SiteMinder®

Federation Release Notes

r12.5

technologies

This Documentation, which includes embedded help systems and electronically distributed materials (hereinafter referred to as the “Documentation”), is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

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

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

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

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

The manufacturer of this Documentation is CA.

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

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

This document contains information about Federation Manager—legacy and partnership federation. These notes describe features, operating system support, known issues and fixes.

Chapter 2: New Features

This section contains the following topics:

Legacy and Partnership Federation in the Administrative UI

SiteMinder now lets you configure Federation Manager from a central management interface. Under the Federation Manager product, there are two federation models: *legacy federation* (formerly Federation Security Services) and partnership federation (formerly standalone Federation Manager). You can

If you are an existing customer of Federation Security Services, you can manage these objects from the Legacy Federation tab in the Administrative UI. Aspects of legacy federation in the Administrative UI differ from previous 12.x SiteMinder releases. However, most of the field names and location of settings are similar to previous 12.x SiteMinder release. To configure SAML 1.0 or WS-Federation profiles for single sign-on, you must use legacy federation.

If you are new to federation and you want to use SAML 1.1 or SAML 2.0 for single sign-on, use partnership federation. If you are an existing customer and simply want to take advantage of the partnership model, use partnership federation.

Note: You cannot upgrade from standalone Federation Manager to partnership federation integrated with SiteMinder.

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.

Chapter 3: Changes to Existing Features

This section contains the following topics:

Federation Security Services UI

In previous r12.x releases, you manage a federated environment using the Federation Security Services UI (FSS Administrative UI). This UI is the applet–based UI installed with the Policy Server and is the only way to configure and manage legacy federation.

The *Federation Security Services Guide* explains how to manage a federated environment using the FSS Administrative UI.

The r12.5 release:

- Ports all legacy federation functionality (formerly Federation Security Services) to the SiteMinder Administrative UI. You manage all legacy federation functionality using the Administrative UI.
- Includes the FSS Administrative UI to facilitate the transition of managing legacy federation using the Administrative UI. Consider the following items:
  - After you upgrade the policy store to r12.5, run the XPS Sweeper utility to manage legacy federation objects originally configured in the FSS Administrative UI. For more information, see the *SiteMinder Upgrade Guide*.
  - This release, including all cumulative releases and service packs, is the last major release that includes the FSS Administrative UI.
  - Support is available for the FSS Administrative UI, but fixes are at the discretion of CA.
- The *Federation Manager Guide: Legacy Federation* explains how to manage a federated environment using the Administrative UI. All references to the FSS Administrative UI are removed from the r12.5 SiteMinder bookshelf. If you want to use the FSS Administrative UI, see the r12.0 SP3 SiteMinder bookshelf.

Important! Do not refer to the r12.0 SP3 documentation for future legacy federation features released in the Administrative UI.

Internal Federated Partnerships Displayed in the FSS UI (152182)

If you create federated partnerships in the Administrative UI, these partnerships can be viewed in the Federation Security Services UI. The FSS Administrative UI managed federation objects in previous r12.x releases.

If you view Administrative UI partnerships in the FSS Administrative UI, special partnership domains are displayed. The following prefixes identify these partnership domains:

- samlidp:
- samlsp:
- samlprd:
- affiliate:

For example, an IdP-to-SP partnership displays the domain samlidp:*partnership_name.*

Do not modify these domains or any child objects using theFSS Administrative UI. These objects are realms and rules that the partnership uses internally.

Note: This behavior only applies to partnership federation.

SiteMinder Key Database

In previous releases, a SiteMinder smkeydatabase stored private key/certificate pairs and standalone certificates. SiteMinder used these keys and certificates for signing, verification, encryption and decryption functions. Each Policy Server in the deployment accessed a local version of the smkeydatabase.

This release replaces the need for multiple, local smkeydatabases with a single certificate data store. By default, the certificate data store is automatically configured and co–located with the policy store. All Policy Servers that share a common view into the same policy store have access to all certificates and keys in the environment.

Note: For more information about managing the certificate data store, see the *Policy Server Configuration Guide* and the *Policy Server Administration Guide*. For more information about migrating a smkeydatabase to the certificate data store, see the *SiteMinder Upgrade Guide*.

LDAP Search Specification Handles Multiple %s Strings (148367)

Symptom:

Specifying an LDAP search filter in a SAML 2.0 authentication scheme at the Service Provider had a limitation. The Policy Server could not process an LDAP filter string with multiple %s characters.The Policy Server was not replacing all %s variable with the login ID.

This problem occurred for legacy federation.

Solution:

You can now specify an LDAP search filter containing multiple %s variables. The following are example strings now supported:

```
|(uid=%s)(uid=%s)
|(abcAliasName=%s)(cn=%s)
```

If user1 is the LoginID, the Policy Server resolves these strings as follows

```
|(uid=user1) (uid=user1)
|(abcAliasName-user1) (cn-user1)
```

Specify LDAP searches in the User Lookup field of the SAML 2.0 authentication scheme in the Administrative UI. The dialog can be found at the location Infrastructure, Authentication Schemes, General.

FWS Deployment Procedures are in the Web Agent Option Pack Guide

SiteMinder Federation Manager requires the Web Agent Option Pack to work. After you install the Web Agent Option Pack, you deploy the Federation Web Services (FWS) application included with the option pack. The instructions for deploying the FWS application are now in the *Web Agent Option Pack Guide*.

Query String Redirection for Delegated Authentication is Only for Testing (165475)

Symptom:

Query string redirection method for delegated authentication was not documented as an option only for test environments.

Solution:

The *Partnership Federation Guide* now says that if you configure the delegated authentication feature for single sign-on, do not use the query string method in a production environment. The query string redirection method is only for a testing environment as a proof of concept.

STAR issue: 21183744;1

Chapter 4: Operating System Support

Before you install Federation Manager components, ensure you are using a supported operating system and third-party software.

For a list of supported operating systems, Web Servers, databases, Web browsers, LDAP directory servers, and servlet:

1. Log into the Technical Support site.
2. Search for the SiteMinder platform matrix for r12.x, which includes r12.5.

Chapter 5: Defects Fixed in 12.5

This section contains the following topics:

Web Agent Option Pack creates an invalid assertion (111451/160502)

Symptom:

Web Agent Option Pack creates an assertion with an expired smsession cookie.

Solution:

STAR Issue: 21843717-01

Incorrect Agent Configuration Object Note in Web Agent Option Pack Guide (171005)

Symptom:

The Web Agent Option Pack Guide contained the following incorrect note:

"Note: The Agent Configuration Object referenced in this WebAgent.conf file must be a new object that you create. Do not specify the object in use by the Web Agent installed in your environment."

Solution:

This note has been removed from the guide.

STAR issue: 21419266-1

Query String Redirection for Delegated Authentication is Only for Testing (165475)

Symptom:

Query string redirection method for delegated authentication was not documented as an option only for test environments.

Solution:

The *Partnership Federation Guide* now says that if you configure the delegated authentication feature for single sign-on, do not use the query string method in a production environment. The query string redirection method is only for a testing environment as a proof of concept.

STAR issue: 21183744;1

Tomcat 6 Reference Removed from Documentation (159125)

Symptom:

The Web Agent Option Pack Guide referenced Tomcat 6 in error.

Solution:

The section that is titled "Modify the Tomcat catalina.properties File (Tomcat 6.0.18 or higher)" has been removed from the Web Agent Option Pack Guide. Tomcat 6 is no longer supported as an application server.

STAR issue: 21093204-01

Prerequisite for ODBC User Directory Setup for Federation (157633)

Symptom:

The federation documentation must clarify that an ODBC user directory for a SAML-related configuration requires a properly defined SQL query scheme.

Solution:

The following note has been added to the User Directory chapter in the *Legacy Federation Guide* and the *Partnership Federation Guide*.

Note: To use an ODBC database for your federated configuration, set up the SQL query scheme and valid SQL queries before selecting an ODBC database as a user directory.

STAR issue: 21043182

Information Missing for the smfedexport Command Options (155515)

Symptom:

No detailed information exists about the usage of the smfedexport command options, such as –pubkey,-sign and –signingcertalias.

Solution:

The *Legacy Federation Guide* has clearer explanations of the smfedexport command options.

STAR issue: 20969179-01

Protection Against XML Signature Wrapping Attacks (168098)

A malicious user can commit an XML signature wrapping attack by changing the content of a document without invalidating the signature. By default, software controls for the Policy Server and Web Agent Option Pack are set to defend against signature wrapping attacks. However, a third-party product can issue an XML document in a way that does not conform to XML specifications. As a result, the default signature checks can result in a signature verification failure.

Signature verification failures occur for the following reasons:

- A duplicate ID element is in the XML document and the signature references this duplicate ID. Duplicate ID attributes are not permitted.
- The XML signature does not reference the expected parent element, and a signature wrapping vulnerability is logged.

If a federation transaction fails, examine the smtracedefault.log file and the fwstrace.log file for a signature verification failure. These errors can indicate that the received XML document is not conforming to XML standards. As a workaround, you can disable the default Policy Server and Web Agent protection against signature wrapping attacks.

Important! If you disable the protection against signature vulnerabilities, determine another way to protect against these attacks.

To disable the XML signature wrapping checks:

1. Navigate to the xsw.properties file. The file exists in different locations for the Policy Server and the Web Agent.
   - For error messages in the Policy Server smtracedefault.log file, go to *siteminder_home*/config/properties
   - For error messages in the Web Agent fwstrace.log, go to

     *web_agent_option_pack_ home/*affwebservices/web-INF/classes.

     Note: If the web agent option pack is installed on the same system as the web agent, the file resides in the *web_agent_home* directory.
2. Change the following xsw.properties settings to true:
   - DisableXSWCheck=true (Policy Server setting only)
   - DisableUniqueIDCheck=true (Policy Server and Web Agent Option Pack setting)

     Note: The value of the DisableUniqueIDCheck setting must be the same for the Policy Server and the Web Agent Option Pack.
3. Save the file.

STAR issue: 21321479;1

Chapter 6: Known Issues for Legacy and Partnership Federation

Federation Does Not Support the Cookie Provider (172511)

SiteMinder Federation proudcts, which use the Web Agent Option Pack, do not support the use of the Cookie Provider for federated configurations.

Back Channel Processing Fails with Client Certificate Protection (168151, 168278, 169147, 168774, 169312)

Symptom:

Back channel processing fails when you use the client certificate option to protect the back channel. The failure impacts all profiles that use the back channel, including HTTP-Artifact single sign-on and SAML 2.0 Single Logout over SOAP.

Failures occur under the following conditions:

- A deployment with IIS web servers and any application server. The failure is the result of an IIS limitation. This problem applies to legacy and partnership federation.
- A certificate that is generated with the OpenSSL toolkit and the UTF-8 flag is set.
- Apache web servers running JBoss at the IdP, unless you make a configuration change to the httpd.ssl.conf file.

Solution:

The following solutions are available:

- Protect the back channel using the Basic option and ensure that all URLs are using the SSL protocol.
- Do not set the UTF-8 flag when generating a certificate with the OpenSSL toolkit.
- For Apache web servers running JBoss at the IdP, uncomment the following line in the Apache httpd.ssl.conf file:

  ```
  SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
  ```

  Note: The Apache solution applies only to partnership federation.

OCSPUpdater Does Not Support the SHA-224 Algorithm (150477,150474)

The OCSPUpdater used for federation certificate validity checking cannot sign OCSP requests using the SHA-224 algorithm. The updater can only sign with the SHA-256, SHA-384, and SHA-512 algorithms.

Java Virtual Machine Installation Error on Solaris can be Ignored (149886)

Symptom:

You are doing a console mode installation of a SiteMinder product on a Solaris platform. The following error message displays: "Unable to install the Java Virtual Machine included with this installer."

Solution:

Ignore this error message. The error is a third-party issue and it has no functional impact.

Web Agent Option Pack on JBOSS Requires Workaround (147357, 149394)

Symptom:

On the JBoss 5.1.2 server, system JARs are overriding application-specific JARs, such as those JARs for the Web Agent Option Pack.

Solution:

Prevent the Web Agent Option Pack XML API files from being overwritten by JBOSS system JARS.

Important! This workaround only applies to the supported version of JBOSS 5.1.2.

Add the following filter package in two places in the **war-deployers-jboss-beans.xml** file:

```
<property name="filteredPackages">javax.servlet,org.apache.commons.
logging,javax.xml.parsers,org.xml.sax,org.w3c.dom</property>
```

The filter package allows the use of the Web Agent Option Pack XML API files instead of the JBOSS system files.

Follow these steps:

1. Locate the war-deployers-jboss-beans.xml file located in the directory:

   /deployers/jbossweb.deployer/META-INF/

2. Find the following entry:

   ```
   <property name="filteredPackages">javax.servlet,org.apache.
   commons.logging</property>
   ```

3. Change the entry to:

   ```
   <property name="filteredPackages">javax.servlet,org.apache.commons.
   logging,javax.xml.parsers,org.xml.sax,org.w3c.dom</property>
   ```

   This entry in the file is on one line.

4. Find the second instance of the entry in step 2 and replace it with the entry in step 3.

   Add the filter package in both places in the XML file.

5. Save the XML file.

Deploying Federation Web Services in JBOSS 5.1.x (150603)

Symptom:

A federation transaction is failing at the asserting party when the federation web services application is deployed on a JBOSS server, version 5.1.0 and higher. An error message indicates one of the following conditions:

- SiteMinder could not decrypt the SMSESSION cookie.
- An encryption exception occurred during session cookie creation.

Solution:

Deploy affwebservices.war file in an exploded folder under the jboss deploy directory.

Follow these steps:

1. Open a command window and navigate to the affwebservices directory, which is in the directory /webagent_option_pack/affwebservices/.
2. Create a WAR file by entering the command:

   ```
   jar cvf affwebservices.war *
   ```

3. Navigate to the directory *JBOSS_home*/server/default/deploy/

   JBOSS_home is the installed location of the JBOSS application server.

4. Under the deploy directory, create a directory named affwebservices.war.
5. Inside the affwebservices.war directory, extract the affwebservices.war file.

   Note: Be sure that the affwebservices.war file is not in the deploy directory.

6. Restart the application server.
7. After the server has restarted, access the JBOSS Administrative Console. The affwebservices.war file is displayed in the JBOSS console under Applications>WARs.
8. Test that the FWS application is working by opening a web browser and entering the following link:

   ```
   http://fqhn:port_number/affwebservices/assertionretriever
   ```

   fqhn

   Represents the fully qualified host name and

   port_number

   Specifies the port number of the server where the Federation Web Services application is installed.

9. Execute a federated single sign-on transaction. A successful transaction confirms that SiteMinder federation is working properly.

SiteMinder Federation does not Support Directory Mapping (147993)

SiteMinder legacy and partnership federation do not support directory mapping. The user is tied to the directory they are initially authenticated against. If that directory is not present in the affiliate domain, the authorization fails.

SPS Federation Gateway in a Federation Deployment

You can install the r12.3 SiteMinder SPS Federation Gateway only in a legacy federation deployment. This release of the gateway is compatible with SiteMinder 12.5.

You cannot use the r12.3 gateway in a 12.5 partnership federation deployment.

Chapter 7: Known Issues for Legacy Federation

Attributes Appear Truncated at the Relying Party (157913)

Symptom:

The following issues occur:

- The directory attributes appear truncated at the relying party.
- The following message appears in the smtracedefault.log file:

  ```
  [WARNING: Response attribute will be trimmed. [attr = SMUSERGRP:memberOf] [actual
  attr len = number] [ response attr len = number]]
  ```

  Note: In the Warning message, SMUSERGRP represents the variable name and memberOf represents the attribute value. The error message is specific to your configuration.

Solution:

The maximum length for the user assertion attributes is configurable by modifying settings in the EntitlementGenerator.properties file. To modify the length, go to the *CA SiteMinder Federation: Legacy Federation Guide* and follow the procedure in the section "Specify the Maximum Length of Assertion Attributes."

Unable to View Legacy Federation Objects in the UI (119335)

Symptom:

After configuring legacy federation objects using the Policy Server Management API or the FSS Administrative UI and then upgrading to the SiteMinder r12.5 Administrative UI, the legacy federation objects are not visible in the Administrative UI. When you try selecting a legacy federation object in the Administrative UI you see the message,

```
Error: [General]  The value for "Enabled" failed to convert to correct
type.
```

Solution:

Run the XPS sweeper utility to help ensure the legacy federation objects build correctly. For information about the XPS sweeper utility, see the *SiteMinder Upgrade Guide*.

Chapter 8: Known Issues for Partnership Federation

Chapter 9: Documentation

This section contains the following topics:

SiteMinder Bookshelf

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

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

View and download the SiteMinder 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 the documentation, we recommend that you download it before beginning the installation process.

Release Numbers on Documentation

The release number on the title page of a document does not always correspond to the current product release number; however, all documentation delivered with the product, regardless of release number on the title page, supports the current product release.

The release number changes only when a significant portion of a document changes to support a new or updated product release. If no substantive changes are made to a document, the release number does not change. For example, a document for r12 can still be valid for r12 SP1. Documentation bookshelves always reflect the current product release number.

Occasionally, we must update documentation outside of a new or updated release. To indicate a minor change to the documentation that does not invalidate it for any releases that it supports, we update the edition number on the cover page. First editions do not have an edition number.

Appendix A: Third–Party Software Acknowledgments

SiteMinder incorporates software from third–party companies. For more information about the third–party software acknowledgments, see the SiteMinder Bookshelf main page.