CA SiteMinder®

Federation Release Notes

12.52 SP1

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.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Metadata File Name is Incorrect During Metadata Export—For partnership federation, there is a known issue regarding an incorrect metadata file name that the software generates during an export. Resolves CQ177331.

Contents

Chapter 1: New Features

New Features for r12.52 SP1

There are no new features in this release.

Chapter 2: Changed Features

Upgrade of CAPKI

CA SiteMinder® is upgraded to use CAPKI 4.3.4 to fix the following OpenSSL vulnerabilities:

- CVE-2014-0224: An SSL/TLS MITM vulnerability exists in OpenSSL 0.9.8y and earlier. An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server.
- CVE-2014-0221: DTLS recursion flaw exists in OpenSSL 0.9.8y and earlier. By sending an invalid DTLS handshake to an OpenSSL DTLS client, the code can be made to recurse, eventually crashing in a DoS attack.
- CVE-2014-3470: Anonymous ECDH denial of service flaw exists in OpenSSL 0.9.8y and earlier. OpenSSL TLS clients enabling anonymous ECDH ciphersuites are subject to a denial of service attack.
- CVE-2014-0076: Fix for the attack described in the paper "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack".

For more information about the vulnerabilities, see the OpenSSL documentation.

Chapter 3: 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

Chapter 4: Federation Defects Fixed in 12.52

Asserting Party Not Accepting ACS URL in an Authentication Request (170971)

Symptom:

CA SiteMinder® Federation was not accepting and processing the Assertion Consumer Service URL in the incoming authentication request. The system did not verify whether the authentication request had an Assertion Consumer Service URL defined.

Solution:

For an IdP-to-SP partnership, the Administrative UI has a new check box labeled **Accept ACS URL in the Authnrequest**. This check box is in the SSO section of the SSO and SLO step of the partnership configuration. To confirm that the URL is present and valid in the authentication request, and it is in the metadata, select this option.

STAR issue: 21361990

decryptionkeyalias Option Missing for the smfedexport Tool (178702)

Symptom:

The -decryptionkeyalias command option was missing from the list of smfedexport command options.

Solution:

The -decryptionkeyalias command option is now in the table of command options.

STAR issue: 21594883-01

PS Exception When Retrieving Password (175936)

Symptom:

Policy server (FIPS only) threw the following exception while searching for IDP information for an SP-initiated request:

Exception while attempting to retrieve passwords:

java.lang.SecurityException: class "com.netegrity.util.ct"'s signer information does not match signer information of other classes in the same package.

Solution:

This issue has been corrected.

Star issue 21530627-01.

GetUserProp() Function Created a Policy Server Failure (174951)

Symptom:

WS-FED Assertion Generation GetUserProp() function was causing a Policy Server failure.

Solution:

This issue is no longer a problem..

Star issue 21505894.

SAML Response Error (172963)

Symptom:

The user encountered the error "ACS_BAD_SAMLRESPONSE_XML" while running federation partnership in Siteminder FSS 12.51.

Solution:

CA SiteMinder® Federation is no longer shipping dom.jar and sax.jar file, which were causing the problem.

Star issue 21478695-1

Updates to the Web Agent Option Pack Guide (171546)

The following updates were made to the *Web Agent Option Pack Guide:*

- Create a WebAgent.conf File—Removed the note, which stated that the agent configuration object referenced in the WebAgent.conf file must be a new object.
- Properties File for Federation Web Services—Revised the description of the AgentConfigLocation setting. This topic applies to the WebLogic, WebSphere, JBOSS, and Tomcat servers.
- Agent Configuration Object Settings Used by FWS—Added this section to describe agent settings that the Federation Web Services application uses.

STAR issue: 21429459

Wrong Recipient Selected for an Assertion (171113)

Symptom:

In an indexed list of Assertion Consumer Service URLs, CA SiteMinder® Federation generated the assertion with the first entry in the list as the Recipient. The Recipient is required to match the index number.

Solution:

This issue is no longer a problem.

Star issues 21423322;1+21287493;1

SAML SSO Failure (169294)

Symptom:

SAML SSO was failing with "Could not parse SAML
response. Error message: null" as well as "ACS_BAD_SAMLRESPONSE_XML".

Solution:

This issue is no longer a problem.

Star issue 21313265;1.

Chapter 5: Federation Defects Fixed in 12.52 SP1

SSO between CA SiteMinder® Federation and Microsoft Exchange Online (Office365)

Symptom:

Users could not use Microsoft Outlook to log in to an email account hosted by Exchange Online, which is part of Office 365. The algorithm for signing assertions prevented successful authentication.

Solution:

Microsoft has fixed the issue and it is no longer a problem.

Incorrectly Formatted Date-Time Stamp in Response Message (177523)

Symptom:

Same issue as CloudMinder (CQ 169860)

Testing SSO between CloudMinder and an application that was developed using Windows Identity Foundation (WIF) for federation.

The CloudMinder operations team has set up a WS-Federation partnership with the application, where CloudMinder is the IDP

When the users go to the application, they are redirected to CloudMinder. He can authenticate successfully to CloudMinder and CloudMinder then redirects the user back to the application with the WS-Fed response message.

The application is failing to validate the response message. It is throwing an error about an incorrectly formatted date-time.

Solution:

This defect has been fixed indirectly by addressing the problem through CloudMinder.

Star issue

WS-FED Invalid SAML Assertion

Symptom:

There is an issue in federation between SiteMinder and Microsoft ACS. ACS is strict about the sequence of the XML response. They matched the schema defined here: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf#page=17 which indicates that the Signature element should appear directly after the Issuer.

In the SAML response captured from SiteMinder, the Signature is coming at the end after the AttributeStatement.

Solution:

This problem has been corrected.

Star issue 21710666-01

Unable to Import Metadata of WS-Federation (55695)

Symptom:

The Metadata of an SP object is imported as that of an IDP object.

Solution:

This issue is resolved.

STAR issue: 21696321-01

No Provision to Configure the NameQualifier Attribute in Federation (55413)

Symptom:

Administrative UI does not provide an option to configure the NameQualifier attribute for partnerships.

Solution:

This issue is fixed. You can use the Java VM configuration directive -DREMOVE_EMPTY_SAML_NAMEQUALIFIER_ATTRIBUTE=TRUE and set it to true if it wants to remove the NameQualifier attribute name when the value is empty or null. However, the default will be false, ie. if this directive was never set or if the directive is set to false. If the directive is false, then the NameQualifier attribute name will be present in the NameIdentifier tag whether there is a value associated with the NameQualifier attribute.

STAR issue: 21562902-1

Open Format Cookie Issue (166765)

Symptom:

The customer receives large data from his federation partner to send to Target URL and to Provisioning URL. The customer was concerned that the data can get lost when stored in the cookie, because of the data length limitation. The customer requested that the data be sent in the form of POST to the Target Application and the Provisioning Application instead of using the cookie.

Solution:

This change has been made.

Star issue 21268919;1

smfedexport Command Failed to Export Metadata (178747)

Symptom:

While exporting an entity and specifying –pubkey or –sing option caused the fedexport utility to fail.

Solution:

This problem has been corrected.

Star issue 21594883

Import into Federation Failed for the SP Entity (178144)

Symptom:

Import into CA SiteMinder® Federation failed for the SP entity from a multi-entity XML metadata file. The metadata has both an IdP and an SP with the same entity name. The confirmation screen showed the SP to be imported and created. After completing the import, the IdP was imported, not the SP.

Solution:

This problem has been corrected.

Star issue 21588277-1

Failed Access to affwebservices While Creating Partnership (175380)

Symptom:

A user specified as needing access to affwebservices during partnership creation was denied access. The user directory was Active Directory and the user class was Group.

Solution:

This problem has been corrected.

Star issue 21422866

Decrypted Assertion Now Available in the postAuthenticateUser() Method (175005)

Symptom:

The decrypted assertion was available in postDisambiguateUser() method to the MCP, and not available in postAuthenticateUser() method to the MCP. Customer had a requirement to have the decrypted assertion available in the postAuthenticateUser() method to the MCP.

Solution:

This problem has been corrected.

Star issue 21407539

java.lang.ClassCastException in SAML1.1 at SP Side in FSS (177920)

Symptom:

The customer was acting as the Service Provider and using persist attributes as redirect mode.
While invoking the session server, the following exception appeared in the smtrace logs:

```
[09/24/2013][12:58:27][9884][8812][SamlValidator.java][smAuthenticate][][][][][][
][][][][][][][][Beginning to invoke session server interface][][][12:58:27.666]
[09/24/2013][12:58:27][9884][8812][SamlValidator.java][smAuthenticate][][][][][][
][][][][][][][][Processing attribute data. Name: urn:mace:dir:attribute-def:mail
Value: Janet.Peri@uth.tmc.edu][][][12:58:27.666]
[09/24/2013][12:58:27][9884][8812][SamlValidator.java][smAuthenticate][][][][][][
][][][][][][][][SamlValidator (SAML POST/Pass 2)Caught unknown exception or error:
java.lang.ClassCastException: [Ljava.lang.String; cannot be cast to java.lang.String
- Stacktrace: java.lang.ClassCastException: [Ljava.lang.String; cannot be cast to
java.lang.String
```

Solution:

This problem has been corrected.

Star issue 21545080-1

Null Pointer Exception During CDS Cache Updates (177205)

Symptom:

Customer reported that they saw a null pointer exception for the certs for every certificate cache update interval.

Solution:

This problem has been corrected.

Star issue 21566550;1

Reworded Error Message (176455)

Symptom:

A customer request thatthis error message be reworded:

“Release is not the WA-OP - not doing anything”

Solution:

After the correction:

“Cannot initialize; Likely caused by uninitialized NETE_WA_ROOT environment variable"

Star issue 21538180

Chapter 6: 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.

Known Issues

The known issues of the following CA SiteMinder® components are confidential and are no longer included in Release Notes:

- Policy Server
- Web Agent
- SDK
- Federation
- Web Services Security
- CA SiteMinder® SPS

To view the known issues, perform the following steps:

1. Click Release Notes in the bookshelf main page.
2. Click Confidential Content against Known Issues and log in to CA Support Online.

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.