# CA SiteMinder®

## Federation Release Notes

12.52

# 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 (see page 25)—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: Federation Release Notes

This document contains information about CA SiteMinder® legacy and partnership federation. These notes describe features, operating system support, known issues and fixes.

# Chapter 2: New Features r12.52

This section contains the following topics:



## Name ID Management Profile

This release supports the de-provisioning of an individual user from a partnership, which is a portion of the SAML Name ID Management profile.

## SAML 2.0 Response to the SP on Authentication Failure

The administrator can configure a partnership to notify the Service Provider when a user fails to authenticate. The Service Provider can determine whether to redirect the user, or any other appropriate action.

## Single Sign-on to Office 365

CA SiteMinder® Federation enables single sign-on between enterprise users and Office 365 services. The following profiles are available for single sign-on to Office 365:

- WS-Federation Passive Requestor Profile
- WS-Federation Active Requestor Profile

**Note:** The CA SiteMinder® Federation Standalone product does not support single sign-on to Office 365.

# Social Sign-on

CA SiteMinder® Federation now lets users get access to a federated resource using their social networking credentials instead of the federation system credentials.

Social sign-on consists of the following features:

- Authentication of users using an OAuth authorization server.
- Configuration of a credential selector page that provides users with various identity providers as authentication choices.

The features are independent of each other. You can configure the federation system to implement one or both of them.

# Federation Use Cases for Partnership Federation

This release includes a series of federation use cases and the associated CA SiteMinder® solutions for solving business problems. See *Federation in Your Enterprise* to review these use cases.

# Log Enhancements to Aid Troubleshooting

The federation log files FWSTrace.log and the smtracedefault.log now contain checkpoint log messages that indicate what is happening during a transaction. You can search on these checkpoint messages to follow some of the processes occurring during a transaction.

In addition to the checkpoint messages, there are transaction IDs in the log to follow a transaction. If a transaction fails, the checkpoint messages and transaction IDs can help you determine the specific problem.

# Federation Transaction Process Flows

A number of diagrams and process flows explain how CA SiteMinder® Federation executes various federated transactions. The process flows also include the associated checkpoint log messages at various stages of a transaction to help troubleshoot problems.

# SAML 2.0 POST Binding

12.52 supports SAML 2.0 HTTP POST binding as a method for exchanging requests and responses during authentication and single log-out requests.

# Certificate List Cross References Partnerships

In the Administrative UI, the Certificate and Private Key List for X509 certificate management now includes a Partnerships column. This column displays the federated partnerships that use each private key/certificate. The partnerships are displayed as a link. If there is only one partnership in the column, the link takes you to a filtered partnership list. The list shows only the one partnership. If there are multiple partnerships in the column, the link takes you to an unfiltered federation partnership list.

# Chapter 3: Known Issues for Legacy and Partnership Federation

This section contains the following topics:



## Federation Does Not Support the Cookie Provider (172511)

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

## UTF-8 Characters in Federation Objects Causing Failures (179000)

**Symptom:**

In an i18n environment, federation transactions fail when a federation object contains any UTF-8 characters, which are not part of the Latin-1 (ISO-8859-1) character set.

**Solution:**

For an i18n environment, confirm that the HTTP connectors for the servlet containers in use by CA SiteMinder® Federation are configured for UTF-8. For instructions on setting the connectors to accept UTF-8 characters, see the appropriate documentation for your servlet container.

# Deployment of Federation Web Services Fails on JBoss 6.1 (174757)

**Symptom:**

Deploying the Federation Web Services (affwebservices.war) on JBoss 6.1 fails with the following exception:

```
Caused by: org.jboss.as.server.deployment.DeploymentUnitProcessingException:
JBAS011232: Only one JAX-RS Application Class allowed
```

This error is caused by an open issue in JBoss.

**Solution:**

Edit the affwebservices deployment descriptor to add a number of <context-param> entries.

**Follow these steps:**

1. Open the affwebservices deployment descriptor file (*webagent_option_pack*/affwebservices/WEB-INF/web.xml) in a text editor.
2. Add the following lines after the <web-app> tag and before the <servlet> tag:

```
<context-param>
<param-name>resteasy.scan</param-name>
<param-value>false</param-value>
</context-param>
<context-param>
<param-name>resteasy.scan.resources</param-name>
<param-value>false</param-value>
</context-param>
<context-param>
<param-name>resteasy.scan.providers</param-name>
<param-value>false</param-value>
</context-param>
```

3. Save and exit the text editor.

# 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 12.52, 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 4: Known Issues for Legacy Federation

This section contains the following topics:



## 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® 12.52 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 5: Known Issues for Partnership Federation

This section contains the following topics:



## 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.

# SSO between CA SiteMinder® Federation and Microsoft Exchange Online (Office 365) Not Yet Available

Users cannot 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 is preventing successful authentication. Users can still access Exchange Online using their web browsers and the CA SiteMinder® WS-Federation Passive Request SSO solution.

Microsoft is developing a solution to this problem.

# Errors While Deploying affwebservices on WebLogic

**Symptom:**

When deploying affwebservices on WebLogic, you see the following message:

WARNING: Unable to locate jaxb.properties for package com.sun.research.ws.wadl javax.xml.bind.JAXBException: Unable to locate jaxb.properties for package com.sun.research.ws.wadl .

**Solution:**

Ignore this message. Affwebservices has deployed without a problem.

# Rename Localized Connector Library After Upgrade

A localized version of the connector library is available for this release.

If you have upgraded from version 12.5 or older to CA SiteMinder® Federation 12.52, rename the localized connector library before using it.

**Follow these steps:**

1. Locate the following library:

   `smauthsmconnectorI18n`

2. Change the name of the library to the following name:

   `smauthsmconnector`

3. Restart CA SiteMinder® Federation 12.52.

# 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 6: Defects Fixed in 12.51

This section contains the following topics:



## 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 7: Defects Fixed in 12.52

This section contains the following topics:



## 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 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.