CA Federation Manager

Installation and Upgrade Guide

r12.5

CA Technologies Product References

This document references the following CA Technologies products:

- 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.

Contents

Chapter 1: Install Federation Manager

This section contains the following topics:

System and Installation Prerequisites

The minimum system requirements for Federation Manager are:

Memory

2 GB (minimum)

Disk Space

3 GB minimum (1GB disk space, 2GB temporary file location)

Browser

Windows Internet Explorer; Mozilla FireFox

Supported Operating System

Windows, Solaris, Linux

For specific version information, see the Federation Manager Platform Support Matrix on the Technical Support site.

Installation Prerequisites

The following prerequisites are necessary for a successful installation.

Note: Review the *Federation Manager Release Notes* for more information about specific platforms.

- Oracle or SQL Server database

  The policy, key, and session stores use the server database. Install a database and name the database instance. This instance name is used later when running the Federation Manager Configuration wizard.

  Important! Multiple Federation Manager servers can share a database instance, but the database instance must be dedicated for your federation environment. Do not share the database instance with servers for other applications, such as a SiteMinder server. Though Federation Manager systems need a dedicated database instance, they do not need a dedicated database server.

  The database administrator must have privileges to create tables in the database and populate the database with data.

  For specific version information, see the Federation Manager Platform Support Matrix on the Technical Support site.

- JDK required

  For specific version information, see the Federation Manager Platform Support Matrix on the Technical Support site.

- Javascript must be enabled
- Windows

  Run the installation as an administrator and stop and start Federation Manager services as an administrator.

- Solaris and Linux
  - Do not install Federation Manager as the root user. If you try to install as a root user, the installation aborts and you receive an error message. Instead, create a user account to install Federation Manager.
  - Avoid running Federation Manager on UNIX platforms using any port below 1024. This recommendation includes the default Apache HTTP port (80) and the default Apache SSL port (443).
  - The installation program requires 32-bit system libraries, even if you are installing on a 64-bit system. Install the 32-bit libraries on the 64-bit system before running the installation.

    On Linux systems, run the **updatedb** command after installing the 32-bit libraries. The updatedb command ensures that the operating system is aware of the new libraries.
  - Install X11 (32-bit) library packages to run a GUI mode installation on an xterminal. These packages are required.
- Linux Only

  To run a Java-based GUI, your system must have the necessary package, such as libXsts. The necessary package is typically available on your system by default.

How to Run the Federation Manager Installation

Complete the following process to install Federation Manager:

1. Gather information required by the installation wizard.
2. Determine which installation mode to use.
3. Run the installation wizard.

Important! Be aware of the following installation restrictions:

- Do not install Federation Manager on a system where the SiteMinder Policy Server or Secure Proxy Server (SPS) is already installed. Installing Federation Manager on a SiteMinder system could negatively impact the existing SiteMinder installation.
- Do not install Federation Manager on a system where there is an existing Apache Web Server or Apache Tomcat Server.

Information Required for Installation

Before you install Federation Manager, be prepared with the following information. You are prompted for it during the installation.

Path to an installed JDK

Prior to installing Federation Manager, install a JDK and know its location.

Federation Manager Administrator Password

Federation Manager requires that you enter a password during installation. This password is the one you will use to log in to the Federation Manager UI.

Note: The Federation Manager administrator password can contain only English (ASCII) characters.

FIPS Mode

You can install Federation Manager in one of the following FIPS modes of operation:

FIPS_COMPAT

FIPS_COMPAT (compatibility) mode is the default FIPS mode of operation during installation. In FIPS_COMPAT mode, Federation Manager continues to support the current set of non-FIPS algorithms as well as the supported FIPS-compliant algorithms.

FIPS_COMPAT mode is compatible with previous versions Federation Manager. This compatibility enables environments with a version of Federation Manager earlier than r12.5 to interoperate with r12.5. FIPS_COMPAT is also suitable for any clients who are satisfied with the degree of security available in the current Federation Manager implementation.

If your organization does not require the use of FIPS, install Federation Manager in FIPS_COMPAT mode. No further configuration is required.

FIPS_ONLY

In FIPS_ONLY mode, the environment uses only FIPS-compliant algorithms to encrypt sensitive data.

Install Federation Manager in FIPS_ONLY mode for new installations where you want to use only FIPS-compliant algorithms.

Important! Anytime you change the FIPS mode, restart Federation Manager.

Determine Which Installation Mode to Use

You can install Federation Manager on Windows or UNIX platforms using one of the following modes:

- GUI mode — enables a graphical user interface installation.
- Console mode — enables a command-line installation.
- Unattended mode — enables a file-based installation that does not require user intervention. You must complete one GUI or console mode installation on a system before using unattended mode on any other system.

Installation Executables for r12.5

The following table identifies the installation executables for Federation Manager. The table is organized by platform.

Platform	Installation Executable
Linux	ca-fedmgr-12.5-rhel30.bin
Solaris	ca-fedmgr-12.5-sol.bin
Windows	ca-fedmgr-12.5-win32.exe

For more information about supported operating systems, see the Federation Manager Platform Support Matrix on the Technical Support site.

Install Federation Manager on Windows Systems

These instructions are for GUI and Console Mode installations on Windows systems. The steps for the two modes are the same, with the following exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number.
- Press ENTER after each step to proceed through the process.
- The prompts for each mode will help guide you through the process.
- You can type BACK to visit the previous step.

Important! Be aware of the following installation restrictions:

- Do not install Federation Manager on a system where the SiteMinder Policy Server or Secure Proxy Server (SPS) is already installed. Installing Federation Manager on a SiteMinder system could negatively impact the existing SiteMinder installation.
- Do not install Federation Manager on a system where there is an existing Apache Web Server or Apache Tomcat Server.

To locate installation kits

1. Go to the Technical Support site.
2. Log on to the site.
3. Click Download Center.

Search the Download Center for the installation kit you need and download it to your local system.

To install Federation Manager on Windows

1. Exit all applications that are running and stop any antivirus software.
2. Run the installation.

   How you run the installation depends on whether you log in as a local administrator or a network user. If you are a network user, you must be part of the Administrators group to run the installation.

   - **GUI Mode**

     Local administrator: double-click the *installation_executable*

     Network user: right-click the *installation_executable* and select Run as administrator

   - **Console Mode:** Open a command window and enter *installation_executable* -i console

   The Federation Manager installation wizard starts.

   Note: View a list of installation executables.
3. Respond to the prompts in each installation dialog using the information you gathered prior to installation.

   In the License Agreement dialog, read the agreement. You have to scroll to the end of the agreement before you can accept or not accept it.
4. Review the installation settings in the Install Summary and click Install (GUI mode) or enter Y to install (Console mode).

   The installation executes.

   If you experience problems during the installation, review the installation log file CA_Federation_Manager_InstallLog.log, which is located in the directory *federation_mgr_home*\install_config_info.
5. After the installation is complete, restart your system.

After the system restarts, continue by running the Configuration wizard.

More information:

Information Required for Installation (see page 12)
How to Run the Federation Manager Configuration Wizard (see page 18)

Install Federation Manager on UNIX Systems

These instructions are for GUI and Console mode installations on UNIX systems. The steps for the two modes are the same, with the following exceptions for Console Mode:

- You are instructed to select an option by entering a corresponding number.
- Press ENTER after each step to proceed through the process.
- The prompts for each mode help guide you through the process.
- You can type BACK to visit the previous step.

Note: If the UNIX system where you plan to install Federation Manager uses an IPv6 address, run the installation in only Console mode. If you try to install in GUI mode, the installation program defaults to console mode due to a third-party limitation.

Important! Be aware of the following installation restrictions:

- Do not install Federation Manager on a system where the SiteMinder Policy Server or Secure Proxy Server (SPS) is already installed. Installing Federation Manager on a SiteMinder system could negatively impact the existing SiteMinder installation.
- Do not install Federation Manager on a system where there is an existing Apache Web Server or Apache Tomcat Server.
- Do not install Federation Manager as the root user. If you try to install as a root user, the installation aborts and you receive an error message. Instead, create a user account to install Federation Manager.
- Avoid running Federation Manager on UNIX platforms using any port below 1024. This recommendation includes the default Apache HTTP port (80) and the default Apache SSL port (443)

To locate installation kits

1. Go to the Technical Support site.
2. Log on to the site.
3. Click Download Center.
4. Search the Download Center for the installation kit you need and download it to your local system.

To install Federation Manager on a UNIX system

1. Exit all applications that are running and stop any antivirus software.
2. If you do not have the necessary permissions, add executable permissions to the installation file by running the chmod command, for example:

   Linux: chmod +x ca-fedmgr-12.5-rhel30.bin
3. Enter one of the following commands in a command window:
   - **GUI Mode:** ./*installation_executable*
   - **Console Mode:** ./*installation_executable* -i console

   The Federation Manager installation wizard starts.

   Note: A list of installation executables is available in this guide.
4. Respond to the installation prompts using the information you gathered prior to installation.

   In the License Agreement dialog, read the agreement. Go to the end of the agreement before you can choose to accept or not accept the license.
5. Review the installation settings and click Install (GUI mode) or enter Y to install (Console mode).

   The Federation Manager installation program runs.

   If you experience problems during the installation, review the installation log file CA_Federation_Manager_InstallLog.log, which is in the directory *federation_mgr_home*/install_config_info.

After the installation is complete, continue by running the Configuration wizard.

More information:

Information Required for Installation (see page 12)
How to Run the Federation Manager Configuration Wizard (see page 18)

Solaris 10 Security Properties File Requires Modifications

Federation Manager cannot execute encryption and decryption properly on Solaris 10 systems if the default security provider configuration is in place.

To solve this problem, list the Sun provider (sun.security.provider.Sun) before the PKCS11 provider (sun.security.pkcs11.SunPKCS11) in the java.security properties file. This file is located in the lib/security directory of the JDK installation.

Modify the java.security file as follows:

security.provider.1=sun.security.provider.Sun

security.provider.2=sun.security.pkcs11.SunPKCS11
${java.home}/lib/security/sunpkcs11-solaris.cfg

security.provider.3=sun.security.rsa.SunRsaSign

security.provider.4=com.sun.net.ssl.internal.ssl.Provider

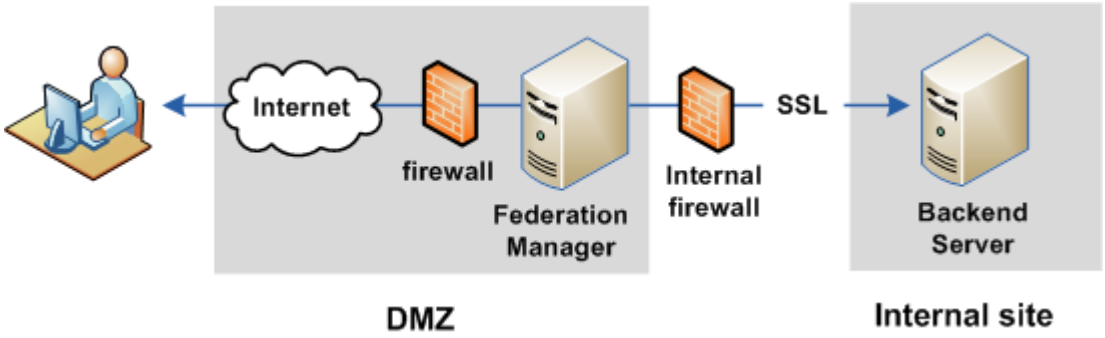
security.provider.5=com.sun.crypto.provider.SunJCE

security.provider.6=sun.security.jgss.SunProvider

security.provider.7=com.sun.security.sasl.Provider

Enable SSL Between Federation Manager and a Backend Server

Your federated network can have Federation Manager communicating to a backend server over an SSL connection. The network configuration is illustrated in the following figure.



To establish an SSL connection between Federation Manager and the backend server

1. Configure the backend server for SSL.

   For instructions, refer to the documentation for the server.

2. On the Federation Manager system, add the CA certificate that signed the server certificate to the file ca-bundle.cert. The server certificate is the one that the backend server used to enabled SSL.

   The ca-bundle.cert file resides in the directory *federation_mgr_home*\secure-proxy\SSL\certs.

   federation_mgr_home is the installed location of Federation Manager.

   Obtain this certificate from the administrator of the backend server.

Reinstall Federation Manager on Windows or UNIX Platforms

You can reinstall the same version of Federation Manager over an existing installation. Reinstalling lets you restore lost application files or restore the default installation settings.

Note: You can reinstall Federation Manager without uninstalling it.

Follow these steps:

1. On UNIX platforms, source the environment script, ca_federation_env.ksh.
2. Run the installation program again using the same program you used for the initial installation.
3. Restart the system when prompted.
4. Rerun the configuration wizard (see page 18).

   Rerun the Configuration wizard after a reinstallation. This step is necessary regardless of whether you are using the same settings as you did for the original installation and configuration.
5. Restart the system when prompted.

Note: If you installed the Federation Manager Agent for Windows Authentication on the reinstalled Federation Manager system, reconfigure the Agent or it will not operate correctly.

The reinstallation is complete.

How to Run the Federation Manager Configuration Wizard

After you install Federation Manager, run the Configuration wizard.

The Configuration wizard sets up the database used as a policy store, the ports for the Federation Manager server, and the Apache web server configuration.

Rerun the Configuration wizard anytime to change your existing configuration but be aware that you discard your existing configuration. To preserve the configuration, back it up.

Note: If you reconfigure a Windows system with SSL enabled, deactivate the SSL configuration before reconfiguring your system. Reactivate SSL after the reconfiguration is complete.

Complete the following process to configure Federation Manager:

1. Gather information required by the Configuration wizard.
2. Run the Configuration wizard.

Determine the Deployment Mode Before Configuration

When you run the Configuration wizard, select one of the following deployment modes:

- Proxy Mode
- Standalone Mode

Base the deployment mode decision on how you want Federation Manager to handle requests as the relying party. The relying party is the side of the federated communication where the mode has the most impact on how federation is implemented.

To modify the deployment mode, rerun the Configuration wizard.

In each mode, Federation Manager can work with a SAML-compatible federation product of your choice. Federation Manager can also, optionally, work with the SiteMinder Connector to integrate with an existing SiteMinder deployment.

Proxy Mode

In a proxy mode deployment, you use Federation Manager in the DMZ to forward requests to backend web servers that host federated applications. These backend systems sit behind a firewall and are not directly accessible.

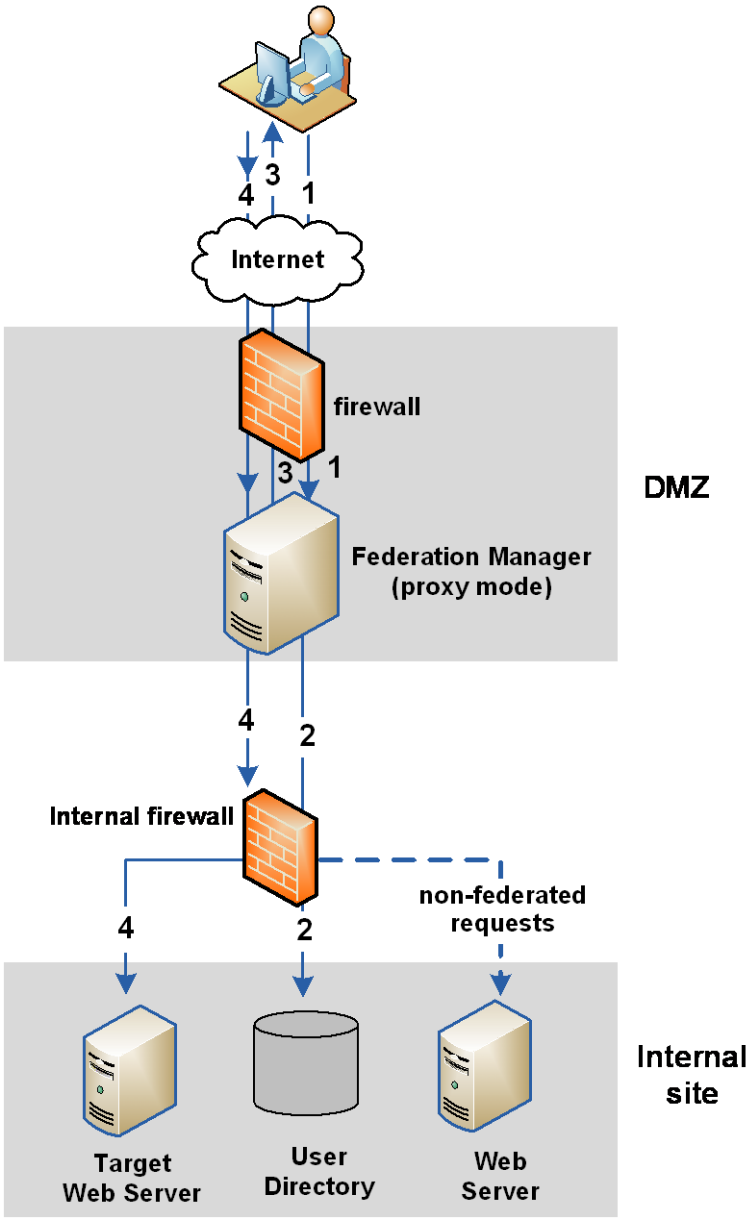
Proxy mode offers the following advantages:

- Provides one access point into your network.
- Enables Federation Manager to supply identity attributes using HTTP headers from the SAML assertion to backend applications. The applications can then be customized to provide a more personalized user experience.

Note: You can protect the HTTP Headers against modification by an unauthorized user by setting an HTTP Header prefix. More information is available for protecting HTTP Headers in proxy mode.

Important! In proxy mode Federation Manager passes *all* requests to the backend network. Therefore, be sure that all resources on a backend web server are protected by SiteMinder or another access control product. For example, a backend web server may host a federated application as well as unprotected resources behind the firewall. If the administrator exposes the federated application, the unprotected resources are also exposed because Federation Manager allows full access to the backend web server without checking for authorization. This assumes that the non-federated resources are URL-addressable.

The following figure shows a typical proxy mode deployment from the perspective of the relying party.



The previous figure shows the following communication flow at the relying party:

1. A user makes an initial request for a federated resource.
2. Based on the data in the assertion, Federation Manager authenticates the user, contacting the user directory at the internal site to complete the user disambiguation process.
3. After successful authentication, Federation Manager returns a redirect response back to the user's browser.
4. Federation Manager proxies the request to the target web server and the user accesses the resource.

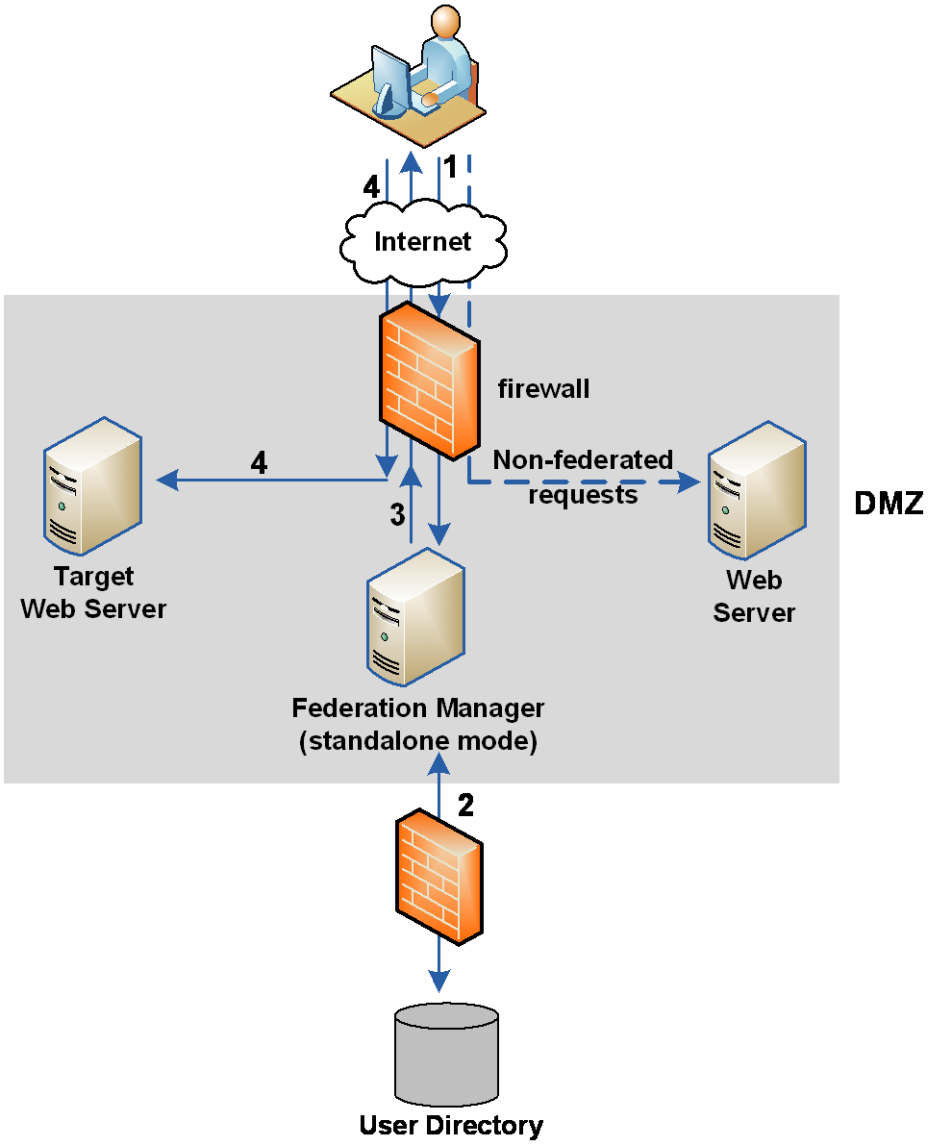
Standalone Mode

In a standalone mode deployment, Federation Manager handles only federated requests, redirecting these requests to the target web servers. Non-federated requests go directly to the appropriate web server, independent of Federation Manager.

The advantage of standalone mode is that it limits federation traffic to Federation Manager and off-loads the handling of other content to other web servers. It also enables a site to add federation to its network without disrupting existing infrastructure.

In standalone mode you cannot pass user attributes from an assertion using HTTP headers because there is no proxy between the web server and the browser to add HTTP headers to the response.

The following figure shows a typical standalone mode deployment from the perspective of the relying party.



The previous figure shows the following communication flow at the relying party:

1. A user requests a federated resource.
2. Based on the data in the assertion, Federation Manager authenticates the user, which includes communicating with the user directory to complete the user disambiguation process.
3. Federation Manager returns a redirect response back to the user's browser.
4. The browser redirects the user to the target resource on the target web server without having to pass through Federation Manager.

Federation Manager Deployment with SiteMinder

Federation Manager includes a built-in SiteMinder Connector that enables it to share user identity information with applications protected by SiteMinder. This integration between Federation Manager and SiteMinder facilitates single sign-on. The SiteMinder Connector can be used with proxy or standalone deployment mode.

You enable the SiteMinder Connector on a per-partnership basis, so that some partnerships can use the Connector while others do not. There is only one global SiteMinder Connector object. When you enable the Connector for a partnership, the partnership uses the global Connector configuration.

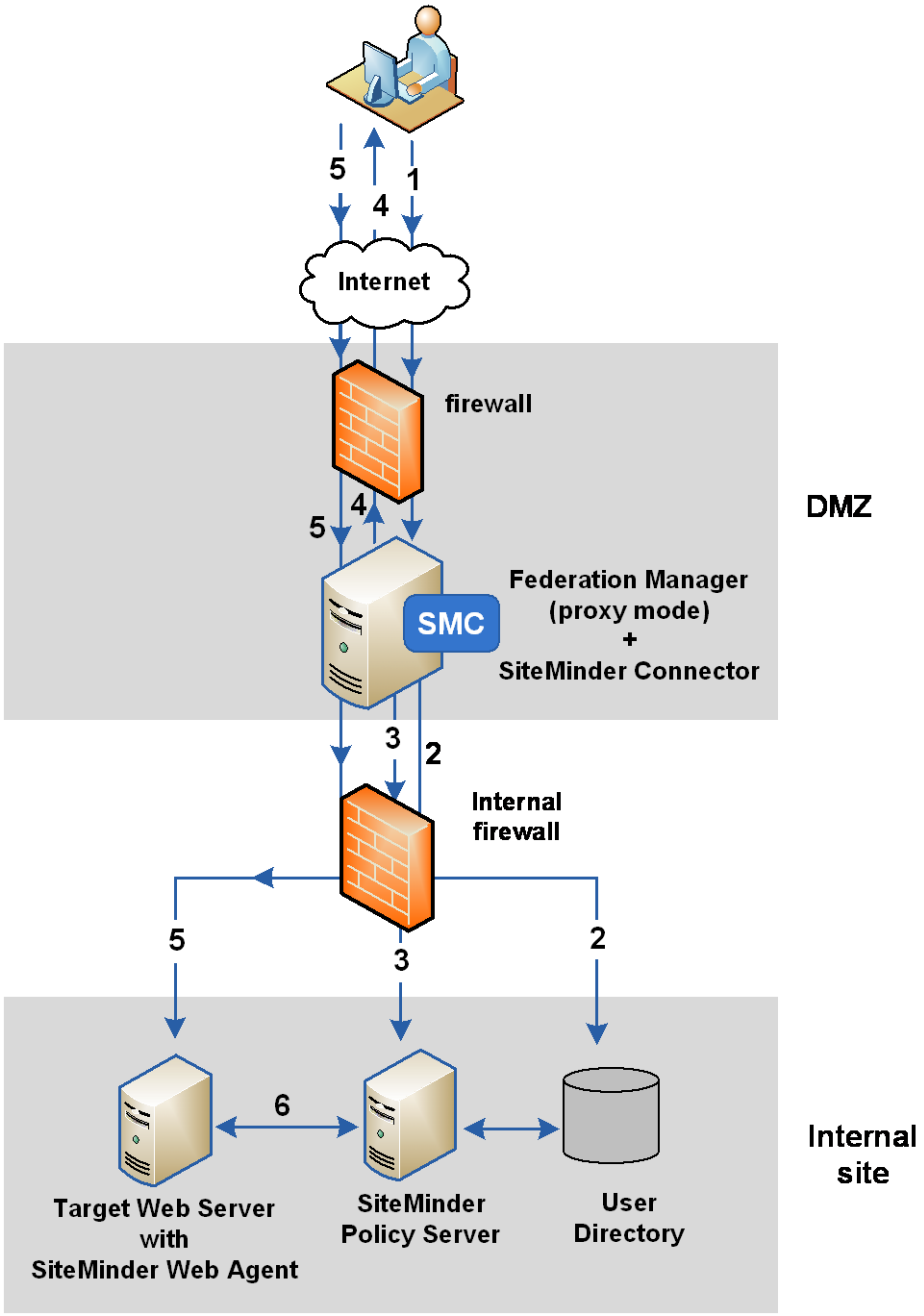
Important! The SiteMinder Connector is for connecting to an independent SiteMinder installation. Do not install Federation Manager on a system where the SiteMinder Policy Server or Secure Proxy Server (SPS) is already installed.

For more information about using the SiteMinder Connector, see the *Federation Manager Guide*.

Proxy Mode with the SiteMinder Connector at the Relying Party

If Federation Manager is communicating with SiteMinder in proxy mode, all requests still pass through Federation Manager; however, Federation Manager has to establish a SiteMinder session with the Policy Server so that when the user requests SiteMinder-protected resources he is not rechallenged. The request is redirected to the target web server, which is protected by a SiteMinder Web Agent.

The following figure shows a proxy mode architecture with the SiteMinder Connector. This figure is from the perspective of the relying party.



The previous figure shows the following communication flow at the relying party:

1. A user requests a federated resource and is redirected to the relying party's assertion consumer service.
2. Based on the data received in the assertion, Federation Manager authenticates the user, which includes communicating with the user directory to complete the user disambiguation process.
3. The SiteMinder Connector, as part of Federation Manager, contacts the custom authentication scheme at the SiteMinder Policy Server. A SiteMinder session ticket is created by the Policy Server, which it sends to Federation Manager. Federation Manager then creates a session cookie that includes the ticket. Establishing a SiteMinder session ensures the user is not challenged later when accessing the target resource.
4. Federation Manager returns a redirect response back to the user's browser.
5. The browser redirects the user to Federation Manager and Federation Manager proxies the request to the web server with the target resource, which is protected by the SiteMinder Web Agent.
6. The SiteMinder Web Agent and Policy Server perform the authorization process.

   After successful authorization, the target resource is presented to the user's browser.

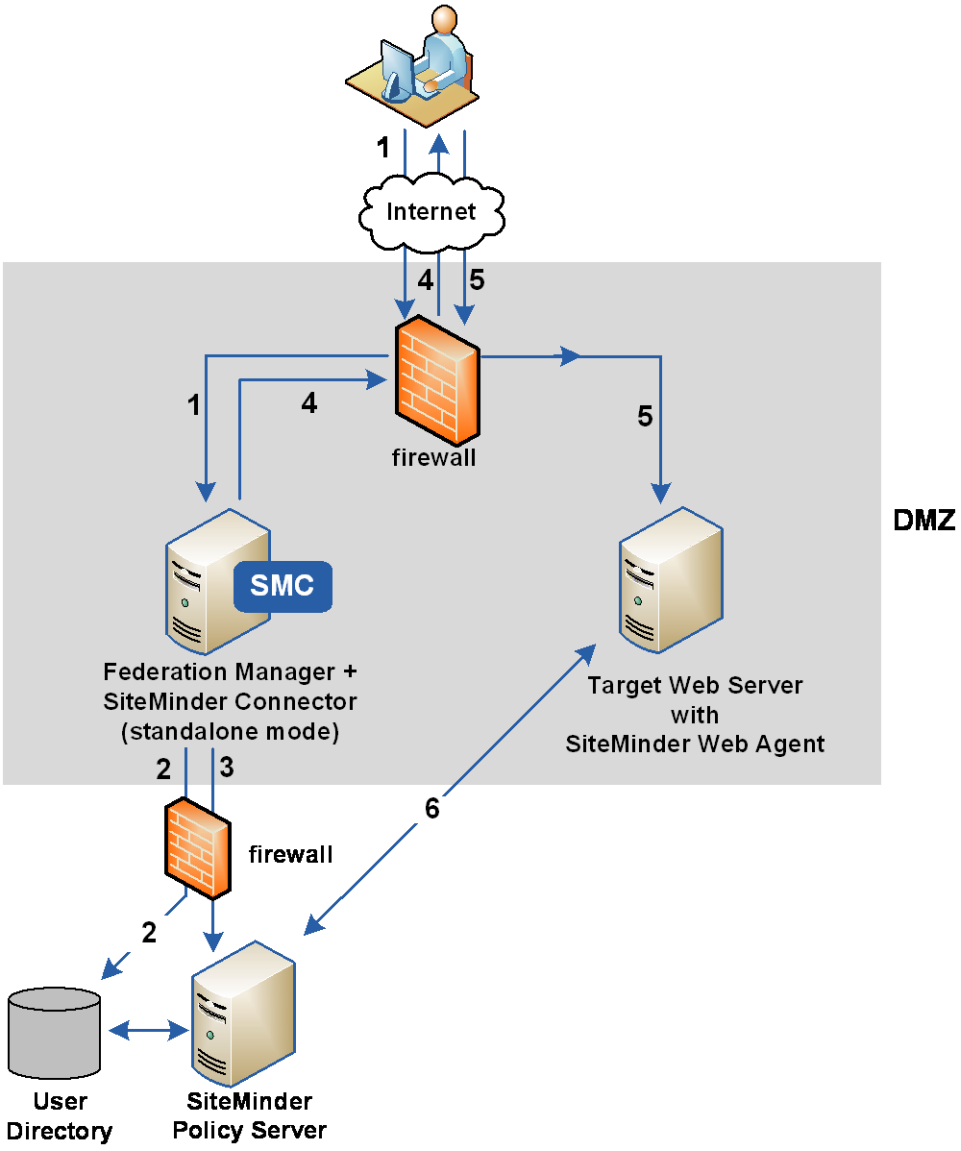
Standalone Mode with the SiteMinder Connector at the Relying Party

If Federation Manager is communicating with an existing SiteMinder environment in standalone mode, Federation Manager handles only federated requests.

To work with SiteMinder, Federation Manager has to establish a SiteMinder session with the Policy Server so that when the user requests SiteMinder-protected resources, he is not rechallenged. The federated request is eventually redirected to the target web server, which is protected by a SiteMinder Web Agent.

Note: Federation Manager and the SiteMinder Web Agent need to share the same cookie domain in standalone mode.

The following figure shows a standalone mode architecture using the SiteMinder Connector. This figure is from the perspective of the relying party.



The previous figure shows the following communication flow at the relying party:

1. A user requests a federated resource and is redirected to the relying party's assertion consumer service.
2. Based on data in the assertion, Federation Manager authenticates the user, which includes communicating with the user directory to complete the user disambiguation process.
3. The SiteMinder Connector, as part of Federation Manager, contacts the custom authentication scheme at the SiteMinder Policy Server. A SiteMinder session ticket is created by the Policy Server, which it sends to Federation Manager. Federation Manager then creates a session cookie that includes the ticket. Establishing a SiteMinder session ensures the user is not challenged later when accessing the target resource.
4. Federation Manager returns a redirect response back to the user's browser.
5. The browser redirects the user to the web server with the target resource, which is protected by the SiteMinder Web Agent.
6. The SiteMinder Web Agent and Policy Server complete the authorization process.

   After successful authorization, the target resource is presented to the user's browser.

Deployment with the SiteMinder Connector at the Asserting Party

At the asserting party, Federation Manager configured with the SiteMinder Connector can use SiteMinder for user authentication. After a successful authentication, the user must be redirected back to Federation Manager, which issues an assertion.

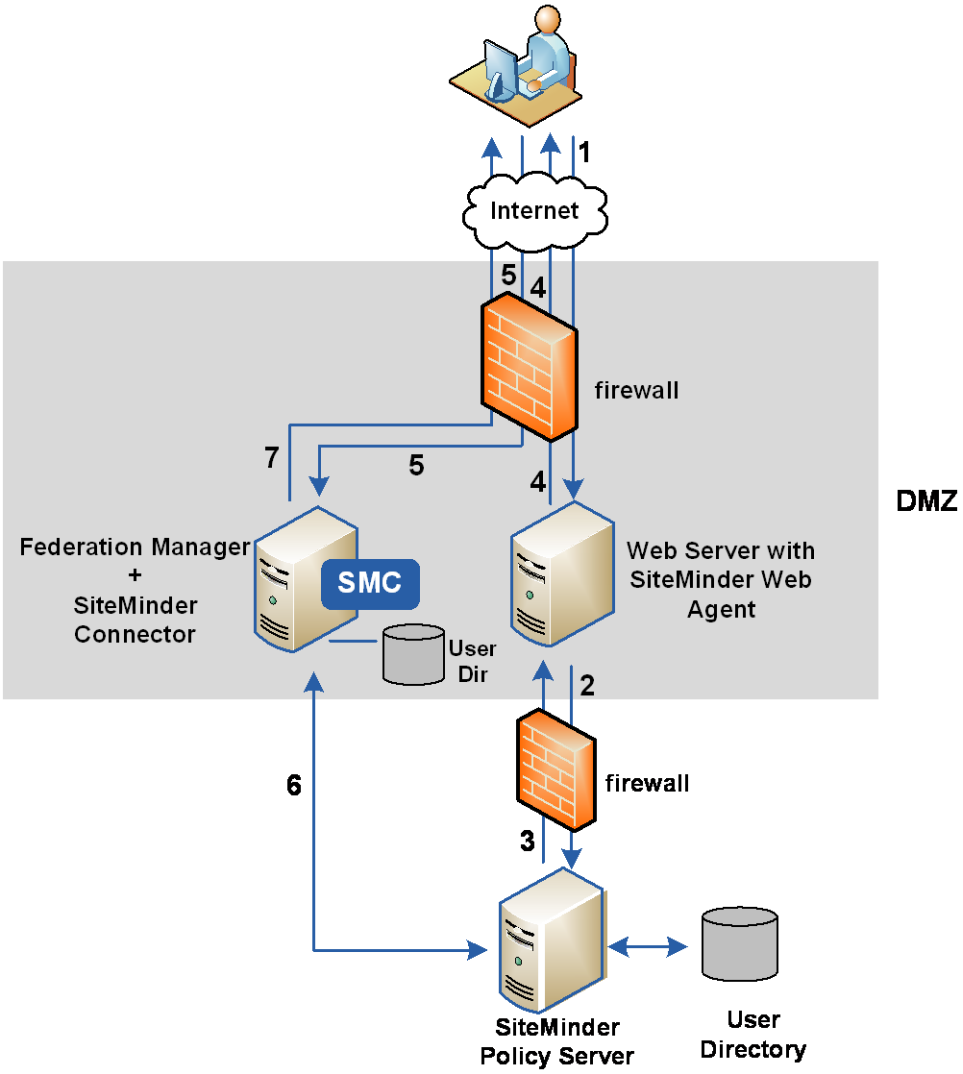
At the asserting party, SiteMinder authenticates a user and then issues an SMSESSION cookie. When the user is sent back to Federation Manager, the presence of the SMSESSION cookie triggers the creation of the FEDSESSION cookie. The deployment mode (proxy or standalone) is not relevant in this case.

Note: If Federation Manager is operating in standalone mode, Federation Manager and the SiteMinder Web Agent need to share the same cookie domain.

In a deployment with SiteMinder, the user has to visit SiteMinder first to authenticate. After authentication is successful, the web resource protected by SiteMinder must send the user back to Federation Manager. A deployment with the SiteMinder Connector is not the same as the Federation Manager feature called delegated authentication, which also allows a web access management system like SiteMinder to handle user authentication. What distinguishes delegated authentication from a SiteMinder Connector deployment without delegated authentication is that the user does not have to initiate authentication at SiteMinder.

Delegated authentication lets Federation Manager initiate an authentication request and then redirect the user to SiteMinder, enabling the redirect to occur automatically, assuming the feature is properly configured. To redirect the user back to Federation Manager after a successfully authenticating the user, the resource that SiteMinder protects must be configured with a mechanism to redirect the user back to Federation Manager. The redirect must include all data that the protected resource received. For example, if the SiteMinder-protected resource received several query parameters from the initial authentication request, it must redirect the user back to Federation Manager with these same query parameters.

The following figure shows an architecture using the SiteMinder Connector at the asserting party.



The previous figure shows the following communication flow at the asserting party:

1. A user requests a federated resource, which triggers an authentication request to the SiteMinder Web Agent at the asserting party.
2. The authentication request is forwarded to the SiteMinder Policy Server.
3. The Policy Server authenticates the user and generates a SiteMinder session ticket. The ticket is returned to the SiteMinder Web Agent, which creates an SMSESSION cookie that contains this ticket.
4. The Web Agent passes the SMSESSION cookie to the user's browser along with a redirect response to Federation Manager.
5. The user's browser with the SMSESSION cookie is redirected to Federation Manager.
6. Federation Manager contacts the SiteMinder Policy Server to validate the SMESSION cookie.
7. After successful validation of the SMSESSION cookie, the Federation Manager session gets created. Federation Manager then handles the rest of the federated communication to the relying party where the target resource resides.

Information Required by the Configuration Wizard

Before you run the Configuration wizard, be prepared with the following information:

Database Type

Specifies the database type (SQL or Oracle) you plan to use for the policy store.

Database Information

Identifies the database that Federation Manager uses.

Database server

Specifies the host name or IP address of the server where the database is installed. The database is the data store repository.

The following entries are allowable, based on operating environment and database type:

Windows (Oracle and SQL): IPv4 address, IPv6 address, host name

UNIX (Oracle): IPv4 address, host name

UNIX (SQL): IPv4 address, IPv6 address, host name

Important! Do not use square brackets around an IPv6 address in this field. The omission of brackets applies only to this setting. Example: 3ff3:1900:4545:3:200:f8ff:fe25:67 (no square brackets)

If you want to use an SQL database named instance, enter the following value for the operating environment:

Windows: *server_name**named_instance*

Example: server01-w3s-t1\federation1

In this example, server01-w3s-t1 is the server name and federation1 is the instance name.

UNIX: *server_name*

Specify the database server name in this field, not the SQL named instance. Additionally, enter the port number of the SQL named instance in the Database port field.

Example: server01-w3s-t1

Database name

Names the database instance.

Limits

SQL: Database name

Oracle: Name of the Oracle user with CONNECT and RESOURCE roles for the tablespace where Federation Manager creates and manages database tables.

Database port

Identifies the port that the database is listening on. Change the port number if the database is not running on the default port. For example, if you specified an SQL named instance for the database server, enter the port for this database instance.

Defaults

SQL:1433

Oracle: 1521

Database username

Names the administrator with super administrative privileges to access the database, and create and manage database tables.

The user name can contain any printable character except for the forward slash (/). The forward slash cannot be used for an Oracle database because it causes the connection to the database to fail.

Database password

Specifies the password for the database administrator account. The password can contain any printable character except for the forward slash (/). The forward slash cannot be used for an Oracle database because it causes the connection to the database to fail.

Federation Manager Server Port

Specifies the TCP port number that Federation Manager is listening on.

Default: 44442

Limit: A numeric value except 44443, 44444, 44445. The port numbers 44443, 44444, 44445 are not permitted.

Deployment mode

Determine how to implement Federation Manager in your environment.

The deployment mode options are:

Proxy Mode

In a proxy mode deployment, Federation Manager is the main entry point to all backend resources.

Select this mode if:

- You want one access point into your network
- Backend applications require attributes from the SAML assertion to provide a personalized user experience. SAML assertion attributes can be delivered as headers.

Note: You can protect the HTTP Headers against modification by an unauthorized user by setting an HTTP Header prefix. More information is available for protecting HTTP Headers in proxy mode.

Standalone Mode

In a standalone mode deployment, Federation Manager is deployed along side either SiteMinder Web Agents or third-party web servers. In this case, Federation Manager handles only federation requests; web servers handle all other requests.

Select this mode if you want to limit federation traffic to Federation Manager and off-load the handling of regular web traffic to other web servers.

In standalone mode, you cannot pass user attributes from an assertion using HTTP headers. You cannot add HTTP headers to the response. No mechanism between the web server and the browser exists to make this modification.

Server Host Name (Proxy mode only)

Identifies the fully qualified domain name of the backend server where Federation Manager forwards the requests for federated resources.

Apache Configuration

Federation Manager uses the open source Apache web server as the HTTP listener for incoming requests.

Server Name

Identifies the fully qualified domain name of the Federation Manager deployment. This server name does not necessarily map to the system where Federation Manager is installed. You can consider it a virtual host.

Admin's Email Address

Specifies the email address for the database administrator.

The Apache server installed with Federation Manager requires this setting. The Apache server uses the e-mail address of the administrator in its default error messages when problems occur. The e-mail address is set with the ServerAdmin directive and can be any valid e-mail address.

Note: The events forwarded to this address are server-specific errors and warnings for the Apache server. The messages are not related to federation.

Apache HTTP Port

Specifies the port listening for HTTP requests.

Default: 80

Note: If you have another web server on your system using port 80, change the default port for the Apache web server.

Apache SSL Port

Specifies the Apache port listening for SSL requests.

Default: 443

Note: If you have another web server on your system using port 443, change the default SSL port for the Apache web server.

Admin UI HTTP Port

Specifies the port listening for Federation Manager UI HTTP requests.

If you change this port, be aware that it must be internal-facing and must not be accessible from the Internet.

Default: 8888

Admin UI SSL Port

Specifies the port listening for Federation Manager UI SSL requests.

If you change this port, be aware that it must be internal-facing and must not be accessible from the Internet.

Default: 8889

Important! The port numbers must be unique for the following settings:

- Federation Manager server port
- Apache HTTP port
- Apache SSL port
- Admin UI HTTP port
- Admin UI SSL port

Configuration Executables

The following table identifies the configuration executables for Federation Manager. The table is organized by platform.

Platform	Configuration Executable
Linux	ca-Federation-config.sh
Solaris	ca-Federation-config.sh
Windows	ca-federation-config.exe

For more information about supported operating systems, see the Federation Manager Platform Support Matrix on the Technical Support site.

Run the Configuration Wizard on Windows

Before you run the Configuration wizard, install Federation Manager and gather all the information that the Configuration wizard requires. Run the Configuration wizard any time you reinstall Federation Manager.

These instructions are for GUI and Console Mode configuration on Windows systems. The steps for the two modes are the same, with the following exceptions for Console Mode:

- You can select an option by entering a corresponding number.
- Press ENTER after each step to proceed through the process.
- You can type BACK to visit the previous step.

The prompts for each mode help guide you through the process.

To configure Federation Manager with the configuration wizard

1. Run the Configuration wizard.

   How you run the wizard depends on whether you log in as a local administrator or a network user. If you are a network user, you must be in the Administrators group to run the wizard.

   - **GUI Mode**

     Local administrator: Select the shortcut on the Start menu or select Start, All Programs, CA, FederationManager, Federation Manager Configuration wizard.

     Network user: Right-click the shortcut on the Start menu or select Start, All Programs, CA, FederationManager then right-click Federation Manager Configuration wizard and select Run as administrator.

   - **Console Mode:** Open a command window, navigate to *federation_mgr_home*\install_config_info and enter the following command:

     ca-federation-config.exe -i -console

     Execute this command from the correct location; the path is not automatically set.

2. Respond to the Configuration wizard prompts using the information you gathered before running the wizard.

3. Review the configuration settings and click Install (GUI mode) or enter Y (console mode) to run the configuration.

   Federation Manager configuration executes.

   If you experience problems during the configuration, review the configuration log file, CA_Federation_Manager_ConfigLog.log, located at *federation_mgr_home*\install_config_info.

4. Reboot the Federation Manager system.

The installation and configuration of Federation Manager is complete.

Important! To change the configuration, for example, to switch the deployment mode, rerun the Configuration wizard. The Federation Manager services must be running when you rerun the wizard. You can rerun the Configuration wizard any time, but by doing so you discard your existing configuration. Before you rerun the Configuration wizard, back up your existing configuration to preserve SSL connections.

Run the Configuration Wizard on UNIX Systems

Before you run the configuration wizard, install Federation Manager and gather all the information that the configuration wizard requires. Run the configuration wizard any time you reinstall Federation Manager.

Important! If you reinstall Federation Manager, rerun the Configuration wizard. Before you rerun the Configuration wizard, back up your existing configuration to preserve SSL and database connections. If you are using an ODBC user directory, also back up the system_odbc.ini file. This file is in the directory *federation_mgr_home*/siteminder/db/.

These instructions are for GUI and Console Mode installations on UNIX systems. The steps for the two modes are the same, with the following exceptions for Console Mode:

- You can select an option by entering a corresponding number.
- Press ENTER after each step to proceed through the process.
- You can type BACK to visit the previous step.

The prompts for each mode help guide you through the process.

Note: If the UNIX system where you plan to configure Federation Manager uses an IPv6 address, run the configuration wizard only in Console mode. If you try to use GUI mode, the program defaults to console mode due to a third-party limitation.

Important! Do not run the configuration wizard as the root user. If you try to run it as root, the wizard aborts and you receive an error message. Run the configuration wizard as the same user that ran the installation.

To run the configuration wizard

1. Open a console window.
2. Navigate to the directory *federation_mgr_home*.
3. Source the environment script, ca_federation_env.ksh.
4. Enter one of the following commands in a command window:
   - **GUI Mode:** ./ca-Federation-config.sh
   - **Console Mode:** ./ca-Federation-config.sh -i console

   The configuration wizard starts.
5. Respond to the Configuration wizard prompts using the information you gathered before running the wizard.
6. Review the configuration settings and click Install (GUI Mode) or enter Y to install (Console mode).

   Federation Manager is configured.

   If you experience problems during the configuration, review the configuration log file, CA_Federation_Manager_ConfigLog.log, located at *federation_mgr_home*/install_config_info.

   The installation and configuration of Federation Manager is complete.
7. Start Federation Manager by running the following script:

   federation_mgr_home/fedmanager.sh start

Important! To change the configuration, for example, to switch the deployment mode, rerun the Configuration wizard. The Federation Manager services must be running when you rerun the wizard. You can rerun the Configuration wizard any time, but by doing so you discard your existing configuration. Before you rerun the Configuration wizard, back up your existing configuration to preserve SSL connections.

Virtual Host Configuration for Federation Manager

You can define multiple virtual hosts for Federation Manager. Virtual hosts can be useful for testing purposes because they allow you to install the asserting and relying party on the same system. Defining multiple virtual hosts also lets you configure SAML 2.0 IdP Discovery profile, using a separate host name and domain for the discovery service.

To define multiple virtual hosts, Federation Manager requires the following configuration setup:

- Add a host to the hostnames parameter in the server.conf file. The server.conf file is in the following directory:

  federation_mgr_home\secure-proxy\proxy-engine\conf.

- If Federation Manager is operating on the same system from which you access the Federation Manager UI or where you run a federation transaction, update the httpd.conf file. The httpd.conf file is in the directory *federation_mgr_home*\secure-proxy\httpd\conf.

  Note: If SSL is enabled for the embedded web server, make the following changes in the httpd-ssl.conf file also. The httpd-ssl.conf file is in the directory *federation_mgr_home*\secure-proxy\httpd\conf\extra folder.

  Update the httpd.conf file based on the system type you have as follows:

  - For IPV4 based systems, add a LISTEN directive as follows:

    LISTEN 127.0.0.1:*port*

  - For dual stack systems with IPv4 and IPv6 support, add LISTEN directives as follows:

    LISTEN 127.0.0.1:*port*

    LISTEN [::1]:*port*

  - For IPv6 systems, add a LISTEN directive as follows:

    LISTEN [::1]:*port*

  Additionally, in the hosts file of the system, update the loopback address entry so the new host name is added to it. The values are:

  - IPv4: 127.0.0.1
  - IPv6: [::1]

Unattended Federation Manager Installation

One of the methods for installing Federation Manager is an unattended installation. An unattended installation lets you install the product without any user intervention.

To run an unattended installation, you must run an attended installation first. The manual installation creates a file called *ca-federation-installer.properties*, which contains all of the parameters, paths, and passwords entered during the manual installation. When you perform an unattended installation, this properties file provides the settings that you would normally enter manually.

You can use the default properties file to run installations with the same settings as the initial installation, or use the file as a template that you modify to suit your environment. Care should be taken in modifying the properties file; its contents are case-sensitive.

Important! You can only run an unattended installation on a system with the same platform as the system where you first installed Federation Manager. For example, you cannot install the product on a Solaris system and then use the properties file to run an unattended installation on a Windows system.

Set up the Installation Properties File

Use the ca-federation-installer.properties file to propagate the installation setup to other systems in your network.

Important! You must first run an attended installation to generate the properties file.

With this properties file do the following:

- Define installation parameters in the file.
- Copy the properties file and the installation executable file to any system in your network where you want to install Federation Manager.

The ca-federation-installer.properties file is created in the following location:

Windows: *federation_mgr_home*\install-config-info

UNIX: *federation_mgr_home*/install-config-info

The default parameters and paths in the file reflect the information you entered during the initial installation.

To modify the installation properties file

1. Open the ca-federation-installer.properties file and modify the parameters in the file.

   Note: The properties file is case-sensitive.

2. Save the file.

The parameters are as follows:

Parameter	Definition
DEFAULT_PRODUCT_INSTALL_TYPE	Defines whether the installation is a new installation, an upgrade, or a re-installation. **Default:** INSTALL
DEFAULT_INSTALL_DIR	Default (Windows): C:\\Program Files\\CA\\FederationManager (Notice the double back slashes.) Default (UNIX): an account on the system Example: /home/myacct/CA/FederationManager
Server Specific Entries	
DEFAULT_JRE_ROOT	Indicates the location of the JRE.
JDK_ROOT	Indicates the location of the JDK.
#FEDADMIN_PW	Defines the password for Federation Manager. This must be uncommented, and the password must be supplied in clear text. For added security, use the ENCRYPTED_FEDADMIN_PASSWORD setting. **Note:** The Federation Manager administrator password can contain only English (ASCII) characters.
ENCRYPTED_FEDADMIN_PASSWORD	Displays the Federation Manager password in encrypted form. We recommend using this encrypted password for added security. If you want the same administrator password on all systems, leave this password in place and do not uncomment the FEDADMIN_PW property.
FIPS Mode Setting	

Parameter	Definition
FED_FIPS_VALUE	Specifies the FIPS 140-2 mode of operation. **Limits:** ■ ONLY ■ COMPAT
LGPL License Setting	
ACCEPT_LGPL_EULA	Indicates whether you accept the LGPL license. Review the license (httpclient-EULA.txt) in the directory *federation_mgr_home*/install_config_info To accept the license, set this variable to YES. **Default:** NO

Run the Unattended Federation Manager Installation

You can run an unattended installation to install Federation Manager without any user intervention.

Note: Before you run an unattended installation, run a manual installation to create a ca-Federation-installer.properties file. This file is required for running an unattended installation on another system. You can modify this file as needed for your installation.

Follow these steps:

1. From a system where Federation Manager is already installed, copy the following two files to a temporary location:
   - installation executable or binary
   - ca-Federation-installer.properties file
2. Run the following command from where you copied the installation and properties files:

   installation_executable -f ca-federation-installer.properties -i silent

The installation starts in unattended mode and uses the parameters in the properties file to install Federation Manager.

Note: To verify an unattended installation on Windows review the installation log file CA_Federation_Manager_InstallLog.log, which is located in the directory *federation_mgr_home*\install_config_info.

Unattended Federation Manager Configuration

One of the methods for configuring Federation Manager is an unattended configuration. An unattended configuration lets you configure Federation Manager without any user intervention.

To run an unattended configuration, you have to first manually configure Federation Manager on a machine. The manual configuration creates a file, called *ca-federation-config.properties*, which you use to run an unattended configuration on a separate machine. By default, the ca-federation-config.properties contains the settings from the initial configuration.

The ca-federation-config.properties file contains all of the parameters, paths, and passwords entered during the initial configuration. When you perform an unattended configuration, this properties file provides the settings that you would normally enter manually.

You can use the default properties file to run configurations with the same settings as the initial configuration or use the file as a template that you modify to suit your environment.

If you plan to use the properties file on more than one system in a network, be sure to set the APACHE_SERVER_NAME setting to a unique value for each system where you run an unattended configuration. The same server name for more than one system may cause conflicts.

Important! You can only run an unattended configuration on a system with the same platform as the system where you first installed Federation Manager. For example, you cannot configure the product on a Solaris system and then use the properties file to run an unattended configuration on a Linux system.

Set Up the Configuration Properties File

Unattended configuration uses the ca-federation-config.properties file to propagate the Federation Manager configuration to another system in your network.

With this properties file, you do the following:

- Define configuration parameters in the file.
- Copy the properties file and the configuration executable file to any system in your network where you want to configure Federation Manager.

The ca-federation-config.properties file is installed in the following location:

Windows: *federation_mgr_home*\install-config-info

UNIX: *federation_mgr_home*/install-config-info

The default parameters and paths in the file reflect the information you entered during the initial configuration.

Important! The configuration properties file is case-sensitive.

To modify the configuration properties file

1. Open the ca-federation-config.properties file and modify the parameters in the file.
2. Save the file.

The parameters are as follows:

Parameter	Description
Database Information	
PARAM_DBTYPE	Indicates the type of database—SQL or Oracle.
PARAM_UID	Displays the database administrator user name.
#PARAM_PWD	Identifies the Federation Manager administrator password used to log in to the UI in clear text. Uncomment this line before entering a value. For added security, use the ENCRYPTED_PARAM_PWD setting.
ENCRYPTED_PARAM_PWD	Specifies the encrypted Federation Manager administrator password. We recommend using this encrypted password for added security.
PARAM_DB_SERVER	Identifies the IP address of the database server.
PARAM_DB_PORT	Displays the port the database is listening on. **Defaults:** ■ SQL: 1433 ■ Oracle: 1521
MSSQL Specific	
PARAM_DB	MS-SQL specific parameter. Names the SQL database.
Oracle Specific	

Parameter	Description
ORACLE_SID	Oracle-specific parameter. Specifies the **service name** (NOT the SID) of the Oracle database.
RECONFIGURE	Indicates whether or not Federation Manager uses an existing database schema or creates a new schema. **Limits:** true (use an existing schema), false (create a new schema)
Federation Manager Server Port	
PARAM_PORT	Defines the port that Federation Manager is listening on. **Default:** 44442 **Important!** Do not assign a value of 44445 for this port.
Deployment Mode	
DEPLOYMENT_MODE	Specifies the Federation Manager deployment mode. **Limits:** ■ Proxy (uppercase P) ■ Standalone (uppercase S)
PROXY_HOST_NAME	(Proxy mode only) Identifies the fully qualified domain name of the backend server where Federation Manager forwards the requests for federated resources. Define this setting using the syntax *server_name.domain:port.* Example: myserver.mycompany.ca.com:5555 If you use this properties file on more than one Federation Manager system and these systems use the same proxy, set this host name to the same value for each system. Federation Manager and the proxy host must be in the same domain.
Apache Server Information	
APACHE_SERVER_NAME	Specifies the name of the Apache web server. If you plan to use the properties file on more than one system in a network, set this value to a unique name for each system where you run an unattended configuration. The same server name for more than one system may cause conflicts.

Parameter	Description
APACHE_ADMIN_EMAIL	Indicates the email address of the Federation Manager administrator. This setting is required by the Apache server installed as part of Federation Manager. Apache uses the administrator's e-mail address in its default error messages when problems are encountered. The e-mail address is set with the ServerAdmin directive and can be any valid e-mail address. The events forwarded to this address are server-specific errors and warnings for the Apache server. The messages are not related to federation. **Default:** admin@mycompany.com
APACHE_HTTP_PORT	Specifies the default port the Apache web server is listening on. **Default:** 80
APACHE_SSL_PORT	Specifies the default SSL port the Apache web server is listening on. **Default:** 443
UI_HTTP_PORT	Specifies the default HTTP port the Administrative UI is listening on. **Default:** 8888
UI_SSL_PORT	Specifies the default SSL port the Administrative UI is listening on. **Default:** 8889

Important! The port numbers must be unique for the following settings:

- Federation Manager server port
- Apache HTTP port
- Apache SSL port
- Admin UI HTTP port
- Admin UI SSL port

Run the Unattended Configuration

You can configure Federation Manager without any user intervention.

Note: You must have previously configured a system manually to create the ca-Federation-config.properties file. You can modify this file to suit your network.

Follow these steps:

1. From a system where Federation Manager is already installed, copy the following two files to a temporary location:
   - Configuration executable or binary (see page 33)
   - ca-Federation-config.properties
2. Run the following command from where you copied the installation and properties files:

   configuration_executable -f ca-federation-config.properties -i silent

   The configuration starts in unattended mode, using the parameters in the properties file for settings.
3. On Windows, reboot the system after the configuration is complete.

   Note: To verify an unattended installation on Windows review the installation log file CA_Federation_Manager_InstallLog.log, which is located in the directory *federation_mgr_home*\install_config_info.

Log in to the Federation Manager User Interface

You configure Federation Manager entities through the Federation Manager User Interface (UI).

Important! Only one administrator can be logged on to the Federation Manager User Interface at one time. In addition, the administrator can open only one browser instance.

To log in to the Federation Manager UI

1. Ensure Java Script is enabled in the browser. This is required to open the Federation Manager UI.
2. Follow the instructions for your platform:

   Windows

   Select Start, All Programs, CA, FederationManager, Federation Manager Admin UI.

   UNIX

   Open a web browser and enter the following URL:
   http://*fedmgr_server:ui_port*/ca/federation/adminui

   fedmgr_server:ui_port

   Specifies the fully qualified domain name of the server where Federation Manager is installed, including the port for the UI. The default port is 8888.

   Example:

   http://fedmgr1.ca.com:8888/ca/federation/adminui

   The login window appears.
3. Enter the user name and password and click Log in.

   Important! The user name is always **admin**. You cannot change it. The administrator password is set during installation.

The Federation Manager UI launches.

Chapter 2: Uninstall Federation Manager

This section contains the following topics:

Uninstall Federation Manager from Windows Systems

Uninstall Federation Manager when it is no longer required on the system.

To uninstall Federation Manager

1. Select Start, All Programs, CA, FederationManager, Uninstall.

   The uninstallation wizard executes.
2. Follow the instructions in the wizard to uninstall Federation Manager.
3. After the uninstallation is complete, navigate to *federation_mgr_home* and delete the Federation Manager folder and all its subfolders, if needed.
4. Reboot the system.

Federation Manager is uninstalled.

Uninstall Federation Manager from UNIX Systems

Uninstall Federation Manager when it is no longer required on the system.

To uninstall Federation Manager

1. Open a command window.
2. Navigate to the directory *federation_mgr_home.*
3. Source the environment script, ca_federation_env.ksh.
4. Enter the following command to execute the uninstallation script:

   ./ca-Federation-uninstall.sh
5. Navigate to the directory *federation_mgr_home* and delete the Federation Manager folder and all subfolders, if needed.

Federation Manager is uninstalled.

Chapter 3: Upgrade a 12.x System to Federation Manager r12.5

This section contains the following topics:

Upgrade and Migration Paths for Federation Manager

An upgrade is an update to a new version of Federation Manager on a system running an existing 12.x version of Federation Manager. An upgrade requires that the existing system be running an operating system, a database, and a JDK that the new version of Federation Manager supports.

A migration is a replicated configuration from an existing system to a system with a new r12.5 installation. The new Federation Manager system must be communicating with a supported database version.

Notes:

- Your migration to a r12.5 environment must include a supported database. If your environment is using a database that is not supported by r12.5, install a supported database server and move over your data to the new database. Finally, migrate to r12.5.
- If you upgrade to r12.5 and the Federation Manager Agent for Windows Authentication is installed, upgrade the Agent to the same version as Federation Manager. Otherwise, the Agent fails to work properly.

For specific version information, see the Federation Manager Platform Support Matrix on the Technical Support site.

You can upgrade or migrate to r12.5 based on these available paths:

Windows

Existing Federation Manager Version	Database Works with r12.5?	Upgrade or Migrate
r12.0 including all SPs	No	Migrate to r12.5
r12.1 including all SPs	No	Migrate to r12.5
r12.1 SP3	Yes	Upgrade to r12.5

Solaris/Linux

Existing Federation Manager Version	Database Works with r12.5?	Upgrade or Migrate
r12.0 including all SPs	No	Migrate to r12.5
r12.1 including all SPs	No	Migrate to r12.5
r12.1 SP3	Yes	Upgrade to r12.5

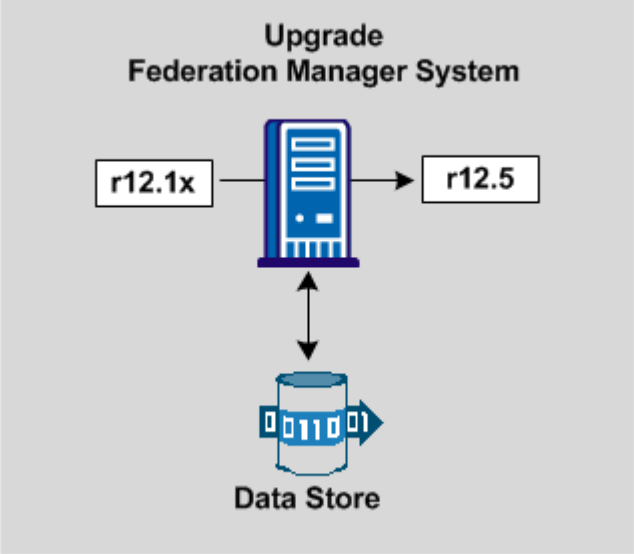
FIPS Migration

Federation Manager supports migration from a non-FIPS to a FIPS-only environment; however, the migration process is complex. If you want to migrate from a non-FIPS to a FIPS-only environment, first complete the upgrade to r12.5. After a successful upgrade, follow the FIPS migration process.

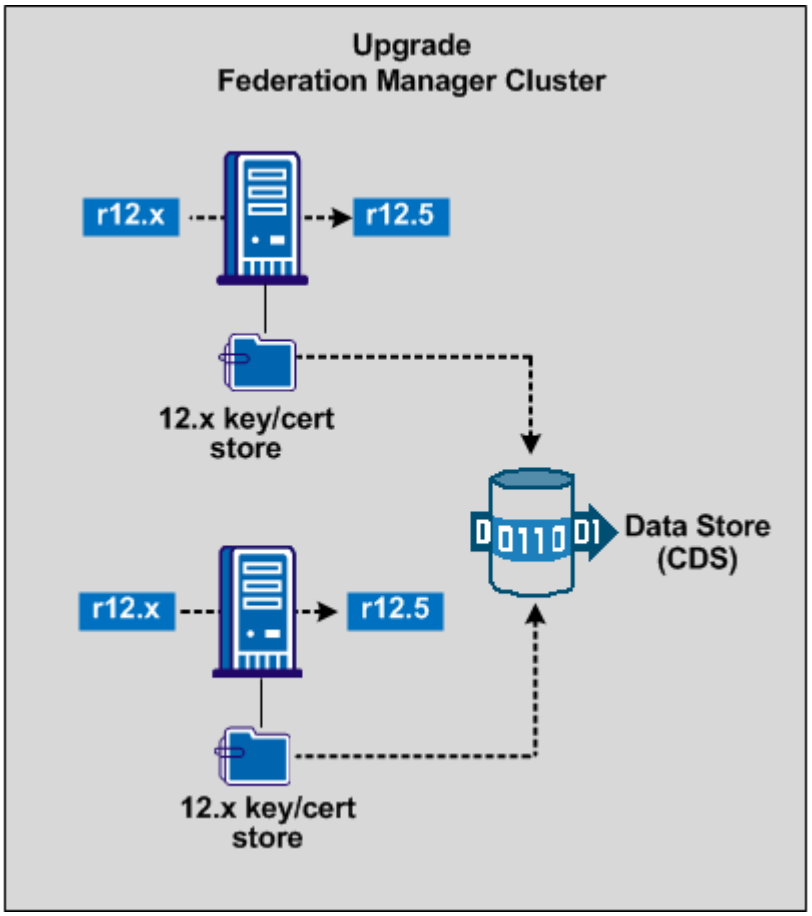
How to Upgrade to Federation Manager r12.5

You can upgrade Federation Manager on Windows and UNIX (Solaris and Linux) systems to r12.5. The existing systems must be running an operating platform and database that supports r12.5.

The following figure shows the upgrade path on a single system.



The following figure shows an upgrade of a clustered environment.



You can set up a Federation Manager cluster to support failover. To upgrade from an existing r12.x cluster to a new cluster, follow a procedure similar to a non-cluster upgrade. Upgrade each system in your existing cluster to r12.5, assuming the current operating platforms support r12.5.

The systems in a cluster share one data store. By running the r12.5 installation program, which detects upgrades, the key and certificate information is automatically moved to the certificate data store (CDS). The CDS is colocated with the main data store.

The process for an upgrade is as follows:

1. Synchronize multiple key databases (only when you are upgrading a cluster)
2. Back up your existing configuration, including data stores and key stores.
3. Upgrade to r12.5 by running the installation program. The installation can detect upgrades.

Each procedure is detailed in the following sections.

Synchronize Multiple Key Databases

Pre-12.5 systems stored private key and certificate data in a key store called smkeydatabase. This data now resides in the certificate data store, which is colocated with the data store. The certificate data store is replacing the requirement that each federation system in the environment access a local smkeydatabase.

As part of the upgrade, the installer automatically backs up the local smkeydatabase and tries to migrate all content to the certificate data store. This process compares the smkeydatabase and CDS before starting the migration. The purpose of the comparison is to identify data inconsistencies, such as the same alias mapping to different certificates, that can prevent a successful migration.

In a cluster environment, there are multiple instances of the smkeydatabase. Before you upgrade or migrate to r12.5, synchronize all smkeydatabase instances so that the information is consistent. Synchronizing the databases helps ensure that no inconsistencies arise as each instance is migrated to the CDS.

Resolve all data inconsistencies between smkeydatabase instances from the Certs and Keys tab in the Administrative UI. Confirm that the following data is consistent across key database instances:

- Each CA certificate must reference certificate revocation lists consistently across instances.
- **Example:** A CA certificate consistently references certificate revocation lists in an LDAP directory service.
- The defaultentpriseprivatekey alias represents the same private key/certificate pair in all instances.
- The same alias maps to the same certificate or key/certificate pair.
- The same CA certificates map to the same certificate revocation lists.
- A revoked or expired certificate is not present.
- All CRL information is valid.

Important! After you resolve all data inconsistencies, do not make any further changes to the smkeydatabase instances until all migrations are complete

Back up an Existing Configuration

A backup of your configuration and key database is useful for system recovery or migration.

To back up a configuration, copy the key database and export the configuration data. The XPSExport tool, which is shipped with Federation Manager, lets you export the configuration data to an XML file.

Important! Federation transactions fail during the export process.

To back up a configuration

1. Copy the key database and save it in a safe location. The key database is in the following directory:

   federation_mgr_home/siteminder/smkeydatabase

2. Log in to the Federation Manager UI.

3. Select the Federation tab and click Partnerships.

   The View Federation Partnerships window opens.

4. Select Deactivate from the Action menu next to each active partnership in the Federation Partnership list.

5. Export the Federation Manager configuration by entering the following command from a command window:

   XPSExport *export_file_name* -xa -passphrase *passphrase*

   export_file_name

   Names the output file that results from the export. The output from XPSExport is in XML format, therefore, the file name must end with the extension **.xml**.

   passphrase

   Specifies the passphrase required to encrypt sensitive data. The passphrase must be at least eight characters and must contain at least one digit, one uppercase and one lowercase letter. If the passphrase contains a space, then it must be enclosed in quotes.

   NOTE: If you do not want to enter the passphrase directly, you can leave it off the command. XPSExport then prompts you for a passphrase and a passphrase confirmation, which is not echoed to the screen.

You now have a copy of the key database and an XML file that contains encrypted configuration data.

Upgrade to Federation Manager r12.5 on Windows

On a Windows system running an operating platform that supports Federation Manager, you can upgrade directly to Federation Manager r12.5 on the same operating platform.

If you are running your existing system on a pre-12.5 operation system, migrate the configuration (see page 59); you cannot directly upgrade.

Note: You do not need to deactivate your partnerships before upgrading.

Run the r12.5 Federation Manager installer executable to upgrade. The upgrade preserves your previous Federation Manager configuration.

Important! Be aware of the following installation restrictions:

- Do not install Federation Manager on a system where the SiteMinder Policy Server or Secure Proxy Server (SPS) is already installed. Installing Federation Manager on a SiteMinder system could negatively impact the existing SiteMinder installation.
- Do not install Federation Manager on a system where there is an existing Apache Web Server or Apache Tomcat Server.

If the installer detects the smkeydatabase file, the installer performs the following actions:

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

Important! If the smkeydatabase migration fails, do not return system back to the original environment because this action causes all transactions that require the certificate data to fail.

To locate installation kits

1. Log onto the CA Technical Support site.
2. Click Download Center.
3. Search the Download Center for the installation kit you need.

To upgrade Federation Manager on Windows

1. Exit all applications that are running.
2. Navigate to the folder where you plan to run the installation program.
3. Copy the installation executable to the folder.

   Note: View a list of installation executables.

4. Double-click the *installation_executable*.

   The installation wizard starts.

5. Go through the installation.

6. Review the installation settings and click Install.

7. The installation program runs and upgrades Federation Manager.

   Restart the system when prompted.

8. After the upgrade is complete, clear all temporary files in the browser so that the correct Federation Manager files load.

Actions to Take if an Upgrade Error Occurs

If the database upgrade fails, Federation Manager displays an error message telling you to run the policy_store_upgrade script. The upgrade script (policy_store_upgrade.bat) is located in *federation_mgr_home*/install_config_info.

If you experience other problems during the installation, review the installation log file CA_Federation_Manager_InstallLog.log and the upgrade log file CA_Federation_policy_store_upgrade.log. Both files are the directory *federation_mgr_home*/install_config_info.

Upgrade to Federation Manager r12.5 on UNIX

On a UNIX system, you can upgrade directly to Federation Manager r12.5 on the same operating platform and the same database.

If you are running your existing system on a pre-12.5 operation system, migrate the configuration (see page 59); you cannot directly upgrade.

Run the r12.5 Federation Manager installer. The upgrade preserves your previous configuration.

If the installer detects the smkeydatabase file, the installer performs the following actions:

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

Important! If the smkeydatabase migration fails, do not return system back to the original environment because this action causes all transactions that require the certificate data to fail.

These instructions are for GUI and Console Mode installations on UNIX systems. The steps for the two modes are the same, with the following exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number.
- Press ENTER after each step to proceed through the process.
- The prompts for each mode will help guide you through the process.
- You can type BACK to visit the previous step.

Important! Be aware of the following installation restrictions:

- Do not install Federation Manager on a system where the SiteMinder Policy Server or Secure Proxy Server (SPS) is already installed. Installing Federation Manager on a SiteMinder system could negatively impact the existing SiteMinder installation.
- Do not install Federation Manager on a system where there is an existing Apache Web Server or Apache Tomcat Server.

Run the r12.5 Federation Manager installer to upgrade Federation Manager. Select the installer for your platform.

To locate installation kits on the Support site

1. Log onto the CA Technical Support site.
2. Click Download Center.
3. Search the Download Center for the installation kit you need.

To upgrade Federation Manager

Important! Do not run the upgrade as the root user. If you try to install as root, the installation aborts and you receive an error message. Instead, create a new user account to install Federation Manager.

1. Exit all applications that are running.

   Note: You do not need to deactivate your partnerships before upgrading.
2. If necessary, add execcutable permissions to the installation file by running the chmod command, for example:

   chmod +x ca-fedmgr-12.5-sol.bin
3. Navigate to the folder where you plan to run the installation program.
4. Copy the installation binary to the folder.

5. Enter one of the following commands in a command window:
   - **GUI Mode:** ./*installation_binary*
   - **Console Mode:** ./*installation_binary* -i console

   Example (GUI mode): ./ca-fedmgr-12.5-sol.bin

   The installation wizard starts.
6. Go through the installation.
7. Review the installation settings and click Install (GUI mode) or enter Y to install (Console mode).

   The Federation Manager installation program runs and then restarts the services.
8. After the upgrade is complete, clear all temporary files in the browser so that the correct Federation Manager files load.

Actions to Take if an Upgrade Error Occurs

In case of database upgrade failure, Federation Manager displays an error message that instructs you to run the policy_store_upgrade script. The upgrade script (policy_store_upgrade.sh) is located in *federation_mgr_home*/install_config_info.

If you experience other problems during the installation, review the installation log file CA_Federation_Manager_InstallLog.log and the upgrade log file CA_Federation_policy_store_upgrade.log. Both files are the directory *federation_mgr_home*/install_config_info.

Important! If the smkeydatabase migration fails, do not return system back to the original environment because this action causes all transactions that require the certificate data to fail.

Upgrades from Environments with the SiteMinder Connector Enabled

If you upgrade from an environment that uses the SiteMinder Connector, the required data is already present for the upgraded product to use.

After an upgrade, existing partnerships that use the Connector operate without requiring any change. Regardless of its state before the upgrade, you can deactivate and edit partnerships to enable or disable the Connector. If the SiteMinder Connector was enabled previously, you can disable it for a given partnership. If the Connector was disabled previously, you can enable it for a given partnership.

Chapter 4: Migrate to Federation Manager r12.5

This section contains the following topics:

Upgrade and Migration Paths for Federation Manager

An upgrade is an update to a new version of Federation Manager on a system running an existing 12.x version of Federation Manager. An upgrade requires that the existing system be running an operating system, a database, and a JDK that the new version of Federation Manager supports.

A migration is a replicated configuration from an existing system to a system with a new r12.5 installation. The new Federation Manager system must be communicating with a supported database version.

Notes:

- Your migration to a r12.5 environment must include a supported database. If your environment is using a database that is not supported by r12.5, install a supported database server and move over your data to the new database. Finally, migrate to r12.5.
- If you upgrade to r12.5 and the Federation Manager Agent for Windows Authentication is installed, upgrade the Agent to the same version as Federation Manager. Otherwise, the Agent fails to work properly.

For specific version information, see the Federation Manager Platform Support Matrix on the Technical Support site.

You can upgrade or migrate to r12.5 based on these available paths:

Windows

Existing Federation Manager Version	Database Works with r12.5?	Upgrade or Migrate
r12.0 including all SPs	No	Migrate to r12.5
r12.1 including all SPs	No	Migrate to r12.5
r12.1 SP3	Yes	Upgrade to r12.5

Solaris/Linux

Existing Federation Manager Version	Database Works with r12.5?	Upgrade or Migrate
r12.0 including all SPs	No	Migrate to r12.5
r12.1 including all SPs	No	Migrate to r12.5
r12.1 SP3	Yes	Upgrade to r12.5

FIPS Migration

Federation Manager supports migration from a non-FIPS to a FIPS-only environment; however, the migration process is complex. If you want to migrate from a non-FIPS to a FIPS-only environment, first complete the upgrade to r12.5. After a successful upgrade, follow the FIPS migration process.

How to Migrate to r12.5

Your pre-r12.5 deployments can be running on operating platforms or use databases that r12.5 does not support. Therefore, migrate from your pre-r12.5 environment to r12.5.

Migrate a Federation Manager configuration to a new system to replicate the configuration. Copying an existing configuration avoids repeating the entire configuration process on the new system.

Complete the following tasks to migrate to a r12.5 system:

Important! Follow the import steps exactly as outlined. Do not access the Certs & Keys tab in the Federation Manager UI until the copying procedure is complete.

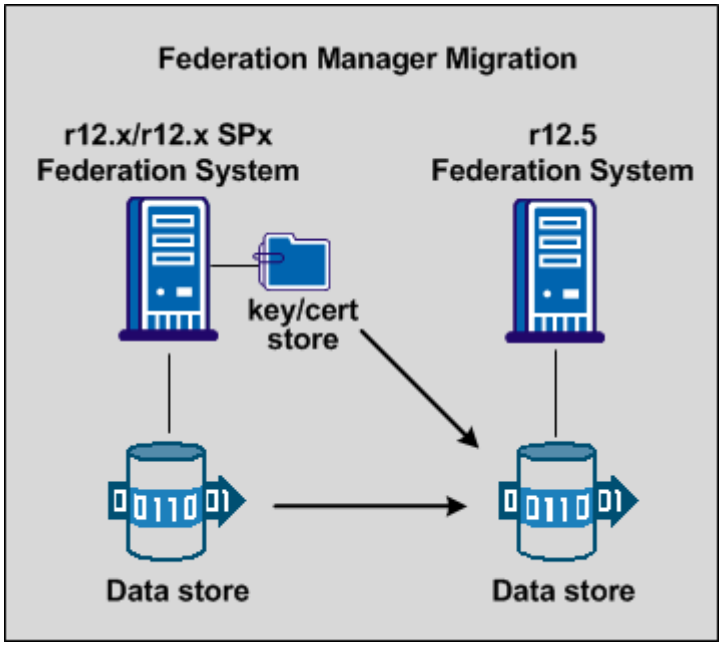
1. Synchronize multiple key databases (for migrating a cluster) (see page 52)
2. Export the existing configuration to an XML file. (see page 64)
3. Return the existing system to its original state. (see page 66)
4. Run the installation program on the new system. (see page 67)
5. Import the existing configuration to the new system (see page 67).
6. Migrate the key database to the certificate data store (see page 69).
7. Migrate SSL key and certificate data (see page 71).

After all the data is migrated, reactivate partnerships.

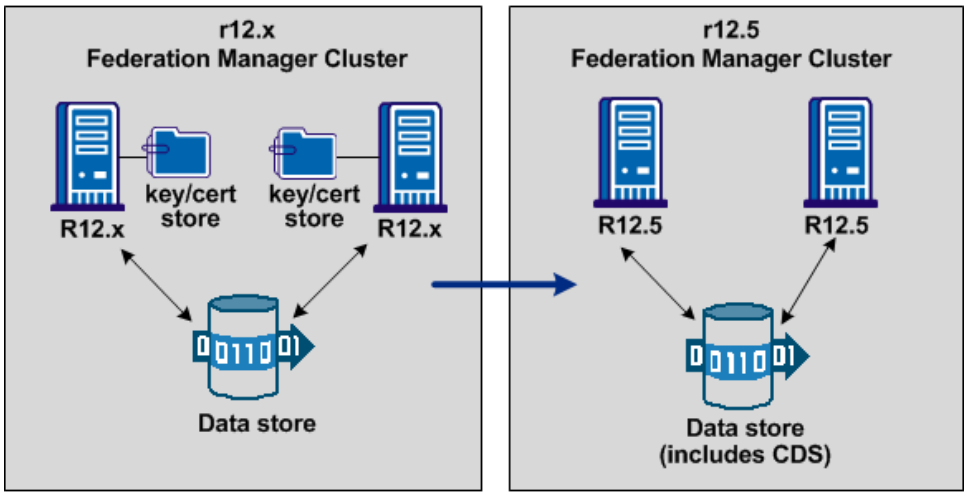
Note: The XPSExport and XPSImport tools are shipped with the product.

Important! We recommend that you perform the migration in a test environment not in a production environment.

The following figure shows the migration path from a single system.



The following figure shows the migration path for a cluster environment.



You can set up a Federation Manager cluster to support failover. You can migrate from an existing r12.x cluster to a new cluster, using a procedure similar to a non-cluster migration. To migrate a cluster, you set up a new r12.5 system for each system in your existing cluster. The systems in a cluster share one data store. You migrate all data to the new r12.5 data store.

Follow these steps:

1. Export the configuration to an XML file and copy the key database. The exported file can act as a backup configuration.
2. Return the existing system to its original state. You deactivate partnerships to export the configuration, so you must reactivate the partnerships to use the original system and its configuration.
3. Synchronize key database instances.
4. Install and configure Federation Manager on each new system.
5. Configure each new system. Use the same settings for the new system that are used for the original system. The following settings for the new system must match:
   - **Deployment mode**

     Use the same deployment mode (proxy or standalone) for the new system.
   - **SiteMinder Connector**

     If SiteMinder is enabled on the original system, it must be enabled for the new system.

- **Port numbers**

  When running the Configuration wizard, specify the same ports for the new system that the original system used.

- **Virtual Host Name**

  If the original system used a virtual host, use the same virtual host name on the new system. Additionally, make the appropriate entries in the host file for the new system.

6. Import the exported configuration from the original system to the new system.

This process is detailed in the following sections.

Synchronize Multiple Key Databases

Pre-12.5 systems stored private key and certificate data in a key store called smkeydatabase. This data now resides in the certificate data store, which is colocated with the data store. The certificate data store is replacing the requirement that each federation system in the environment access a local smkeydatabase.

As part of the upgrade, the installer automatically backs up the local smkeydatabase and tries to migrate all content to the certificate data store. This process compares the smkeydatabase and CDS before starting the migration. The purpose of the comparison is to identify data inconsistencies, such as the same alias mapping to different certificates, that can prevent a successful migration.

In a cluster environment, there are multiple instances of the smkeydatabase. Before you upgrade or migrate to r12.5, synchronize all smkeydatabase instances so that the information is consistent. Synchronizing the databases helps ensure that no inconsistencies arise as each instance is migrated to the CDS.

Resolve all data inconsistencies between smkeydatabase instances from the Certs and Keys tab in the Administrative UI. Confirm that the following data is consistent across key database instances:

- Each CA certificate must reference certificate revocation lists consistently across instances.
- **Example:** A CA certificate consistently references certificate revocation lists in an LDAP directory service.
- The defaultentpriseprivatekey alias represents the same private key/certificate pair in all instances.
- The same alias maps to the same certificate or key/certificate pair.
- The same CA certificates map to the same certificate revocation lists.
- A revoked or expired certificate is not present.
- All CRL information is valid.

Important! After you resolve all data inconsistencies, do not make any further changes to the smkeydatabase instances until all migrations are complete

Export the Configuration to an XML File

Export the configuration of the existing system to an XML file so you can replicate the pre-r12.5 configuration onto the new system. Use the XPSExport tool to complete this task.

The XPSExport tool shipped with Federation Manager lets you export all data in the data store to an XML file.

Important! Federation transactions fail while the configuration backup is in process.

To export a Federation Manager configuration

1. Copy the key database directory and save it in a safe location. The key database is in the following directory:

   federation_mgr_home/siteminder/smkeydatabase

   You copy this directory to the other system during the migration process.

2. Log on to the Administrative UI.

3. Select the Federation tab and click Partnerships.

   The View Federation Partnerships window opens.

4. Select Deactivate from the Action menu next to each active partnership in the Federation Partnership list. This deactivates all the active partnerships.

5. If you enabled SSL for the artifact back channel or for the Federation Manager UI, you must disable it, as follows:

   a. Click the Infrastructure tab and select SSL Configuration.

      The SSL Configuration dialog opens.

   b. Click Enable in the Embedded web SSL Configuration group box to change the setting to Disable.

   c. Click Activate in the Administrative UI SSL Configuration group box to change the setting to Deactivate.

6. If you changed the SSL status (enabled or disabled), restart the Federation Manager services as follows.

   - **Windows**

     Use the Federation Manager stop and start shortcuts as follows. If you logged in as a network user and not a local administrator, right-click the shortcut and select Run as administrator.

     a. Start, All Programs, CA, FederationManager, Stop services

     b. Start, All Programs, CA, FederationManager, Start services

   - **UNIX**

     a. Open up a command window.

     b. Run the following scripts:

     federation_mgr_home/fedmanager.sh stop

     federation_mgr_home/fedmanager.sh start

     Note: Do not stop and start the services as the root user.

7. Export the configuration by entering the following command from a command window:

   XPSExport *export_file_name* -xa -passphrase *passphrase*

   export_file_name

   Names the output file that results from the export. The output from XPSExport is in XML format, therefore, the filename should end with the extension **.xml**.

   passphrase

   Specifies the passphrase required to encrypt sensitive data. It must be at least eight characters and must contain at least one digit, one upper case and one lower case letter. If the passphrase contains a space, then it must be enclosed in quotes.

   NOTE: If you do not want to enter the passphrase directly, you may leave it off the command. XPSExport then prompts you for a passphrase and a passphrase confirmation, which will not be echoed to the screen.

   You now have an XML file that contains encrypted configuration data, which you can use to replicate the configuration on a different system.

8. After you successfully back up the configuration, return the backed-up system to its original state (see page 66).

Return the Existing System to its Original State

After you successfully export a configuration and copy the key database, reactivate all partnerships and reenable SSL. Restore your original system so you can use it, if necessary.

To return the existing system to its original state

1. Log on to the Federation Manager UI.
2. Select the Federation tab and click Partnerships.

   The View Federation Partnerships window opens.
3. Select Activate from the Action menu next to each deactivated partnership in the Federation Partnership list. This re-activates all the partnerships.
4. If you disabled SSL, you have to re-enable it, as follows:
   a. Click the Infrastructure tab and select SSL Configuration.

      The SSL Configuration dialog opens.
   b. Click Disable in the Embedded web SSL Configuration group box to change the setting back to Enable.
   c. Click Deactivate in the Administrative UI SSL Configuration group box to change the setting to Activate.
5. If you changed the SSL status (enabled or disabled), restart the Federation Manager services as follows.
   - **Windows**

     Use the Federation Manager stop and start shortcuts as follows. If you logged in as a network user and not a local administrator, right-click the shortcut and select Run as administrator.

     a. Start, All Programs, CA, FederationManager, Stop services

     b. Start, All Programs, CA, FederationManager, Start services
   - **UNIX**

     a. Open up a command window.

     b. Run the following scripts:

     federation_mgr_home/fedmanager.sh stop

     federation_mgr_home/fedmanager.sh start

     Note: Do not stop and start the services as the root user.

Run the Federation Manager Installation Program

Run the installation program on the new system before migrating your configuration.

Follow these steps:

1. Install Federation Manager using the same settings for the new installation that were used for the installation of the original system.
2. Set up a new database instance to import the <fedmg> data objects.

   Important! Do not use an existing database. The import fails if you do.
3. Run the Configuration wizard, specifying the new database instance when prompted.

   Use the same settings for this new configuration used for the original system. These settings include:

   - Deployment mode
   - Port numbers
   - Virtual Host Name
   - SiteMinder Connector

Import the Existing Configuration to the New System

1. Import all the configuration data using the XPSImport command. The syntax is as follows:

   XPSImport *export_file_name* -passphrase *passphrase*

   export_file_name

   Names the XML file that resulted from the export of the original configuration. The file name must end with the extension **.xml**.

   passphrase

   Specifies the passphrase that is required to decrypt sensitive data. This passphrase must be the same one that encrypted the data for the export to the file. Obtain the passphrase from the administrator who created the XML file originally.

   The passphrase must be at least eight characters and must contain at least one digit, one upper case, and one lower case letter. If the passphrase contains a space, then it must be enclosed in quotes.

2. Stop Federation Manager services according to your platform.

   - Windows

     Use the Federation Manager stop shortcut. If you logged in as a network user and not a local administrator, right-click the shortcut and select Run as administrator.

     Select Start, All Programs, CA, FederationManager, Stop services.

   - UNIX

     a. Open a command window.

     b. Run the script *federation_mgr_home*/fedmanager.sh stop

   Note: Do not stop and start the services as the root user.

3. For environments using an ODBC database (SQL or Oracle) as a user store, you must designate a data source name for the database.

   Windows:

   a. Go to the Data Sources (ODBC) from the Administrative Tools control panel.

   b. Add a new data source entry and specify a data source name for that entry.

   Refer to Windows documentation for adding data sources.

   UNIX:

   Modify the system_odbc.ini file to include the data source name (DSN) for the database. This DSN names the database in use before the migration. This DSN entry is required for the Federation Manager system to connect to the database and complete transactions.

   a. Navigate to the directory *federation_mgr_home*/siteminder/db.

   b. Open the system_odbc.ini file in a text editor.

   c. Add the DSN.

   d. Save the file.

   Note: You can add SQL and Oracle data sources in the same system_odbc.ini file.

4. Rerun the Configuration wizard, using the same settings as the Federation Manager configuration on the original system. These settings include:

   - Deployment Mode
   - Port numbers
   - Virtual Host Name
   - SiteMinder Connector

   Important! If you manually changed the Apache Tomcat http.conf file or the SPS server.conf file, make those same changes to those files on the new system.

5. Migrate SSL keys and certificate by doing one of the following tasks:
   - Migrate SSL keys and certificates to the new system. Follow the SSL migration procedure. Migrating SSL data lets you avoid the purchase of a new key or certificate.
   - Generate a new key/certificate request and then get the certificate signed. SSL certificates are not included in the imported configuration file.

After all the data is migrated, reactivate partnerships.

Migrate the Key Database to the Certificate Data Store

If your environment contains one or more key databases (smkeydatabase), migrate the contents to the r12.5 certificate data store.

Note: To migrate SSL keys and certificates, review the SSL migration procedure (see page 71).

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

- The certificate data store is collocated with the data server. A single certificate data store replaces the need for an individual smkeydatabase instance on each host system.
- As part of the upgrade, all smkeydatabase content is automatically backed up and migrated to the certificate data store.
- A Federation Manager system can only communicate with a certificate data store. A smkeydatabase does not operate in compatibility mode.

  Important! If the migration of the smkeydatabase fails, do not return Federation Manager to the environment. Returning the system 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 Federation Manager systems share a common view into the same database server and 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 SiteMinder environment:
  - Certificate authority (CA) certificates
  - Public and private keys
  - Certificate revocation lists

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

Run the Migration Utility to Move Data to the CDS

After you review the considerations for migrating the key database to the CDS, run the migration utility, named smmigratecds.

Follow these steps:

1. Be sure that all r12.x smkeydatabases are synchronized (see page 52).
2. Log in to an r12.x host system and go to the following location:

   federation_mgr_home\siteminder\config\properties

   federation_mgr_home

   Specifies the Federation Manager installation path.
3. Copy the following file

   smkeydatabase.properties
4. Log in to an r12.5 host system and complete the following steps:
   a. Go to the following location:

      federation_mgr_home\siteminder\config\properties
   b. Rename the r12.5 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 r12.5 and the 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 r12.5 version.

      Windows Example

      DBLocation=C:\CA\FederationManager\siteminder\smkeydatabase

      Solaris/Linux Example

      DBLocation=export/fedmgr/CA/FederationManager/siteminder/smkeydatabase

f. Save the r12.x properties file and close the r12.5 properties file.

g. Create the following directory at the root of the Federation Manager installation:

```
smkeydatabase
```

Windows Example:

```
C:\Program
Files\CA\FederationManager\siteminder\smkeydatabase
```

Solaris/Linux Example

```
export/fedmgr/CA/FederationManager/siteminder/smkeydatabase
```

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

6. Return to the r12.5 host system and complete the following steps:

   a. Add the contents of the r12.x smkeydatabase directory to the r12.5 smkeydatabase directory you created.

   b. Migrate the smkeydatabase to the certificate data store by entering the following command:

   ```
   smmigratecds
   ```

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

The migration is complete.

If the key database migration fails, you can migrate to the CDS manually. Refer to the information on how to troubleshoot a key database migration (see page 100).

Migrate SSL Keys and Certificates (optional)

For Federation Manager r12.5, the SSL key and certificate files for the embedded Apache and Tomcat servers are encrypted. For releases 12.0 and 12.0 SP1, these files are not encrypted. To avoid purchasing a new key/certificate pair for an encrypted file, migrate existing key or certificate files from Federation Manager r12.0/r12.0 SP1 to r12.5. You can also export these files for backup purposes without migrating them.

Important! For Federation Manager systems before r12.1, the embedded Tomcat server uses a self-signed certificate. You cannot use this self-signed certificate for a migration to r12.5. Purchase a signed certificate and upgrade the Tomcat SSL configuration with the signed certificate.

For Apache, you can migrate files for SSL connections beginning at Federation Manager r12.0. For Tomcat, you can migrate files only from Federation Manager r12.1 forward because in Federation Manager 12.0, a self-signed certificate secured the Tomcat key store. Beginning with r12.1, Federation Manager requires that a Certificate Authority signs the certificate.

Migrating SSL keys and certificate files is useful in the following situations:

- To move to a different version of Federation Manager on a new system instead of upgrading an existing system. Migrate the SSL keys or certificates from the existing system to the new system.
- To migrate SSL keys and certificates from one system in a cluster to another. Migrating lets you reuse the keys and certificates. For example, if a load balancer passes SSL requests to the Federation Manager systems in a cluster, each system must use the same keys and certificates. Therefore, you would migrate keys and certificates from one system to the other.

Note: If you upgrade a Federation Manager 12.0 system to Federation Manager r12.5, the installer automatically upgrades Apache and Tomcat SSL key and certificate files to encrypted files. This automatic does not apply to migrations.

The Federation Manager certificate and private key files are as follows:

Apache

- The server.key file contains a private key.
- The server.cert file contains a server certificate.

Tomcat

- For Federation Manager r12.0, the tomcat.keystore file contains a self-signed certificate. For Federation Manager r12.x, the tomcat.keystore file contains a CA-signed certificate and private key pair.

To migrate or export these files, use the Federation Manager SSL utility named migratessl. The migration utility is included with Federation Manager r12.5 as a batch file for Windows systems and a shell script for UNIX systems. Federation Manager installs the tool in the *federation_mgr_home*/bin folder.

The process to migrate SSL files is as follows:

1. Copy the key and certificate files from the existing Federation Manager system to any location on the r12.5 system.
2. Copy the migratessl tool to the location where you copied the key and certificate files.
3. If you migrate signed certificates, export the Certificate Authority certificate that signed the SSL certificate. Before you continue with the migration, import the CA certificate.

Note: You can also skip this migration process, generate a new key/certificate request, and then get the certificate signed. SSL certificates are not included in the imported configuration file.

Copy Key and Certificate Files from the r12 System

To use the SSL migration tool, first gather the key and certificate files for the Federation Manager system from which you plan to migrate or export then copy them.

To copy the SSL key and certificate files

1. Locate the files on the existing Federation Manager system.

   The Apache SSL key and certificate files are in the following locations:

   - *federation_mgr_home*/secure-proxy/SSL/keys/server.key
   - *federation_mgr_home*/secure-proxy/SSL/certs/server.crt

   The Tomcat SSL key store file is in the following location:

   - *federation_mgr_home*/secure-proxy/SSL/keys/tomcat.keystore
2. Copy the key and certificate files to any location on the new Federation Manager machine.

Copy the SSL Migration Tool to Same Folder as the Key/Certificate Files

The SSL migration tool requires software that is deployed with Federation Manager 12.1 SP3. Run the tool on the machine where the Federation Manager 12.1 SP3 product has been installed. Specifically, the tool has to reside in the same folder where you copied the files to be migrated.

To copy the SSL utility tool

1. Navigate to *federation_mgr_home*/bin on the r12.5 system.
2. Copy the migratessl file (.bat or .sh) to the location on the r12.5 system where you copied the key and certificate files.

Migrate or Export SSL Keys and Certificates

Complete the SSL key or certificate file migration by running the migratessl utility.

Follow these steps:

1. Import the Certificate Authority certificate that originally signed the SSL certificate you are migrating.
   a. On the system from which you are migrating, export the CA certificate using the Federation Manager UI.
   b. On the new system to which you are migrating, import the CA certificate using the Federation Manager UI.
2. Open a command window on the new system where you copied the existing key or certificate files.
3. Navigate to the folder where you copied the components.
4. Specify the migratessl command with the necessary command arguments. Refer to the list of migration tool command arguments (see page 75) for all the options.

   Examples

   - To migrate the SSL server.key for Apache SSL connections, enter:

   ```
   migratessl.bat -op migrate -keytype Apache
   -sourcefile server.key -certfile server.crt
   -sourcever 12.0 -sourceos Windows -oldpwd admin1
   -newpwd admin2 -issueralias trustedca
   ```

   - To migrate a key/cert file for Tomcat SSL connections, enter:

   ```
   migratessl.sh -op migrate -keytype Tomcat
   -sourcefile tomcat.keystore -sourcever 12.1
   -sourceos UNIX -issueralias trustedca
   -oldpwd admin1 -newpwd admin2
   ```

   - To export a key/cert file for Tomcat SSL connections, enter:

   ```
   migratessl.sh -op export -keytype Tomcat
   -sourcefile tomcat.keystore -sourcever 12.1
   -sourceos UNIX  -dest ca/federationmgr/secure-proxy/
   SSL/keys/ -oldpwd admin1 -newpwd admin2
   ```

If you are migrating SSL keys and certificates as part of an entire configuration migration, complete the migration process by reactivating partnerships.

SSL Migration Tool Command Arguments

The migratessl tool is invoked at the command line. When entering a command:

- Follow each command agrument (except for Help flags) by only one value.
- Enclose values that have spaces, such as directory paths in double quotes.

Command Argument	Meaning
-op	Migrate or Export Default: Migrate When exporting for Apache, the tool exports a server.key file and a server.crt file, if you specify the -certfile argument. For Tomcat, the tool exports a tomcat.p12 file, which is a PKCS#12 key/cert file.
-keytype	Apache or Tomcat Default: Apache
-sourcefile	Name of the file containing the SSL key (Apache) or the key store containing the key and certificate (Tomcat).
-certfile	Name of the file containing the Apache SSL server certificate (Apache only).
-sourcever	Federation Manager version the key or certificate comes from, such as 12.0, 12.1. Default: 12.0
-sourceos	Operating system of the environment the key comes from, Windows or UNIX. **Note:** There is no Linux option because Linux support was introduced in r12.1 SP3. Default: The OS of the machine where the tool is being run.
-dest	Path to the folder for output files. This option is ignored for migration. Default for Export: Current folder **Important!** If you do not specify a destination folder, the files that you are migrating are overwritten.
-issueralias	The alias of the CA certificate that signed the certificate you are migrating. Import the CA certificate under this alias to the destination Federation Manager system. (Used only for Migrate; ignored for Export.)

-oldpwd	The Federation Manager administrative password of the system that is the source of the key.
-newpwd	The Federation Manager administrative password of the system to which the key is being moved.
-h	Displays these usage instructions.
-help	Displays these usage instructions.
-?	Displays these usage instructions.

Reactivate Federation Partnerships

After you complete the migration, reactivate the partnerships.

Note: If the SiteMinder Connector was enabled on a previous system, it is configured and enabled by default on the new system. All partnerships then use the Connector by default. To disable the Connector for individual partnerships, you have to edit the specific partnership.

1. Log back in to the Federation Manager UI.

   Important! Do not access the Certs & Keys tab in the Federation Manager UI until this entire procedure is complete.

2. Select the Federation tab and click Partnerships.

   The View Federation Partnerships window opens.

3. Select Activate from the Action menu next to each deactivated partnership in the Federation Partnership list.

4. (Optional) If the SiteMinder Connector was enabled in the original configuration, reestablish the Connector by doing the following:

   a. Click the Infrastructure tab and select Deployment Settings.

   b. Reconfigure the SiteMinder Connector settings using the same values from the original configuration.

   c. Click Register Host to reregister Federation Manager with the SiteMinder Policy Server.

5. (Optional) If SSL was enabled in the original configuration, reenable it as follows:

   a. Click the Infrastructure tab and select SSL Configuration.

      The SSL Configuration dialog opens.

   b. Click Disable in the Embedded web SSL Configuration section to change the setting back to Enable.

   c. Click Deactivate in the Administrative UI SSL Configuration section to change the setting to Activate.

   Before enabling SSL for the embedded web server, migrate existing SSL keys and certificates or generate a new key/certificate request. Finally, get the certificate signed. SSL certificates are not included in the imported configuration file.

6. If you changed the SSL status (enabled or disabled), restart the Federation Manager services as follows.

   - **Windows**

     Use the Federation Manager stop and start shortcuts as follows. If you logged in as a network user and not a local administrator, right-click the shortcut and select Run as administrator.

     a. Start, All Programs, CA, FederationManager, Stop services

     b. Start, All Programs, CA, FederationManager, Start services

   - **UNIX**

     a. Open up a command window.

     b. Run the following scripts:

        federation_mgr_home/fedmanager.sh stop

        federation_mgr_home/fedmanager.sh start

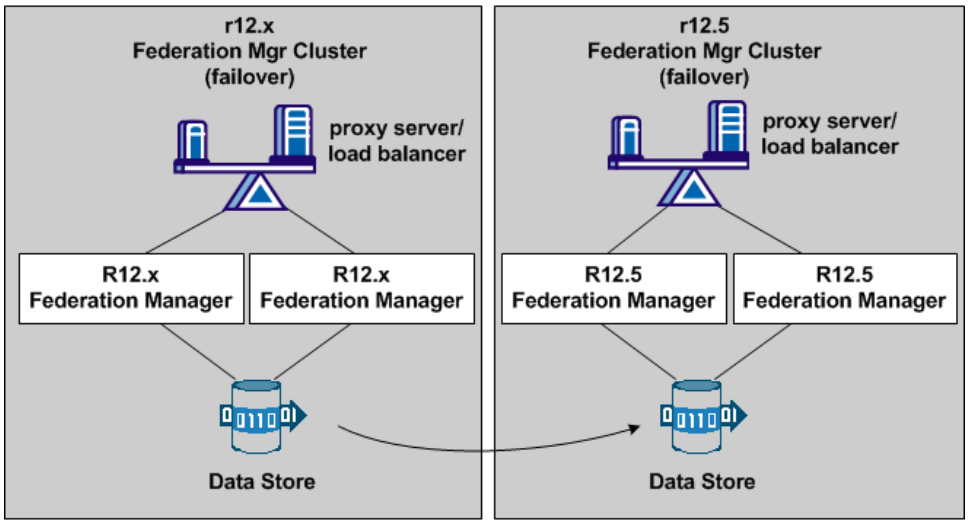
     Note: Do not stop and start the services as the root user.

The new system is now operating with the same configuration as the original system.

How to Migrate a Failover Deployment

You can migrate an existing r12x failover deployment to an r12.5 failover deployment.

The following figure shows a clustered environment to support failover.



Migrating a failover deployment to r12.5 requires the following steps:

1. Copying your existing configuration to the new r12.5 systems.
2. Updating the proxy server or load balancer to pass the appropriate URLs to the new r12.5 systems.

Migrating an r12 Failover Deployment to r12.5

You can migrate an existing r12.x failover deployment to an r12.5 Federation Manager deployment.

To migrate a failover configuration

1. Install r12.5 onto each machine in your deployment.
2. Run the configuration wizard on the first upgraded machine and enter the same information that was used for any previous configurations.

   To determine the existing configuration settings, go to the following file on the r12.x system:
   federation_mgr_home\install_config_info\ca-Federation-Config.properties.

3. Run the r12.5 configuration wizard on the second machine. Enter the following information:
   a. Database information from the first machine.
   b. All other entries from the ca-Federation-Config.properties file.
4. Log in to the Federation Manager UI.
5. From the Infrastructure tab, select System Settings.

   The Configure System Settings dialog displays.
6. Change the Global Base URL in the UI to include the host and port of the Proxy Server or load balancer in your federated network. Setting this URL properly ensures that the default URL for all metadata used to create partnerships is correct.
7. Change the default base URL for the proxy engine to include the host and port of the Proxy Server or load balancer in your federated network. Setting this URL properly ensures that the default URL for all metadata used to create partnerships is correct.

   The base URL is defined in the server.conf file.

   To modify the server.conf file

   a. Navigate to *federation_mgr_home*/secure-proxy/proxy-engine/conf.
   b. Open the server.conf file in an editor.
   c. Go to the # Default Virtual Host section.
   d. Add the base URL to the **hostnames** setting using fully qualified host names, as follows:

      <VirtualHost name="default">

      hostnames="defaultbaseurl.ca.com:80, newbaseurl.ca.com:80"

      </VirtualHost>

      Note: Specify multiple *host_name:port* entries for the hostnames setting, separating each entry with a comma.
8. If you have enabled SSL for failover on an r12x system, you have to migrate the SSL configuration to the r12.5 primary and secondary system, as instructed in the SSL migration steps (see page 71).

Both Federation Manager systems are now pointing to the same database server and can be configured for failover from a proxy server or load balancer.

Set up Failover at the Proxy Server or Load Balancer

This guide assumes that the administrator of the proxy server or load balancer knows how to set up failover for their system.

At the proxy server/load balancer machine

1. For the proxy server configuration, identify one Federation Manager system as the primary host and the other as the secondary host.

   Do not configure load balancing for the machines.

2. Configure the server to pass the following URLs s to the Federation Manager machines:

   - /affwebservices/*
   - /siteminderagent/*

Other traffic can be routed through Federation Manager, depending on the deployment mode (standalone or proxy).

The proxy server or load balancer should now be able to failover to Federation Manager.

Chapter 5: Migrate Federation Manager to Use FIPS Encryption

This section contains the following topics:

FIPS Migration Issues to Consider

Be aware of the following issues before you migrate to FIPS_Only mode:

- If you deploy Federation Manager in FIPS_ONLY mode with the SiteMinder Connector enabled, the back-end SiteMinder system must be version r12x and be operating in FIPS_ONLY mode.

  If the SiteMinder system is r6.0 SP5, this system does not support FIPS-compatible operations, so Federation Manager cannot operate in FIPS_ONLY mode.

- Federation Manager releases prior to r12.1 do not support FIPS-approved encryption algorithms for private key generation. These releases support only MD5 as the signature algorithm for private key generation, which is not an approved FIPS algorithm.

  If you have private keys that use only MD5 as the signature algorithm, take the following actions at both sites in a partnership:

  - Generate new private keys
  - Get new certificates
  - Update all required partnerships with the new public keys.

How to Migrate from FIPS_COMPAT Mode to FIPS_Only Mode

The securing of sensitive data using the robust encryption algorithms provided by FIPS helps protect the data from security breaches and makes Federation Manager more secure overall.

You can migrate your Federation Manager system to operate using only FIPS-compatible encryption algorithms to secure sensitive data.

You can install Federation Manager in one of the following FIPS modes of operation:

FIPS_COMPAT

FIPS_COMPAT (compatibility) mode is the default FIPS mode of operation during installation. In FIPS_COMPAT mode, Federation Manager continues to support the current set of non-FIPS algorithms as well as the supported FIPS-compliant algorithms.

FIPS_COMPAT mode is compatible with previous versions Federation Manager. This compatibility enables environments with a version of Federation Manager earlier than r12.5 to interoperate with r12.5. FIPS_COMPAT is also suitable for any clients who are satisfied with the degree of security available in the current Federation Manager implementation.

If your organization does not require the use of FIPS, install Federation Manager in FIPS_COMPAT mode. No further configuration is required.

FIPS_ONLY

In FIPS_ONLY mode, the environment uses only FIPS-compliant algorithms to encrypt sensitive data.

Install Federation Manager in FIPS_ONLY mode for new installations where you want to use only FIPS-compliant algorithms.

Federation Manager allows only a one-way migration path from FIPS_COMPAT mode, which is the default mode through MIGRATE mode to FIPS_ONLY mode. FIPS_MIGRATE mode lets you transition a Federation Manager environment running in FIPS_COMPAT mode to FIPS_ONLY mode. In MIGRATE mode, Federation Manager continues using existing encryption algorithms for existing data as you migrate your environment to FIPS_ONLY mode. However, any new data requiring encryption is encrypted using only FIPS-compliant algorithms.

Important! An environment operating in FIPS_ONLY mode cannot interoperate with, or be backward compatible with earlier versions of Federation Manager, which includes custom software using older versions of Federation Manager APIs. If you have custom software built with pre-r12.5SDKs, recompile this software using the r12.5 SDKs to achieve the required support for FIPS_ONLY mode.

To migrate Federation Manager to FIPS_ONLY mode:

1. Deactivate any SSL configuration, if activated.
2. Back up your existing configuration.
3. Set the OPENSSL_FIPS environment variable.
4. Set the policy engine to FIPS_MIGRATE mode.
5. Reencrypt the policy store key.

6. Reencrypt the policy store administrator password.
7. Reencrypt the SiteMinder super user password.
8. Reencrypt client shared secrets.
9. Reencrypt policy and key store data.
10. Set the Administrative UI to FIPS_ONLY mode.
11. Set the embedded secure proxy engine to FIPS_ONLY mode.
12. Set the embedded policy engine to FIPS_ONLY mode.

Important! After you migrate to FIPS_ONLY mode, partnerships configured with non-FIPS approved certificates stop working and consequently, partnerships stop working. Reencrypt partnership data using FIPS-compliant algorithms before migrating to FIPS_ONLY operation.

The following sections describe each procedure in detail.

Deactivate the SSL Configuration

The first step to migrate to FIPS Only mode is to deactivate SSL for the Embedded web server or Administrative UI section. If you did not activate SSL to begin with, skip this step.

To deactivate SSL

1. Begin at the SSL Configuration dialog.
2. Deactivate any active service. To do this, click Deactivate in the Embedded web server and/or Administrative UI section.

   A confirmation prompt is displayed asking if you want to disable SSL.
3. Click Yes to complete the deactivation.
4. Restart the federation services according to your operating environment.
   - **Windows**

     Use the stop and start shortcuts as follows. If you logged in as a network user and not a local administrator, right-click the shortcut and select Run as administrator.

     a. Start, All Programs, CA, FederationManager, Stop services

     b. Start, All Programs, CA, FederationManager, Start services

- **UNIX**

  a. Open a command window.

  b. Run the following scripts:

  federation_mgr_home/fedmanager.sh stop

  federation_mgr_home/fedmanager.sh start

Note: Do not stop and start the services as the root user.

The SSL connection is no longer active and the SSL Configuration Status setting changes to **Server cert signed by CA, SSL ready**. The certificate and key files remain so you can re-enable SSL.

Back Up the Existing Configuration

You can restore an existing configuration as part of a system recovery, upgrade, or migration.

To restore a configuration, copy the key database and export configuration data. The XPSExport tool, which is shipped with Federation Manager, lets you export the configuration data to an XML file.

Important! While restoring a configuration, federation transactions will fail.

To export a configuration

1. Copy the key database and save it in a safe location. The key database is in the following directory:

   federation_mgr_home/siteminder/smkeydatabase
2. Log in to the Federation Manager UI.
3. Select the Federation tab and click Partnerships.

   The View Federation Partnerships window opens.
4. Select Deactivate from the Action menu next to each active partnership in the Federation Partnership list.

5. Export the Federation Manager configuration by entering the following command from a command window:

   XPSExport *export_file_name* -xa -passphrase *passphrase*

   export_file_name

   Names the output file that results from the export. The output from XPSExport is in XML format, therefore, the filename must end with the extension **.xml**.

   passphrase

   Specifies the passphrase required to encrypt sensitive data. The passphrase must be at least eight characters and must contain at least one digit, one uppercase and one lowercase letter. If the passphrase contains a space, then it must be enclosed in quotes.

   NOTE: If you do not want to enter the passphrase directly, you can leave it off the command. XPSExport then prompts you for a passphrase and a passphrase confirmation, which is not echoed to the screen.

You now have an XML file that contains encrypted configuration data. Use the XML file to restore a configuration.

Set the OPENSSL_FIPS Environment Variable

Enable FIPS mode by setting the OPENSSL_FIPS environment variable. Set this variable one time only when you are migrating from COMPAT mode to FIPS Only mode.

Follow these steps:

Windows

1. Access the Windows System Properties
2. Access the environment variables.
3. Add an environment variable as follows:

   Variable Name

   OPENSSL_FIPS

   Variable Value

   1
4. Save the new variable.

UNIX

1. Navigate to *federation_mgr_home*.
2. Edit the environment script, ca_federation_env.ksh.

3. Add the following the entry to the script:

   `OPENSSL_FIPS=1;export OPENSSL_FIPS=1`

4. Run the environment script, ca_federation_env.ksh to set the environment variables.

5. On UNIX systems only, run the *federation_mgr_home*/bin/migratessltofips.sh script.

   This script ensures that the private key associated with the SSL certificate is properly encrypted.

Set the Policy Engine to FIPS_MIGRATE Mode

The first step to migrate to FIPS_Only mode is to configure the policy engine in FIPS_MIGRATE mode.

Follow these steps:

1. Check that Federation Manager is in COMPAT mode. If it is not, reinstall and configure it to run in COMPAT mode.

2. From a command prompt, run the setFIPSmigration command, as follows:

   Windows

   Enter setFIPSmigration

   UNIX

   a. Navigate to *federation_mgr_home*/siteminder/bin.

   b. Enter setFIPSmigration.ksh

   c. Run the environment script, ca_federation_env.ksh to set the environment variables.

   The migration process begins.

3. Do one of the following:

   Windows

   Reboot the Federation Manager system.

   UNIX

   Restart the Federation Manager services by executing the following scripts from a command window:

   a. *federation_mgr_home*/fedmanager.sh stop

   b. *federation_mgr_home*/fedmanager.sh start

   Note: Do not stop and start the services as the root user. You must be a non-root user.

4. Look at the smps.log file to verify that the policy engine is now in MIGRATE mode.

   The location of the log file is *federation_mgr_home*/logs/server/smps.log.

The policy engine is now operating in FIPS_MIGRATE mode.

Reencrypt the Policy Store Encryption Key

The next step in the migration process is to re-encrypt the policy store encryption key.

To re-encrypt the policy store key

1. If you have not already downloaded the Federation Manager web kit, go to the Technical Support site and download the kit for your operating environment.
2. Copy smreg to *federation_mgr_home*/siteminder/bin.
3. Open a command prompt window.
4. Enter the following command at a command prompt:

   smreg -cf MIGRATE -key *admin_password*

   admin_password

   Specifies the Federation Manager administrator password you provided during installation.

5. Open the EncryptionKey.txt file in the directory *federation_mgr_home*\siteminder\bin.

   The new encryption key is present and has a prefix with a FIPS-compliant algorithm, such as AES.

The re-encryption is complete.

Re-encrypt the Database Administrator Password

The migration process requires that you reencrypt the database administrator password.

To reencrypt the password

1. From a command prompt, run the fedconfig utility as follows:

   Windows

   Navigate to *federation_mgr_home*/bin and enter fedconfig.bat.

   UNIX

   a. Navigate to *federation_mgr_home.*

   b. Run the environment script, ca_federation_env.ksh to set the environment variables.

   c. Go to the /bin directory.

   d. Enter fedconfig.sh.

   The fedconfig utility displays a list of utility options.

2. Enter 5 to change the database administrator password.
3. Enter C and enter the password that you entered when running the Federation Manager Configuration wizard.
4. Confirm the password entry.
5. Enter 0 to save the password and quit.

You successfully changed the password.

Re-encrypt the Super User Password

To migrate to FIPS_Only mode, re-encrypt the Federation Manager super user password.

To re-encrypt the super user password

1. If you have not already downloaded the Federation Manager web kit, go to the Technical Support site and download the kit for your operating environment.
2. Copy smreg to *federation_mgr_home*/siteminder/bin.

3. Enter the following command:

   smreg -cf MIGRATE -su *admin_password*

   admin_password

   Specifies the Federation Manager administrator password you provided during installation.

4. Delete smreg from siteminder\bin.

   Note: Deleting smreg prevents anyone from changing the password without knowing the previous one.

The super user password is now set.

Re-encrypt the Proxy Engine Agent Shared Secret

To migrate, re-encrypt the shared secret for the proxy engine Web Agent.

To re-encrypt shared secrets

1. Open a command prompt window.
2. Navigate to the SmHost.conf file, located at *federation-mgr_home*\secure-proxy\proxy-engine\conf\defaultagent\SmHost.conf.
3. Enter the following command, using the values in the SmHost.conf file for some of the settings.

   smreghost -i *policy_server_ip_address,port,port,port* -u a*dmin_user_name* -p *admini_password* -hn *host_name* -hc *host_config_object* -f *host_config_file_path* -o -cf MIGRATE

   policy_server_ip_address, port, port, port

   Specifies the IP address and port numbers of the policy engine. Look for the address in the SmHost.conf file. The default ports are 44441,44442,44443.

   You only have to specify the port numbers if you are using non-default ports. For non-default ports you can use the same number or different numbers for all three ports.

   admin_user_name

   Specifies the name of the administrator. Enter **siteminder** for this value when using the smreghost utility.

   admin_password

   Specifies the password for the Federation Manager administrator you specified during installation.

hostname

Specifies the name of the trusted host that the policy engine uses for host registration. Enter a unique value for this parameter. Do not use the hostname in the SmHost.conf file because that host name already exists in the policy store.

host_config_object

Indicates the name of the host configuration object that the policy engine uses. Look for the value of the hostname in the SmHost.conf file.

host_config_file_path

Specifies the location of the SmHost.conf file.

Example

```
smreghost -i localhost -u siteminder -p mypassword
-hn lfed-localhost20090511024942 -hc fed-localhost20090511024942
-f "C:\Program Files\CA\FederationManager\secure-proxy\proxy-engine
\conf\defaultagent\SmHost.conf" -o –cf  MIGRATE
```

After executing this command, the re-encryption of the shared secret is complete.

4. Navigate to the SmHost.conf file, located at the following directory:

   federation-mgr_home\secure-proxy\proxy-engine\
   conf\defaultagent\SmHost.conf

5. Open the SmHost.conf file and verify that the shared secret is present and has a FIPS-approved algorithm prefix, such as {AES}.

Re-encryption of the shared secret is complete.

Re-encrypt the Policy Store and Key Store Data

Re-encrypt policy and key store data so that is uses a FIPS-compatible encryption algorithm.

To re-encrypt policy and key store data

1. Open a command prompt window.
2. Export the key data by entering the following command

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

admin_name

Specifies the name of the administrator. You must enter siteminder for this value when using the smkeyexport utility.

admin_password

Specifies the password Federation Manager administrator.

export_file

Specifies the name of the file that results from the export. This file must end in an .smdif extension.

3. Export the policy store data by entering the following command

XPSExport *export_file* -xa –xs –xc -passphrase *passphrase* -v -e *file_name* -l *log_file*

export_file

Names the output file that results from the export. The output from XPSExport is in XML format, therefore, the filename should end with the extension **.xml**.

passphrase

Specifies the passphrase required to encrypt sensitive data. The passphrase must be at least eight characters and must contain at least one digit, one uppercase and one lowercase letter. If the passphrase contains a space, then it must be enclosed in quotes.

NOTE: If you do not want to enter the passphrase directly, do not specify it in the command. XPSExport then prompts you for a passphrase and a passphrase confirmation, which is not echoed to the screen.

file_name

Specifies the name of the error file where Federation Manager writes error messages.

log_file

Specifies the name of the log file where Federation Manager writes the results of the export. This file can be any name, but the extension .log is recommended.

You can enter a full path to the file or only the file name. If you enter only a file name, Federation Manager creates the file in the location where you are running the XPSExport command. The name you enter for this parameter should be different from the log_path value you enter when you import the policy store data.

4. Import the key data into the new or existing key store by entering the following command:

   Note: You may be using the policy store as your key store.

   smkeyimport -i*export_file* -da*dmin_name* -w*admin_password* -l -v -t -cf

   export_file

   Specifies the name of the XML file that resulted from the export of the original store.

   admin_name

   Specifies the name of the administrator. You must enter siteminder for this value when using the smkeyimport utility.

   admin_password

   Specifies the password Federation Manager administrator.

5. Import the policy store data into the new or existing policy store by entering the following command:

   XPSImport –fo *export_file* -passphrase *passphrase* -vT -vI -vW -vE -vF -l *log_path*

   export_file

   Names the XML file that resulted from the export of the original configuration.

   passphrase

   Specifies the passphrase required to decrypt sensitive data. The passphrase must be the same as passphrase you specified when you ran the XPSExport command in the previous step.

   log_path

   Specifies the location and name of the log file where Federation Manager writes the results of the import. This file can be any name, but the extension .log is recommended.

Set the Federation Manager UI to FIPS_Only Mode

After re-encrypting all the necessary data to use FIPS-compatible algorithms, confirm all that all the partnerships and the SSL configuration is FIPS-compatible.

Follow these steps:

1. Restart the federation services according to your operating environment.

   - **Windows**

     Use the stop and start shortcuts as follows. If you logged in as a network user and not a local administrator, right-click the shortcut and select Run as administrator.

     a. Start, All Programs, CA, FederationManager, Stop services

     b. Start, All Programs, CA, FederationManager, Start services

   - **UNIX**

     a. Open a command window.

     b. Run the following scripts:

     federation_mgr_home/fedmanager.sh stop

     federation_mgr_home/fedmanager.sh start

     Note: Do not stop and start the services as the root user.

2. Log in to the Federation Manager UI.

3. Navigate to Infrastructure, Deployment Settings.

   The Configure Deployment Settings dialog opens.

4. Verify that the Confirm button in the Deployment Settings section is active and the message Ready to Migrate to Only mode is set to Yes.

   If these two conditions are not met, one or more of the partnerships or the SSL configuration is not FIPS-enabled. A partnership is not FIPS-enabled because of the following reasons:

   - Redirect Mode setting in the Application Integration dialog using an Agent for Open Files with a PBE algorithm.

     If you configure the Redirect Mode setting to use an Agent for Open Files with a PBE encryption algorithm, the mode is not FIPS-compatible.

   - Delivery type for provisioning is set to the Agent for Open Files with a PBE algorithm.

     If you configure the Provisioning Delivery Type to use an Agent for Open Files with a PBE encryption algorithm, this delivery mechanism is not FIPS-compatible.

- Global Agent for Open Files settings for delegated authentication are set to the Agent for Open Files with a PBE algorithm.

  If you set the Agent for Open Files settings in the Deployment Settings dialog to use a PBE encryption algorithm, the cookie is not FIPS-compatible.

To correct these problems, do the following:

- If there are non-FIPS partnerships, deactivate these partnerships or verify that all such partnerships use FIPS-approved certificates and encryption algorithms.
- If the SSL configuration is not FIPS approved, deactivate SSL and configure it again using FIPS-approved certificates.

5. Click Confirm to migrate the UI to FIPS_ONLY mode.

The Administrative UI is now operating in FIPS_ONLY mode.

Set the Secure Proxy Engine to FIPS_Only Mode

Set the secure proxy engine to FIPS_Only mode as part of the migration process.

To set the secure proxy engine to FIPS_Only

1. Open a command window.
2. Navigate to *federation-manager_home*\secure-proxy\proxy-engine\conf\defaultagent\SmHost.conf.
3. Open the SmHost.conf file in a text editor.
4. Change the fipsmode setting from MIGRATE to ONLY.

   Example: fipsmode="ONLY"

The proxy engine is now operating in FIPS_Only mode.

Set the Policy Engine to FIPS_Only Mode

The final step in the migration process is to set the policy engine to FIPS_Only mode.

Follow these steps:

1. (Solaris only) Source the Federation Manager environment script, ca_federation_env.ksh to set the proper environment variables.
2. From a command prompt, run the setFIPSmigration command, as follows:

   Windows

   Enter setFIPSonly

UNIX

a. Navigate to *federation_mgr_home*\secure-proxy.

b. Enter setFIPSonly.ksh.

c. Run the environment script, ca_federation_env.ksh to set the environment variables.

After the command is successful, the words FIPS_ONLY appears at the command prompt.

3. Do one of the following:

Windows

Reboot the Federation Manager system.

UNIX

Restart the Federation Manager services by executing the following scripts from a command window:

a. *federation_mgr_home*/fedmanager.sh stop

b. *federation_mgr_home*/fedmanager.sh start

4. Verify that the policy engine is operating in FIPS_ONLY mode. Check the smps log in the directory *federation_mgr_home*\logs\server.

Obtain FIPS-Compatible SSL Certificates (Optional)

After you migrate Federation Manager to FIPS_Only mode, the server certificates that Federation Manager uses for SSL configuration must be FIPS-compatible. If the server certificates that Federation Manager is using for SSL are MD5 format, obtain new certificates that use a SHA1 algorithm, which is FIPS-compatible.

To determine whether you need to update the SSL certificates:

1. Verify the FIPS status of the current SSL certificates.

   These are the certificates for the embedded web server and the Federation Manager UI.

2. If the FIPS status is False, request a new certificate.

3. Upload the new FIPS-compatible a server certificate.

Specific procedures are described in the sections that follow.

Verify The FIPS Status of the SSL Certificate

Verify the FIPS status of the SSL certificates for the Embedded web server and the Administrative UI. Determine whether you need a new FIPS-approved certificate.

To verify the status of the SSL certificates

1. Log in to the Federation Manager UI.
2. Navigate to Infrastructure, SSL Configuration.

   The SSL Configuration dialog displays.
3. Look at the FIPS Approved field for the Embedded web server and the Administrative UI. Do one of the following:
   - If the FIPS Approved status is True, do not take any further action.
   - If the status is False, obtain a FIPS-approved certificate, as described in the following procedure.

Request a FIPS-Compatible Server Certificate

If the FIPS Approved setting for the Embedded web server or the Administrative UI is False, request a new FIPS-compatible certificate. If both components require a new certificate, generate a separate request for each component and complete the entire request process.

To request a FIPS-compatible server certificate

1. Log in to the Federation Manager UI.
2. Navigate to Infrastructure, SSL Configuration.

   The SSL Configuration dialog displays.
3. Click Request in the appropriate section for the component that requires a new certificate.

   The Request Certificate dialog displays.
4. Complete the fields in the Request Certificate dialog.

   You are required to request a certificate with a SHA-1signature algorithm so the certificate is FIPS-approved. Some CAs use MD5 by default unless asked to use a different algorithm.
5. Click Save.

   A file in PKCS#10 format is saved.
6. Submit the file to a Certificate Authority to receive new certificates. Contact your Certificate Authority for the appropriate procedure to submit a request.

   CA sends a response with a signed certificate.

7. Upload the new certificate to the Federation Manager key store, as described in the following procedure.
8. Repeat this procedure for another request, if necessary.

Upload the FIPS-Compatible Certificate

After you acquire a new certificate, upload it to the key store. If you requested more than one certificate, upload each one separately.

To upload a new certificate

1. Navigate to Infrastructure, SSL Configuration.

   The SSL Configuration dialog displays.
2. Click Browse next to the Signed Certificate Response field to locate the new signed response file.

   Note: You only need one key and certificate pair for the SSL features because SSL does not support more than one pair.
3. Select the CA that signed the SSL certificate from the pull-down menu in the CA Certificate field.

   If the CA certificate is not in the key store, import a copy of the CA certificate used to sign the SSL certificate request.
4. Click Import to import the certificate and complete the import steps.
5. Click Apply to upload the server certificate to Federation Manager.

   A confirmation message is displayed and the SSL Configuration changes to reflect that the certificate is now updated.
6. Click Activate and restart the SSL configuration.

   The FIPS Approved status must read True, indicating the certificate is FIPS-compatible.
7. Restart the federation services according to your operating environment.
   - **Windows**

     Use the stop and start shortcuts as follows. If you logged in as a network user and not a local administrator, right-click the shortcut and select Run as administrator.

     a. Start, All Programs, CA, FederationManager, Stop services

     b. Start, All Programs, CA, FederationManager, Start services

- **UNIX**

  a. Open a command window.

  b. Run the following scripts:

  federation_mgr_home/fedmanager.sh stop

  federation_mgr_home/fedmanager.sh start

  Note: Do not stop and start the services as the root user.

The server certificates for SSL configuration are now FIPS-compatible.

Chapter 6: Troubleshooting Federation Manager

This section contains the following topics:

Installation Troubleshooting

The following information may help you solve installation and configuration issues.

Trouble Getting a Federation Manager License or Downloading Software

Symptom:

You are having trouble getting a Federation Manager license or downloading Federation Manager software.

Solution:

Contact your Sales Account Manager for assistance.

Federation Manager UI or Component Services Not Starting

Symptom:

The Federation Manager UI does not start.

Solution:

1. Check whether the URL has the correct port and the correct host name.
2. Restart the federation services according to your operating environment.
   - **Windows**

     Use the stop and start shortcuts as follows. If you logged in as a network user and not a local administrator, right-click the shortcut and select Run as administrator.

     a. Start, All Programs, CA, FederationManager, Stop services

     b. Start, All Programs, CA, FederationManager, Start services

   - **UNIX**

     a. Open a command window.

     b. Run the following scripts:

     federation_mgr_home/fedmanager.sh stop

     federation_mgr_home/fedmanager.sh start

   Note: Do not stop and start the services as the root user.

Installation Fails When Running the Configuration Manager

Symptom:

The Federation Manager installation hangs or fails when you run the Configuration Manager.

Solution:

When you are prompted for database server information, enter the IP address for the Database Server instead of the fully qualified host name. Using the IP address lets the installation and configuration complete successfully.

Troubleshoot a Key Database Migration

The following sections detail ways to troubleshoot a migration of the key database to the certificate data store.

Status of SiteMinder Key Database Migration Unknown

Symptom:

I know that Federation Manager 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 *federation_mgr_home*\siteminder\bin.

federation_mgr_home

Specifies the Federation Manager installation path.

Follow these steps:

1. Log in to the 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.

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.

   If you run the smmigratecds utility, you can specify a log file.

   The default location for the log file is *federation_mgr_home*/siteminder/log.

   federation_mgr_home is the installation directory for Federation Manager.

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, review how to use smkeytool.

4. Migrate the key database manually (see page 103).

Certificate Data Store Error Appears

Symptom:

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

Solution:

Follow these steps:

1. Log in to the Federation Manager host system.
2. Run the following command:

   ```
   XPSDDInstall CDSObjects.xdd
   ```

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

3. 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.

4. Migrate the key database manually (see page 103).

Migrate a 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.
2. Log in to the Federation Manager 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. Compare the contents of the smkeydatabase to the certificate data store. Comparing the contents identifies data inconsistencies that can prevent a successful migration.

   Follow the step for your operating platform:
   - (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:\FederationManager\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`* `-p` *`unencrypted_password`*

   - (UNIX) Run the following command:

     `smmigratecds.sh -migrate -log` *`log_file`* `-p` *`unencrypted_password`*

   The command arguments indicate the following action:

   -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.

   Examples:

   -log "C:\Progam Files\Sample\Logs"

   -log export/fedmgr/Sample/Logs"

   -p

   (Optional). Specifies the unencrypted value of the smkeydatabase password. Use this argument to avoid any problems if a system cannot decrypt the password stored in smkeydatabase.properties file.

   unencrypted_password

   Specifies the unencrypted password for the smkeydatabase.

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

Protect Against XML Signature Wrapping Attacks

A malicious user can commit an XML signature wrapping attack by changing the content of a document signature without invalidating the signature.

If a federation transaction fails, examine the smtracedefault.log file and the fwstrace.log file. These log files can contain a signature verification failure. The failure to verify a signature can occur for the following reasons:

- A duplicated ID element exists in the XML document, and duplicate ID attributes are not permitted. the signature references this duplicated ID.
- A signature wrapping vulnerability is logged, such as the signature does not reference the expected parent element.

To protect against signature vulnerabilities:

1. Navigate to the xsw.properties file in one of the following locations:
   - If you see the error message in the smtracedefualt.log file, go to *federation_mgr_home*/siteminder/config/properties
   - If you see the error message in the fwstrace.log, go to *federation_mgr_home/*secure-proxy/tomcat/webapps/affwebservices/web-INF/classes.
2. Add the following settings to the xsw.properties file, and set each one to true.

   DisableXSWCheck=true

   DisableUniqueIDCheck=true
3. Save the file.

Upgrade a JDK on an Existing System

If you upgrade the JDK on an existing Federation Manager system, rerun the Federation Manager installation program and point to the upgraded JDK version.

Appendix A: Key Tool Reference

This section contains the following topics:

Key Tool Overview

Use key tool utility (smkeytool) is only to resolve CDS migration issues. For all other certificate management, use the Federation Manager Administrative UI.

The key tool utility (smkeytool):

- Gives you access to a legacy smkeydatabase during an upgrade/migration to r12.5. Use the access legacy key store flag (-accessLegacyKS) to resolve all data collisions that can result in a failed migration to the certificate data store.
- Is installed to the following location:

  *federation_mgr_home/siteminder/*bin

  federation_mgr_home

  Specifies the Federation Manager installation path.

Follow these steps:

1. Open a command line or shell.
2. Run one of the following commands:
   - (Windows) smkeytool.bat -*option* [-*arguments*]
   - (UNIX) smkeytool.sh -*option* [-*arguments*]

Add a Private Key and Certificate Pair

Use the addPrivKey option to import only a private key/certificate pair into the certificate data store. Consider the following items:

- You can have multiple private key/certificate pairs in the store, but SiteMinder supports only RSA keys in the store.
- Only private key/certificate pairs are stored in encrypted form.
- A Policy Server at a producing authority:
  - Uses a single private key/certificate pair to sign SAML assertions.
  - Uses the certificate to decrypt encrypted SAML assertions received from the consuming authority.

  Typically, the key is the first private key/certificate pair found in the certificate data store.
- Delete the certificate metadata from the certificate file before importing it. Import only the data starting with the --BEGIN CERTIFICATE-- marker and ending with the --END CERTIFICATE-- marker. Be sure to include the markers.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-alias *alias*

Required. Assigns an alias to a private key/certificate pair in the database. The alias must be a unique string and can contain only alphanumeric characters.

-certfile *cert_file*

Specifies the full path to the location of the certificate that is associated with the private key/certificate pair. Required for keys in PKCS1, PKCS5, and PKCS8 format.

-keyfile *private_key_file*

Specifies the full path to the location of the private key file. Required for keys in PKCS1, PKCS5, and PKCS8 format.

-keycertfile *key_cert_file*

Specifies the full path to the location of the PKCS12 file that contains the private key/certificate pair data. Required for keys in PKCS12 format.

-password *password*

(Optional) Specifies the password that was used to encrypt the private key/certificate pair when the pair was created. Supply this password to decrypt the key/certificate pair before it gets written to the certificate data store.

Note: This password is not stored in the certificate data store.

After the key/certificate pair is decrypted and placed in the certificate data store, SiteMinder encrypts the pair again using its own password.

Add a Certificate

Use the addCert option to add a public certificate or trusted CA certificate to the certificate data store.

Consider the following items:

- The certificate can be a certificate that is associated with a private key/certificate pair. However, only the certificate is added to the certificate data store.
- If you trust a certificate as a Certificate Authority, this certificate is always treated as a CA certificate.
- For X.509 certificate formats, SiteMinder supports V1, V2, and V3 versions. For encoding formats, SiteMinder supports DER and PEM formats.
- Restart the Web Agent when you add a Certificate Authority certificate.
- Delete the certificate metadata from the certificate file before importing it. Import only the data starting with the --BEGIN CERTIFICATE-- marker and ending with the --END CERTIFICATE-- marker. Be sure to include the markers.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-alias *alias*

Required. Specifies the alias to the certificate associated with the private key in the certificate data store.

Limit: A unique string that contains only alphanumeric characters.

-infile *cert_file*

Required. Specifies the full path to the location of the newly added certificate.

-trustcacert

Optional. Checks that the user provider certificate being added is a CA certificate. The utility checks that the certificate has a digital signature extension and that the certificate has the same IssuerDN and Subject DN values.

-noprompt

(Optional) The user is not prompted to confirm the addition of the certificate.

Add Revocation Information

Use the addRevocationInfo option to specify the location of a CRL. The certificate data store references the location of the CRL.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-issueralias *issuer_alias*

Required. Specifies the alias of the Certificate Authority who issues the CRL.

Example: -issueralias verisignCA

-type (*ldapcrl* | *filecrl*)

Required. Specifies if the CRL is LDAP–based or file–based.

-location *location*

Required. Specifies the location of the CRL.

- (File-based) The full path to the file.

  Example: -location c:\crls\siteminder_root_ca.crl

- (LDAP directory service) The full path to the LDAP server node.

  Example: -location "http://localhost:880/sn=siteminderroot, dc=crls,dc=com"

Delete Revocation Information

Use the deleteRevocationInfo option to delete a CRL from the certificate data store.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-issueralias *issuer_alias*

(Required) Specifies the name of the Certificate Authority who issues the CRL.

-noprompt

(Optional) The user is not prompted to confirm that the CRL can be deleted.

Remove Certificate Data

Use the removeAllCertificateData option to remove all certificate data from the certificate data store.

The argument for this option is the following:

-noprompt

(Optional) The user is not prompted to confirm that the certificate data can be removed.

Delete a Certificate

Use the delete option to remove a certificate from the certificate data store. If the certificate has an associated private key, the key is also deleted.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-alias *<alias>*

(Required) Specifies the alias of the certificate that the option is to remove.

-noprompt

(Optional) The user is not prompted to confirm that the certificate can be removed.

Export a Certificate or Private Key

Use the export option to export a certificate or private key to a file.

Consider the following items:

- Certificate data is exported using PEM encoding.
- Private key data is exported using DER encoded PKCS8 format.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-alias *alias*

(Required) Identifies the certificate or key to be exported.

-outfile *out_file*

(Required) Specifies the full path to the file to which the data is exported.

-type (key|cert)

(Optional) Specifies whether a certificate or key is being exported.

Default: certificate.

-password *password*

Required only when exporting a private key. Specifies the password that is used to encrypt the private key when exported. You do not need a password to export the certificate holding the public key because certificates are exported in clear text.

To add this private key back to the certificate data store, use the addPrivKey option with this password.

Find an Alias

Use the findAlias option to find the alias that is associated with a certificate in the certificate data store.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-infile *cert_file*

(Required) Specifies the full path to the certificate file associated with the alias you want.

-password *password*

Required only when a password–protected P12 file is specified as the certificate file.

Import Default CA Certificates

Use the importDefaultCACerts option to import all default trusted Certificate Authority certificates that are included with SiteMinder to the certificate data store.

The argument for this option is the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

List Metadata for all Certificates

Use the listCerts option to list some metadata of all certificates stored in the certificate data store.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-alias *alias*

(Optional) Lists the metadata details of the certificate and key that are associated with the alias specified.

This option supports an asterisk (*) as a wildcard character. Use the wildcard at the

- Beginning or end of an alias value.
- Beginning and end of an alias value.

Enclose the wildcard in quotes to prevent a command shell from interpreting the wildcard character.

List Revocation Information

Use the listRevocationInfo option to display a list of certificate revocation lists in the certificate data store. The following items are listed:

- The CRL name.
- Whether the CRL is file–based or LDAP–based.
- The CRL location.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-issueralias *issuer_alias*

(Optional) Name of the Certificate Authority who issues the CRL.

This option supports an asterisk (*) as a wildcard character. Use the wildcard at the:

- Beginning or end of an alias value.
- Beginning and end of an alias value.

Enclose the wildcard in quotes to prevent a command shell from interpreting the wildcard character.

Display Certificate Metadata

Use the printCert option to display some metadata for a specified certificate. This command is useful on systems where viewing certificate properties is difficult.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-infile *cert_file*

Required. Location of the certificate file.

-password *password*

The password is required only when a password-protected P12 file is specified as the certificate file.

Rename an Alias

Use the renameAlias option to rename an alias that is associated with a certificate.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-alias *current_alias*

(Required) Specifies the alias that is associated with a certificate.

-newalias *new_alias*

(Required) Specifies the new alias name.

Limits: Must be a unique string that contains only alphanumeric characters.

Validate a Certificate

Use the validateCert option to determine if a certificate is revoked.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the r12.5 certificate data store.

-alias *alias*

(Required) Specifies the alias to the certificate associated with the private key in the certificate data store

Limits: Must be a unique string that contains only alphanumeric characters.

-infile *crl_file*

(Optional) Specifies the CRL that you want the utility to look in for the certificate to validate it.

Index

O

P

R

S

T

U

V