CA Federation Manager

Release Notes

r12.5

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: Welcome

Welcome to CA Technologies Federation Manager. These release notes contain product installation considerations, operating system support, known issues, and information about contacting CA Technologies Technical Support.

Chapter 2: Operating System Support

For a list of supported operating systems for Federation Manager, refer to the Platform Support Matrix for the product.

To locate the platform matrix:

1. Log into the Technical Support site.
2. Search for the Federation Manager Platform Support Matrix for r12.5.

Chapter 3: New Features in Federation Manager r12.5

This section contains the following topics:

r12.5 Highlights

The following sections highlight some of the major features new in r12.5.

eGov 1.5 Profile for SAML 2.0 Compliance

Partnership federation is enhanced to comply with eGov 1.5 certifications. The new features apply only for SAML 2.0 and include:

- User Consent and customizable user consent form

  Before the Identity Provider sends identity information to a partner, the user must grant permission.

- Local Logout

  Local logout enables a user to be logged out at the local SP-side application. The session at the SP is removed, but no communication with the IdP or other SPs is involved.

- Use of an AllowCreate query parameter

  The product can use a query parameter to override the AllowCreate attribute. The query parameter can be part of a request from the Service Provider to the Identity Provider.

- Authentication Context support at the Identity Provider and Service Provider

  A Service Provider can now request information about how a user authenticates at the Identity Provider. An Identity Provider can respond to the authentication context request. If an Identity Provider initiates single sign-on and the authentication context is defined, the Identity Provider includes the authentication context in an assertion by default.

- SP Session Validity

  The product can now manage the duration of the authentication session at the Service Provider. The SessionNotOnOrAfter attribute is an optional attribute that the IdP can include in the <AuthnStatement> of an assertion.

- Control over Single Sign-on Initiation

  For SAML 2.0 partnerships, you can determine whether the IdP or the SP or both can initiate single sign-on.

For more information on these features, see the *Federation Manager Guide*.

User Attribute Mapping for a Common View of Information

This release lets you configure user attribute mapping. User attribute mapping lets you create a common view of the same information by defining a universal schema.

The universal schema can resolve user information across multiple user directories. The system can reference user attributes without regard for the directory type, reducing the number of configuration objects that are required for multiple user directories.

For more information, see the *Federation Manager Guide*.

Certificate Data Store to Replace Key Databases

In previous releases, a key database (smkeydatabase) stored private key/certificate pairs and standalone certificates. These keys and certificates are used for signing, verification, encryption, and decryption functions. Each federation system in the deployment accessed a local version of the smkeydatabase.

Release r12.5 replaces the multiple, local smkeydatabases with a single certificate data store. By default, the certificate data store is automatically configured and co–located with the data store. All systems that share a common view into the same store have access to all certificates and keys in the environment.

For more information, see the *Federation Manager Guide*.

Multiple Federation Manager Administrators

Multiple administrators can now manage Federation Manager. Multiple administrators enable the delegation of administration tasks. This feature establishes accountability and separation of duties in the Administrative UI.

For more information, see the *Federation Manager Guide*.

Open Format Cookie Enhancements

The following enhancements have been made to the open format cookie:

- Includes a cookie creation timestamp.
- Get and set URIs for AuthnContext and UserConsent.

For more information, see the *Federation Manager Guide,* the *Federation Manager Java SDK Guide, and the Federation Manager .NET SDK Guide.*

Message Consumer Plug-in for Assertion Processing

The message consumer plug-in is a Java program that implements the Message Consumer Extension API. The plug-in lets you implement your own business logic for processing assertions, such as rejecting an assertion and returning a status code. This additional processing works together with the standard processing of an assertion.

For more information, see the *Federation Manager Guide* and the *Java SDK Programming Reference.*

2048-bit Support for Certificates

Federation Manager now supports certificates with a key size of 2048 bits.

Customizable POST Forms

You can customize the auto-POST form sent to the relying party in a SAML response to improve the user experience.

SAML 1.1 Partnership Enhancements

In addition to the highlighted features, the following enhancements are new:

Producer-to-Consumer partnership features:

- Time and IP address restrictions for assertion generation.
- Hash secret for delegated authentication using a query string.
- Set Do Not Cache setting, which tells the consumer not to retain an assertion for future use.
- Back channel user name and password as credentials for basic authentication across the back channel.
- Maximum and idle timeout values to control user sessions.

Consumer-to-Producer partnership features:

- Time and IP address restriction for assertion generation.
- Back channel user name and password as credentials for basic authentication across the back channel.
- Single-use of an assertion.
- Maximum and idle timeout values to control user sessions.
- Redirect mode to the target application includes the open format cookie as an option.
- Remote user provisioning with the open format cookie as an option.

For more information on these features, see the *Federation Manager Guide*.

SAML 2.0 Partnership Enhancements

In addition to the highlighted features, the following enhancements are new:

IdP-to-SP partnership features:

- Time and IP address restrictions for assertion generation.
- Maximum and idle timeout values to control user sessions.
- Hash secret for delegated authentication using a query string.
- Back channel user name and password as credentials for basic authentication across the back channel.
- Setting one time use of assertions.
- Reuse of the same assertion session index to the same partner during a given browser session.
- Status redirect URLs to override the server errors, invalid requests, and unauthorized access errors
- IdP can sign the artifact response messages before returning it to the SP.
- IdP can require the SP to sign the artifact resolve message before returning message to the IdP.

SP-to-IdP partnership configuration features:

- Time and IP address restrictions for assertion generation.
- Maximum and idle timeout values to control user sessions.
- Enforce the one time use of assertions.
- SP can sign the artifact resolve message before returning it to the IdP.
- SP can require the IdP to sign the artifact response message before returning the message.
- Validate target URL domains setting to ensure the replying party access to the requested target domain.
- Redirect mode to the target application includes the open format cookie as an option.
- Remote user provisioning with the open format cookie as an option.
- Status redirect URLs to override the server errors, invalid requests, and unauthorized access errors.

For more information on these features, see the *Federation Manager Guide*.

Chapter 4: Changes to Existing Features

This section contains the following topics:

Key Size Increased for SSL Certificates

You can now select a key size of 2048 bits for SSL certificates used by Federation Manager.

Cookie Skew Time Setting for Delegated Authentication

You can select the open-format cookie as the authentication type for delegated authentication. When you select the open-format cookie, a cookie skew time parameter becomes available. The skew time setting is available only at the partnership-level configuration. The cookie skew time is not available for the global open format cookie settings.

Chapter 5: Known Issues

This section contains the following topics:

Installation, Upgrade, and Performance Issues

The following topics describe issues that you can occur when installing or upgrading Federation Manager. Other issues are related to system performance.

Configure the Session Store Timeout for Heavy Load Conditions

Under heavy load conditions, long-running queries necessary for session store maintenance tasks, such as removing idled–out or expired sessions, can timeout. Adjust the timeout for session store maintenance tasks (60 seconds by default), by increasing the value of the MaintenanceQueryTimeout registry setting. Increase the value so that the maintenance thread can complete its tasks successfully.

The MaintenanceQueryTimeout registry setting can be found at the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\
SessionServer
```

Console Mode Required for UNIX Systems with IPv6 Addresses (159528)

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

Federation Manager Fails after First Request on UNIX Systems (138362)

Symptom:

On UNIX systems, the policy engine fails after an initial installation and configuration of Federation Manager.

Solution:

Always restart the Federation Manager services after running the configuration wizard.

To restart Federation Manager services on a UNIX system

1. Open a command window.
2. 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.

Microsoft SQL Express is Not Supported as a Database

Do not install Microsoft SQL Express as a database for Federation Manager. It is not supported.

Uninstalling SiteMinder Before Installing Federation Manager

Symptom:

If you are installing Federation Manager on a system where SiteMinder or SPS was installed previously and is now removed, you might get an error message when installing Federation Manager.

Solution:

In this case you can follow this procedure:

1. Navigate to one of the following locations for your platform:

   Windows

   C:\Program Files\Zero G Registry

   UNIX

   /var or federation_mgr_home/

2. Back up the .com.zerog.registry.xml file, saving it under a new name.

3. Remove any information related to SiteMinder or SPS in the registry file.
4. Save the changes to the registry file.

Federation Manager UI Issues

The following topics describe issues you may encounter when using the Federation Manager UI.

SSL UI Connection Allows Non-SSL Access to the UI (87262)

Symptom:

If you enable SSL for the connection to the Federation Manager UI, the UI is still accessible over a non-SSL (HTTP) connection, potentially exposing an administrator's credentials.

Solution:

Enable the UI SSL port then disable the UI HTTP port.

To enable SSL for the UI

1. Run the Configuration Wizard, supplying values or accepting the defaults for the Admin UI HTTP Port and the Admin UI SSL Port settings.

   Note: You can skip this step if these ports were already defined when you first installed and configured Federation Manager.
2. Log in to the Federation Manager UI.
3. Select Infrastructure, SSL Configuration.

   The SSL Configuration dialog displays.
4. Click Activate in the Administrative UI SSL Configuration box.

   By clicking this button, SSL is enabled to protect the UI.
5. Exit the UI.

To disable the HTTP UI Port

1. Navigate to *federation_mgr_home*\secure-proxy\proxy-engine\conf.
2. Open the server.conf file.
3. Comment out the setting **local.http.port=***port_number* by adding a pound sign (#) in front of the setting.
4. Save the server.conf file.

5. 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.

Federation Manager UI Permits only ASCII Characters (97031, 97033, 97034, 96471, 96473, 98181)

The Federation Manager Installation Wizard, Configuration Wizard, and User Interface support only ASCII characters for entries. Do not use UTF-8 characters.

Custom Post Form Help Description

For HTTP-POST single sign-on, the description for the Custom Post Form field is incorrect. The correct description is:

Custom Post Form

Names the custom auto-POST HTML form for HTTP-POST single sign-on. Enter only the name of the form, not the path to the form. The product provides a form named defaultpostform.html.

The physical page must reside in the directory *federation_mgr_home*\customization, where *federation_mgr_home* is the installed location of Federation Manager.

Partnership and Entity Issues

The following topics describe issues you may encounter when configuring federation partnerships and entities.

Encryption of an Assertion and the NameID fails with Java 1.7 (160057)

Symptom:

Encryption of an assertion and of the NameID fails with Java 1.7 installed.

Solution:

For Java 1.7, remove the following security provider entry from the java.security file:
`security.provider.1=com.oracle.security.ucrypto.UcryptoProvider ${java.home}/lib/security/ucrypto-solaris.cfg`

HTTP-Artifact Requires Encrypted Assertion with Non-ASCII Characters (98479)

If an assertion contains non-ASCII characters and it is sent using the HTTP-Artifact profile, encrypt the assertion or check that the artifact back channel is an SSL connection. This issue is only relevant for SAML 2.0.

Spaces Not Allowed in Partnership Names (74945)

Do not use embedded spaces in names for federation partnerships.

Chapter 6: Documentation

This section contains the following topics:

Federation Manager Bookshelf

Complete information about SiteMinder is available from the documentation bookshelf. The bookshelf lets you:

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

View the bookshelf from the CA Technical Support site. You do not need to log in to the site to access the bookshelf.

If you plan to download any documentation, we recommend that you download it before beginning the installation process.

Chapter 7: International Support

An *internationalized* product is an English product that runs correctly on local language versions of the required operating system and required third-party products, and supports local language data for input and output. Internationalized products also support the ability to specify local language conventions for date, time, currency and number formats.

A *translated* product (sometimes referred to as a *localized* product) is an internationalized product that includes local language support for the product's user interface, online help and other documentation, as well as local language default settings for date, time, currency, and number formats.

Federation Manager has been internationalized and localized to the extent indicated in the platform support matrix for Federation Manager r12.5.

Chapter 8: Third-Party Software Acknowledgements

Federation Manager incorporates software from third–party companies. For more information about the third–party software acknowledgements, see the Federation Manager Bookshelf main page.

Appendix A: Accessibility Features

CA Technologies is committed to ensuring that all customers, regardless of ability, can successfully use its products and supporting documentation to accomplish vital business tasks. This section outlines the accessibility features that are part of Federation Manager.

Product Enhancements

Federation Manager offers accessibility enhancements in the following areas:

- Display
- Sound
- Keyboard
- Mouse

Note: The following information applies to Windows-based and Macintosh-based applications. Java applications run on many host operating systems, some of which already have assistive technologies available to them. For these existing assistive technologies to provide access to programs written in JPL, they need a bridge between themselves in their native environments and the Java Accessibility support that is available from within the Java virtual machine (or Java VM). This bridge has one end in the Java VM and the other on the native platform, so it will be slightly different for each platform it bridges to. Sun is currently developing both the JPL and the Win32 sides of this bridge.

Display

To increase visibility on your computer display, you can adjust the following options:

Font style, color, and size of items

Lets you choose font color, size, and other visual combinations.

Screen resolution

Lets you change the pixel count to enlarge objects on the screen.

Cursor width and blink rate

Lets you make the cursor easier to find or minimize its blinking.

Icon size

Lets you make icons larger for visibility or smaller for increased screen space.

High contrast schemes

Lets you select color combinations that are easier to see.

Sound

Use sound as a visual alternative or to make computer sounds easier to hear or distinguish by adjusting the following options:

Volume

Lets you turn the computer sound up or down.

Text-to-Speech

Lets you hear command options and text read aloud.

Warnings

Lets you display visual warnings.

Notices

Gives you aural or visual cues when accessibility features are turned on or off.

Schemes

Lets you associate computer sounds with specific system events.

Captions

Lets you display captions for speech and sounds.

Keyboard

You can make the following keyboard adjustments:

Repeat Rate

Lets you set how quickly a character repeats when a key is struck.

Tones

Lets you hear tones when pressing certain keys.

Sticky Keys

Lets those who type with one hand or finger choose alternative keyboard layouts.

Mouse

You can use the following options to make your mouse faster and easier to use:

Click Speed

Lets you choose how fast to click the mouse button to make a selection.

Click Lock

Lets you highlight or drag without holding down the mouse button.

Reverse Action

Lets you reverse the functions controlled by the left and right mouse keys.

Blink Rate

Lets you choose how fast the cursor blinks or if it blinks at all.

Pointer Options

Let you do the following:

- Hide the pointer while typing
- Show the location of the pointer
- Set the speed that the pointer moves on the screen
- Choose the pointer's size and color for increased visibility
- Move the pointer to a default location in a dialog box

Keyboard Shortcuts

The following table lists the keyboard shortcuts that Federation Manager supports:

Keyboard	Description
Ctrl+X	Cut
Ctrl+C	Copy
Ctrl+V	Paste

Keyboard	Description
Ctrl+Right	Next Word
Ctrl+Down	Scroll Line Down
End	Line End