CA SiteMinder®

Federation Release Notes

12.51

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: Federation Release Notes

These topics contain information about CA SiteMinder 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:

Claims Transformation of Assertion Attributes

Claims transformation manipulates claims during a federated single sign-on transaction. Claims, also known as attributes, help customize the attributes and improve the user experience at a partner.

The software can perform three different modifications to assertion attributes:

- **Transformation:** Changing the value of an assertion attribute to a different value.
- **Addition:** Adding an assertion attribute if it does not exist already.
- **Deletion:** Deleting an assertion attribute on a conditional basis.

Session Store Attributes Available for Assertions

Session attributes can be persisted in the session store after a user is authenticated. From the session store, the system can add the attributes to an assertion to customize the requested application.

WS-Federation 1.2 Support

CA SiteMinder now supports the WS-Federation 1.2 profile for partnership federation. You can configure single sign-on and sign-out using the WS-Federation profile.

WS-Federation Metadata Exchange

The Policy Server supports the Web Services Metadata Exchange profile for WS-Federation partnerships. This web service enables the CA SiteMinder local partner to respond to requests from a remote partner for metadata. The exchange occurs as an HTTP request and response.

SAML 2.0 Attribute Query Support

A CA SiteMinder IdP supports the SAML 2.0 Assertion Query/Request profile and can respond to attribute queries. The IdP also extends the profile functionality by accepting queries for attributes not in the assertion or in the metadata. When the IdP receives an attribute query, the IdP first checks its user directory to find the attributes. If the attributes are not found, the Policy Server checks the session store.

Note: Only the CA SiteMinder IdP supports the query profile. A CA SiteMinder SP as the requesting partner only supports the proxied attribute query feature.

SAML 2.0 User Attribute Retrieval from a Third-Party Identity Provider

In a SAML 2.0 federated environment, CA SiteMinder supports a feature referred to as a proxied attribute query. The proxied attribute query is based on the SAML 2.0 Assertion Query/Request profile.

A proxied query enables the Policy Server to contact a third-party Identity Provider and request values for attributes that are not in its session store. The Policy Server can then pass the attributes back to the application at the Service Provider.

SAML 2.0 Attribute Authority Metadata

When you export metadata from a local SAML 2.0 IdP entity or an IdP-to-SP partnership, the attribute service URL is in the exported metadata. This information is relevant for local IdPs acting as an Attribute Authority, one of the roles necessary for the Attribute Query/Response profile.

Chapter 3: Changes to Existing Features

This section contains the following topics:

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: Known Issues for Legacy and Partnership Federation

Data Table Entries are Not Saved when You Navigate Backward in the Partnership Wizard (178861)

If you go backward from any step in the partnership wizard to a previous step, the entries in a data table are not saved. A data table is any table in the Administrative UI where you click "Add Row" and then specify values in the new row.

For example, you can add a row and entries in the SLO Service URLs table of step 4. If you select the Back button or select step 3 in the wizard, the entries in the table are not maintained.

You can only go forward in the partnership wizard for the values in a data table to be preserved.

Federation Does Not Support the Cookie Provider (172511)

CA 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.

Signature Wrapping Checks Impact Artifact SSO After Upgrade (168864)

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

The following conditions result in failed transactions:

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

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

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

Follow these steps:

1. Navigate to the xsw.properties file. Locate the file in the following directory:

   siteminder_install_dir\config\properties\xsw.properties

   siteminder_install_dir is the location where you installed the Policy Server.

2. Open the file in a text editor, and set the DisableXSWCheck to true (DisableXSWCheck=true). Setting the value to true disables the vulnerability check.

3. After the entire deployment is at version 12.51, and the Policy Server is running, return the DisableXSWCheck setting to false (DisableXSWCheck=false). Setting the value to false enables the signature vulnerability check.

For complete upgrade instructions for all CA SiteMinder components, see the CA SiteMinder *Upgrade Guide*.

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 CA 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:

- CA 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 CA SiteMinder federation is working properly.

CA SiteMinder Federation does not Support Directory Mapping (147993)

CA 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 CA SiteMinder SPS Federation Gateway only in a legacy federation deployment. This release of the gateway is compatible with CA SiteMinder 12.5.

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

Chapter 5: 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 CA SiteMinder 12.51 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 *CA SiteMinder Upgrade Guide*.

Filtered Packages for JBoss Container Require Changes (168893)

Symptom:

The JBOSS container version 5.1 requires changes to the filtered packages specifications.

Solution:

1. Install the JBoss container.
2. Navigate to the following folder:
   JBoss_home/server/default/deployers/jbossweb.deployer/META-INF.
3. Open the war-deployers-jboss-beans.xml file.
4. Change the filteredPackages property:

   From:

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

   To:

   <property name="filteredPackages">javax.xml.namespace,org.apache.xml.resolver.helpers,javax.servlet,org.apache.commons.logging,javax.xml.parsers,org.xml.sax,org.w3c.dom</property>
5. Repeat the preceding step for the other entry of filteredPackages in the same file. Overall, there are two entries.
6. Save the file.

Continue with other configuration steps of affwebservices deployment.

Chapter 6: Known Issues for Partnership Federation

Metadata File Name is Incorrect During Metadata Export (172063)

Symptom:

For a Administrative UI using Internet Explorer 9, exporting metadata for a federation entity results in an incorrect file name that you cannot open or download.

When you export metadata at the entity level, a window opens and displays the information to be exported. After you review the information and click Export, a dialog at the bottom of the screen opens, asking to open or save the file. For example:

```
Do you want to open or save LocalIdPMetadata.xml from exampleserver01?
```

Instead of using a proper metadata filename, it uses the name FileDownload. You cannot download the file with this name.

Solution:

For Internet Explorer 9, verify that the browser setting “Do not save encrypted pages to disk” is unchecked before exporting entity metadata. To download the metadata file successfully, this option must be disabled. The setting is in Tools, Internet Options, Advanced tab, under the Security section.

Consistent Use of CONSUMERID or NAME in an Intersite Transfer URL Required (169724)

Symptom:

At the SAML 1.1 producer, links that represent URLs to the intersite transfer service initiate single sign-on. The CONSUMERID or the NAME query parameter is required in the URL.

If you change the query parameter in a URL from one request to another, an error can occur.

Solution:

Select the CONSUMERID or the NAME query parameter for all intersite transfer URLs. Do not interchange these parameters from request to request.

This limitation applies only to SAML 1.1 Producer-to-Consumer partnerships.

WSFED RP Entity with SAML 2.0 Token Type Not Supported (167916)

The Administrative UI lets you configure a CA SiteMinder local WSFED RP entity with a SAML 2.0 token type. However, when you create a WSFED RP-to-IP partnership, you cannot select this RP entity then proceed with the partnership configuration.

The WSFED RP-to-IP partnership does not support the RP entity with the SAML 2.0 token type.

Chapter 7: Federation Defects Fixed in 12.51

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

Single Log Out after a ForceAuthN request results in Session Errors (153740)

Symptom:

The Policy Server log reports session errors when the following conditions are met:

1. A user logs in to Service Provider 1.
2. A user logs in to Service Provider 2. The Service Provider send an authentication request with a ForceAuthN query parameter to the Identity Provider.
3. A user logs out from either Service Provider.

Solution:

The issue is fixed. Session errors are no longer reported.

STAR issue: 20122645–1

System Error after a CA SiteMinder Upgrade (154892)

Symptom:

The customer is required to track all SLOs in the audit log. The customer setup an unprotected realm with an anonymous authentication scheme on /affwebservices/public/saml2slo. Before the upgrade to CA SiteMinder R12 SP3 CR2, this setup worked.

Solution:

The problem has been corrected. The customer gets a successful logout page.

Star Issue: 20160464;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

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

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

Defects Fixed in 12.51 CR 06

The following defects were fixed in 12.51 CR 06.

Provisioning Page Fails to Receive the Headers (64678)

Symptom:

Provisioning page fails to receive the Headers when you enable Open Format Cookie (OFC) in Federation.

Solution:

This issue is fixed.

STAR Issue: 21750471-01

SiteMinder WAOP Fails to Decrypt (134371)

Symptom:

SiteMinder WAOP fails to decrypt the SMFED_TEMPORARY_STATE cookie when you enable Agent Key Rollover feature.

Solution:

This issue is fixed.

STAR Issue: 21918653-01

Chapter 8: Documentation

This section contains the following topics:

CA SiteMinder Bookshelf

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

- Use a single console to view all documents published for CA 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 CA 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

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