml to entities.xml.
5. Start the r12.1 SOA Security Gateway (see the r12.1 *SOA Security Gateway Configuration Guide* for details) and check that it reflects the upgraded r12.0 configuration.

## Uninstall r12.0 SOA Security Gateway Components

After the r12.0 to r12.1 SOA Security Gateway upgrade is successful, you can uninstall all r12 components. See the r12.0 documentation for details.

## Upgrade a SOA Security Gateway to r12.1 on UNIX

In the SOA Security Manager r12.0 release, the SOA Security Gateway comprised the following three separately installable components:

- SOA Security Gateway
- SOA Security Gateway Configuration Manager
- SOA Security Gateway Management Console

In r12.1, the SOA Security Gateway installation comprises the following two components, which are installed together:

- SOA Security Gateway
- SOA Security Gateway Management Console

Because of this new component structure and a change to the Entity Store configuration, a number of steps are required to upgrade an existing SOA Security Gateway to r12.1.

**To upgrade an r12.0 SOA Security Gateway to r12.1 on UNIX**

1. Stop r12.0 components and install the r12.1 SOA Security Gateway (see page 39)
2. Run the SOA Security Gateway configuration upgrade utility (see page 41)
3. Replace the r12.1 Entity Store configuration file with the upgraded r12.0 file produced by the configuration upgrade utility (see page 42)
4. Uninstall all r12.0 SOA Security Manager components (see page 38)

## Run the Installer to Install the r12.1 SOA Security Gateway on UNIX

You run the respective UNIX installation executable to install the r12.1 SOA Security Gateway software. The installation executables are in the SOA Security Manager kit available on the Technical Support site. They are the following:

- **Solaris**—ca-soasm-12.1-cr001-sol.bin
- **Red Hat Linux**—ca-soasm-12.1-cr001-linux.bin

**To locate installation kits on the Support site**

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

**Note:** Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

If you do not have sufficient rights, add executable permission to the install file by running the following command:

chmod+x ca-soasm-12.1-cr001-*os_version*.bin

***os_version***

Specifies sol or linux.

**Important!** If you execute the SOA Security Manager installer across different subnets it can crash. To avoid this problem, install the Policy Server directly on the host system.

**To run the SOA Security Manager installer to install a SOA Security Gateway**

1. Stop all r12.0 SOA Security Gateway components and any other applications that are running.
2. Open a command window and navigate to where the install program is located.
3. Enter one of the following commands:

   **GUI mode**: sh./ca-soasm-12.1-cr001-*os_version*.bin

   **Console mode**: sh./ca-soasm-12.1-cr001-*os_version*.bin -i

   The SOA Security Manager installation wizard starts.
4. Use gathered system and component information to install the SOA Security Gateway.Consider the following when running the installer:

   - When prompted to select features to install, select CA SOA Security Manager Agents and then specify the SOA Security Gateway as the agent type you require.
   - (GUI mode) If you cut and paste path information into the wizard, you must also enter a character before the Next button is enabled.
5. Review the information on the Pre-Installation Summary page, then proceed.

   **Note:** The installation program may detect that newer versions of certain system dlls are installed on your system. It asks if you want to overwrite these newer files with older files. Select No To All if you see this message.

   The SOA Security Gateway r12.1 files are copied to the installed location of the r12.0 SOA Security Gateway. The original directories for each installed component are renamed with a ".backup" extension such that the installation directories for the three r12 SOA Security Gateway become SOASecurityGateway.backup, SOASecurityGatewayCM.backup, and SOASecurityGatewayMMC.backup, respectively.
6. Re-configure the upgraded SOA Security Gateway with the SOA Security Manager Configuration Wizard.

   **Note:** You do not need to re-register your trusted host.

After installation, you can review the installation log file in *SOA_HOME/*install_config_info. The file name is: CA_SOA_Security_Manager_r12.1_InstallLog.log

***soa_home***

Specifies the path to where SOA Security Manager is installed.

## Run the SOA Security Gateway Configuration Upgrade Utility on UNIX

The SOA Security Gateway configuration upgrade utility takes an existing r12.0 Entity Store configuration file (entities.xml) and upgrades it for use with the r12.1 SOA Security Gateway.

**To run the configuration upgrade utility on UNIX**

1. Start the r12.0 SOA Security Gateway Configuration Manager and SOA Security Gateway (in that order) from their renamed install directories:
   a. Open a command window.
   b. Navigate to the renamed r12.0 SOA Security Gateway Configuration Manager bin directory, *SOA_HOME*/SOASecurityGatewayCM.backup/posix/bin.
   c. Run the Configuration Manager startup script:

      soagatewayconfigmanager.sh

   d. Open another command prompt window.
   e. Navigate to the renamed r12.0 SOA Security Gateway bin directory, *SOA_HOME*/SOASecurityGateway.backup/posix/bin.
   f. Run the SOA Security Gateway startup script:

      soagateway.sh

2. Open a command prompt window and navigate to *SOA_HOME*/SOASecurityGateway/upgrade/posix.
3. Run the configuration upgrade script:

   upgradeconfig.sh

4. When prompted to enter the location of the installation to upgrade, hit Enter to search for the renamed r12.0 SOA Security Gateway.

   The Update Utility searches for and displays a numbered list of possible r12.0 install directories.

5. When prompted to select the install to upgrade, type the numerical entry corresponding to the renamed r12.0 SOA Security Gateway install directory and hit Enter. For example, if the backup directory for the r12.0 SOA Security Gateway (~/CA/SOA Security Manager/SOASecurityGateway.backup by default) is listed as the second entry, type “2”.
6. When asked whether you want to upgrade the configuration at http:localhost:8090/configuration/policies, type "y" and hit Enter.
7. When asked whether you want to push the configuration back to the originating SOA Security Gateway Configuration Manager, type "n" and hit Enter.

8. When prompted to enter a location for the newly upgraded entities-upgraded.xml file, hit Enter to accept the default (*SOA_HOME*/SOASecurityGateway/upgrade/posix).
9. When prompted to enter the host name, hit Enter to accept the default (localhost).
10. When prompted to enter the process name, hit Enter to accept the default value (SOA Security Gateway).
11. When prompted to enter the configuration service host name, hit Enter to accept the default value (locallhost).
12. When Prompted to enter the configuration service process name, hit Enter to accept the default value (SOA Security Gateway Configuration Manager).

    The upgrade proceeds. If successful, the upgraded Entity Store configuration file (entities-upgraded.xml) is created in the current directory.
13. Stop the r12.0 SOA Security Gateway and SOA Security Gateway Configuration Manager.

## Replace the r12.1 Entity Store Configuration File With the Upgraded r12.0 File

To configure the r12.1 SOA Security Gateway to use the upgraded r12.0 Entity Store configuration file created by the upgrade utility, you must rename and move it to replace the default r12.1 file.

**To replace the r12.1 Entity Store configuration file with the upgraded r12.0 file**

1. Navigate to *SOA_HOME*/SOASecurityGateway/conf
2. Rename the r12.1 entities.xml file to entities.backup (or similar) to preserve it in case of problems.
3. Copy the entities-upgraded.xml file created by the upgrade utility from *SOA_HOME*/SOASecurityGateway/upgrade/upgrade/*os_version* to *SOA_HOME*/SOASecurityGateway/conf.

   ***os_version***

   Specifies sol or rhel30.
4. Rename entities-upgraded.xml to entities.xml.
5. Start the r12.1 SOA Security Gateway (see the r12.1 *SOA Security Gateway Configuration Guide* for details) and check that it reflects the upgraded r12.0 configuration.

## Uninstall r12.0 SOA Security Gateway Components

After the r12.0 to r12.1 SOA Security Gateway upgrade is successful, you can uninstall all r12 components. See the r12.0 documentation for details.

## SOASM--Upgrade an r12.0 Policy Store

Upgrading some of the policy and key stores in the environment is the third step in the migration process.

The following sections detail how to upgrade 6.x policy and key stores to r12.1.

### Options for Upgrading a Policy Store

There are two possible policy store paths for the r12.1 migration. You can:

- Upgrade the existing policy and key store to r12.1.
- Create a new r12.1 policy and key store and import the existing policy and key store data into the new instance.

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

If you want to create a new r12.1 policy and key store:

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

   **Note:** More information on using the SiteMinder 6.x version of smobjimport required for use with SOA Security Manager r12.0 exists in the *SiteMinder Policy Server Installation Guide* for 6.x.

2. Create a r12.1 policy and key store.

   **Note:** More information on creating a r12.1 policy and key store exists in the *Policy Server Installation Guide*.

3. Import the policy and key store data into the r12.1 policy and key store using the r12.1 version of smobjimport.

   **Note:** More information on the r12.1 version of smobjimport exists in the *Policy Server Administration Guide*.

### How to Upgrade an r12.0 Policy Store

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

**To upgrade a supported LDAP or relational database policy store**

1. Extend the Policy Store Schema.

   **Note:** There is no change to the existing r12.0 policy store schema. The r12.1 migration requires that you upgrade the policy store schema to extend the policy store for objects required by r12.1.

2. Import the Base Policy Store Objects.

3. Import the Policy Store Data Definitions.

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

## Extend the Active Directory Policy Store Schema

You extend the policy store schema to store objects introduced by r12.1. The existing r6.x policy store schema has not changed.

**To extend the Active Directory policy store schema**

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

   ***policy_server_home***

   Specifies the Policy Server installation path.

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

   **Example:** dc=domain,dc=com

3. Navigate to *policy_server_home*/bin from a command window.
4. Run the following command:

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

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

## Extend the ADAM Policy Store Schema

You extend the policy store schema to store objects introduced by r12.1. The existing r6.x policy store schema has not changed.

**To extend the ADAM policy store schema**

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

   ***policy_server_home***

   Specifies the Policy Server installation path.

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

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

3. Navigate to *policy_server_home*/bin from a command window.
4. Run the following command:

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

   The policy store schema is extended for objects required by r12.1.

## Extend the CA Directory Policy Store Schema

You extend the policy store schema to store objects introduced by r12.1. The existing r6.x policy store schema has not changed.

**To extend the CA Directory policy store schema**

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

   etrust.dxc

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

   ***policy_server_home***

   Specifies the policy server installation path.

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

   - etrust_schema.txt
   - schema.txt

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

   ***policy_server_home***

   Specifies the Policy Server installation path.

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

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

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

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

   set ignore-name-bindings=true;
   ```

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

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

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

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

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

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

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

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

dxserver stop *DSA_Name*

dxserver start *DSA_Name*

***DSA_Name***

Specifies the name of the policy store DSA.

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

## Extend the Sun Java System Directory Server Policy Store Schema

You extend the policy store schema to store objects introduced by r12.1. The existing r6.x policy store schema has not changed.

**To extend the Sun Java System Directory Server policy store schema**

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

***policy_server_home***

Specifies the Policy Server installation path.

2. Run the following command:

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

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

## Extend the MS SQL Server Policy Store Schema

You extend the policy store schema to store objects introduced by r12.1. The existing r6.x policy store schema has not changed.

**To extend the Microsoft SQL Server policy store schema**

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

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

   ***policy_server_home***

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

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

## Extend the Oracle Policy Store Schema

You extend the policy store schema to store objects introduced by r12.1. The existing r6.x policy store schema has not changed.

**To extend the Oracle policy store schema**

1. Log into Oracle with sqlplus or some other Oracle utility as the user who administers the Policy Server database information.

   **Note:** We recommend that you do not create the SOA Security Manager schema with the SYS or SYSTEM users. If necessary, create an Oracle user, such as SMOWNER, and create the schema with that user.
2. Import the following r12.1 script into the 6.x database instance:

   $NETE_PS_ROOT/xps/db/Oracle.sql

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

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

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

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

## Import the Base Policy Store Objects

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

**To import the base policy store objects**

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

   ***policy_server_home***

   Specifies the Policy Server installation path.

2. Run the following command:

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

   **-i**

   Specifies the path and name of the import file.

   ***upgrade_smdif_file_name***

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

   **-d*siteminder_super_user_name***

   Specifies the name of the SOA Security Manager administrator account.

   **-w*siteminder_super_user_password***

   Specifies the password for the SOA Security Manager administrator account.

   **-v**

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

   **Default output:** stdout

**-f**

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

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

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

**UNIX example:** smobjimport

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

The base policy store objects are imported.

3. Run the following command:

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

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

**-i**

Specifies the path and name of the import file.

**-d*siteminder_super_user_name***

Specifies the name of the SOA Security Manager administrator account.

**-w*siteminder_super_user_password***

Specifies the password for the SOA Security Manager administrator account.

**-f**

Overrides duplicate objects.

**-v**

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

**Default value:** stdout

**-l**

Creates a log file.

**-c**

Indicates that the smdif input file contains unencrypted data.

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

You can now import the policy store data definitions.

## Import the Policy Store Data Definitions

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

**To import the base policy store objects**

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

   ***policy_server_home***

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

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

   XPSDDInstall SmObjects.xdd

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

   XPSDDInstall EPMObjects.xdd

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

   XPSDDInstall SecCat.xdd

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

   XPSDDInstall FssSmObjects.xdd

   You have imported all required policy store data definitions.

## Install the Administrative User Interface

Unlike previous versions of SOA Security Manager, the Policy Server User Interface is not installed with the Policy Server. Rather, you are required to install the r12.1 Administrative UI separately.

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

# Chapter 3: Upgrade Worksheets

This section contains the following topics:



## Active Directory Information Worksheet

You can use this worksheet to gather the required information for configuring an Active Directory directory server as a policy store or upgrading an existing policy store.

| Information Needed | Your Value |
|---|---|
| Host information | |
| Directory server port information | |
| Administrative DN | |
| Administrative password | |
| Policy store root DN | |
| (Optional) SSL client certificate | |

## CA Directory Information Worksheet

You can use this worksheet to gather the required information for configuring a CA Directory database as a policy store.

| Information Needed | Your Value |
|---|---|
| Host information | |
| CADSA port number | |
| Base DN | |
| Administrative DN | |
| Administrative password | |

# Sun Java System Directory Server Information Worksheet

You can use this worksheet to gather the required information for configuring a Sun Java System Directory Server as a policy store or upgrading an existing policy store.

| Information Needed | Your Value |
|---|---|
| Host information | |
| Directory server port information | |
| Administrative DN | |
| Administrative password | |
| Policy store root DN | |
| (Optional) SSL client certificate | |

# Microsoft ADAM Information Worksheet

You can use this worksheet to gather the required information for configuring a Microsoft ADAM directory server as a policy store or upgrading an existing policy store.

| Information Needed | Your Value |
|---|---|
| Host information | |
| Directory server port information | |
| Administrative DN | |
| Administrative password | |
| Policy store root DN | |
| (Optional) SSL client certificate | |

# Administrative UI Registration Worksheet

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

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