Sun Java System SAML v2 Plug-in for Federation Services Release Notes

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–5210–12
May 2006

071120@19028

◆ ◆ ◆ CHAPTER 1

Sun Java System SAML v2 Plug-in for Federation Services Release Notes

The Sun Java System SAML v2 Plug-in for Federation Services is an auxiliary program that works with either Sun Java System Access Manager or Sun Java System Federation Manager. The plug-in incorporates a subset of features based on the Security Assertion Markup Language (SAML) version 2 specifications and, when installed, allows support for interactions based on those specifications. A listing of key features can be found in *Sun Java System SAML v2 Plug-in for Federation Services User's Guide*.

The *Sun Java™ System SAML v2 Plug-in for Federation Services Release Notes*(this guide) contains important information available at the time of the product or patch releases of the Sun Java System SAML v2 Plug-in for Federation Services. New features and enhancements, known issues and workarounds, technical notes, and other information is addressed. Read this document before you begin using the SAML v2 Plug-in for Federation Services.

The most up-to-date version of these release notes can be found in the Sun Java System Access Manager 7 2005Q4 collection, the Sun Java System Federation Manager 7 2005Q4 collection, and the Sun Java System Access Manager 7.1 collection of manuals. You might check these locations periodically to see the most recent updates to this document and related manuals.

Read these Release Notes before you install and begin to use the plug-in. They are comprised of the following sections:

Release History

This table shows the SAML v2 Plug-in for Federation Services release history. Following are definitions of terms used to describe the releases.

- **Patch #** refers to a patch that contains code differences to upgrade a current installation.
- **Patch # Upgrade** refers to a Linux release that contains code differences to upgrade a current installation.
- **Product Release** is a full package that includes the original product code plus patch differences, if applicable.

Note – Product Releases are posted on the Sun Microsystems download web site (`http://www.sun.com/download`). Patches and patch upgrades are posted on SunSolve Online (`http://sunsolve.sun.com/pub-cgi/show.pl?target=home`).

TABLE 1–1 Release History

Date	Description
June 2007	■ Solaris (SPARC and x86) Patch 3 for Sun Java System Federation Manager 7.0 and Sun Java System Access Manager 7.0 ■ Linux Patch 3 Upgrade for Sun Java System Federation Manager 7.0 and Sun Java System Access Manager 7.0 ■ Windows Product Release (includes Patch 3) for Sun Java System Federation Manager 7.0 and Sun Java System Access Manager 7.0 ■ Solaris, Linux, and Windows Product Release (includes Patch 3) for Sun Java System Access Manager 7.1 installed using the Java Enterprise System installer or the single WAR installer
February 2007	■ Solaris (SPARC and x86) Patch 2 for Sun Java System Federation Manager 7.0 and Sun Java System Access Manager 7.0 ■ Linux Patch 2 Upgrade for Sun Java System Federation Manager 7.0 and Sun Java System Access Manager 7.0
August 2006	■ Windows Product Release for Sun Java System Federation Manager 7.0 and Sun Java System Access Manager 7.0

TABLE 1–1 Release History *(Continued)*

Date	Description
May 2006	■ Solaris (SPARC and x86) Patch 1 for Sun Java System Federation Manager 7.0 and Sun Java System Access Manager 7.0 ■ Linux Patch 1 Upgrade for Sun Java System Access Manager 7.0 ■ Linux Product Release (includes Patch 1) for Sun Java System Federation Manager 7.0
February 2006	■ Solaris (SPARC and x86) Product Release for Sun Java System Federation Manager 7.0 and Sun Java System Access Manager 7.0 ■ Linux Product Release for Sun Java System Access Manager 7.0
December 2005	■ Early Access Release (Limited Distribution)

SAML v2 Plug-in for Federation Services for Sun Java System Access Manager 7.1

The Product Release of the SAML v2 Plug-in for Federation Services for Sun Java System Access Manager 7.1 can be downloaded from the URLs listed below. This download is a full installation of the SAML v2 Plug-in for Federation Services including Patch 3 (as described in "SAML v2 Plug-in for Federation Services Patch 3" on page 8).

TABLE 1–2 SAML v2 Plug-in for Federation Services for Access Manager 7.1 Download URLs

Download URL	Operating System
`http://www.sun.com/download/products.xml?id=43e00414`	■ For instances of Access Manager 7.1 on Solaris operating system (SPARC) ■ For instances of Access Manager 7.1 on Solaris operating system (x86) ■ For instances of Access Manager 7.1 on Linux application environment ■ For instances of Access Manager 7.1 on the Windows operating system

There are two ways to install Access Manager 7.1: using the Java Enterprise System (JES) installer or using the Access Manager 7.1 single WAR. The following sections contain instructions for installing the SAML v2 Plug-in for Federation Services on these different installation types.

- "Installing SAML v2 Plug-in for Federation Services on JES Access Manager 7.1 Installation" on page 5
- "Installing SAML v2 Plug-in for Federation Services on Single WAR Access Manager 7.1 Installation" on page 6

Installing SAML v2 Plug-in for Federation Services on JES Access Manager 7.1 Installation

The procedure for installing SAML v2 Plug-in for Federation Services on an instance of Access Manager 7.1 installed using the JES Installer is the same as the procedure used for installing the plug-in on an instance of Access Manager 7.0. Instructions for installing SAML v2 Plug-in for

Federation Services on an instance of Access Manager 7.0 can be found in Chapter 2, "Installing the SAML v2 Plug-in for Federation Services," in *Sun Java System SAML v2 Plug-in for Federation Services User's Guide*. Follow this 7.0 procedure to install the plug-in on an instance of Access Manager 7.1 installed using the JES Installer.

Installing SAML v2 Plug-in for Federation Services on Single WAR Access Manager 7.1 Installation

Before you begin installing the SAML v2 Plug-in for Federation Services on a single WAR Access Manager 7.1 installation, select a machine that has had no previous installations of Access Manager or Federation Manager and at least 50MB of free space in the default installation directory for your operating system. The default installation directories are:

- Solaris: `/opt/SUNWam`
- Linux: `/opt/sun/identity`
- Windows: `/sun/identity`

The SAML v2 Plug-in for Federation Services installation procedure itself follows.

▼ To Install SAML v2 Plug-in for Federation Services on Access Manager 7.1 Single WAR Install

1. **Download the Access Manager single WAR ZIP from Sun Downloads.**

2. **Extract the ZIP to a new directory.**

   For example, `/AMzip`.

3. **Deploy `amserver.war` according to the Java Development Kit (JDK) version running on your machine.**

   - **Deploy the *extract_dir*`/application/jdk15/amserver.war` if your web container is running JDK 1.5**
   - **Deploy the *extract_dir*`/application/jdk14/amserver.war` if your web container is running JDK 1.4**

4. **Configure the deployed Access Manager with `configurator.jsp` by accessing `http://`*host-name*`:`*port*`/amserver`.**

   Fill in values for the `configurator.jsp` fields and click Configure.

5. **Make sure that the value of the `com.iplanet.am.jdk.path` attribute in *configuration_dir*`/AMConfig.properties` points to a valid JDK path.**

6. **Create a staging directory by extracting the `amserver.war` previously used in a new directory.**

   For example, `/export/war_staging`.

7. **Unzip `amAdminTools.zip` to a new directory.**

   For example, `/export/amadmin`. `amAdminTools.zip` is located in the `tools` directory of the parent directory to which you initially extracted the Access Manager single WAR ZIP.

8. **Run setup following the instructions in the extracted README.**

   You will be asked for the name of the staging directory previously created. Following the setup, an instance of `amadmin` will be created in `/export/amadmin/`*am_deploy_uri*`/bin/amadmin`

9. **Download the SAML v2 Plug-in for Federation Services Product Release for Access Manager 7.1 from the Sun Microsystems download web site (`http://www.sun.com/download/products.xml?id=43e00414`) and unpack it.**

10. **Add the following two properties to the `saml2silent` installation configuration properties file.**

    These are specific to the Access Manager single WAR install:

    - `AM_CONFIGURATION_DIR`

      Path to the location of `AMConfig.properties`. This is the value entered as the configuration directory in the Access Manager Single WAR configurator page.

    - `AMADMIN_DIR`

      The value of this property should be the same as the directory location to which the `amAdminTools.zip` was extracted. For example, **`/export/amadmin/`***am_deploy_URI***`/bin`**

11. **Choose one of the following steps, depending on the operating system you are using.**

    - **WINDOWS: Copy `ldapjdk.jar` from the WAR staging directory to the `\share\lib` directory.**

      For example:

      ```
      copy \export\war_staging\WEB-INF\lib\ldapjdk.jar \share\lib
      ```

    - **SOLARIS: Create a symbolic link in `/opt/SUNWam/bin` for the `ldapsearch` and `ldapmodify` command line interfaces.**

      For example:

      ```
      ln -s /usr/bin/ldapmodify /opt/SUNWam/bin/ldapmodify

      ln -s /usr/bin/ldapsearch /opt/SUNWam/bin/ldapsearch
      ```

    - **LINUX: The `ldapsearch` and `ldapmodify` command line interfaces installed with Linux do not have the `-j` option required by the installer. If you do not have an instance of Sun Java System Directory Server, you need to download and install the Directory Server Resource Kit (DSRK).**

- Download the DSRK ZIP from the Sun Microsystems web site.
- Unzip and install the DSRK.
- Note the location of the `ldapsearch` and `ldapmodify` command line interfaces.
- Create a symbolic link in `/opt/SUNWam/bin` for the `ldapsearch` and `ldapmodify` command line interfaces.

  For example:

```
ln -s dsrk_dir/bin/dsrk52/ldapmodify /opt/sun/identity/bin/ldapmodify

ln -s dsrk_dir/bin/dsrk52/ldapsearch /opt/sun/identity/bin/ldapsearch
```

12 **Ensure `java` is in your PATH.**

13 **Run `saml2setup install -s saml2silent` to install the patch.**

14 **Update the `AM_CLASSPATH` variable in the `saml2meta` script to include the `amSAML.properties` locale file.**

The `saml2meta` script is in `/opt/SUNWam/SAML2/bin`.

More Information Postinstallation

When finished, you will need to do the postinstallation steps as described in "Postinstallation" in *Sun Java System SAML v2 Plug-in for Federation Services User's Guide*.

SAML v2 Plug-in for Federation Services Patch 3

The following versions of Patch 3 are now available from SunSolve. For information about applying these patches, see the `rel_notes.html` included inside the patch binary.

Caution – The SAML v2 Plug-in for Federation Services Patch 3 can not be installed directly on Access Manager 7.0 or Federation Manager 7.0. You must first install the SAML v2 Plug-in for Federation Services product release, or already have an existing installation of the product release. Then, following the appropriate procedure, you can update your installation to Patch 3 for Solaris (SPARC and x86), Linux and Windows.

TABLE 1–3 SAML v2 Plug-in for Federation Services Patch 3 Numbers

Patch Number	Operating System
122983-03	For instances of Access Manager 7 2005Q4 and Federation Manager 7.0 on Solaris operating system (SPARC)

TABLE 1–3 SAML v2 Plug-in for Federation Services Patch 3 Numbers *(Continued)*

Patch Number	Operating System
122984-03	For instances of Access Manager 7 2005Q4 and Federation Manager 7.0 on Solaris operating system (x86)
122985-03	For instances of Access Manager 7 2005Q4 and Federation Manager 7.0 on Linux application environment
126360-03	For instances of Access Manager 7 2005Q4 and Federation Manager 7.0 on the Windows operating system

Note – The following issues are fixed when Patch 3 is installed:

- 6518149 Attribute name for passive request should be `IsPassive` instead of `isPassive`
- 6518158 Extra line when converting `NameIDPolicy` object to String expression
- 6518161 `XMLEncryption` message needs to support alternative form
- 6518163 Unable to handle `AttributeStatement` with both clear Attribute and EncryptedAttribute elements
- 6518944 Unable to encrypt `AttributeStatement` with multiple Attributes
- 6526628 Single logout fails if one of the SOAP binding is unavailable
- 6526665 Forced Authentication function is broken on the identity provider side
- 6527086 UTF-8 characters are corrupted in Attributes Assertions
- 6527095 UTF-8 character corruption leads to signature validation failure
- 6528347 `spSSOInit.jsp` and `idpSSOInit.jsp` do not work correctly in load balanced environment
- 6535921 SAML v2 SSO needs option to generate Liberty ID-WSF Discovery Service bootstrap resource offering. See "Bootstrapping the Liberty ID-WSF with SAML v2" in *Sun Java System SAML v2 Plug-in for Federation Services User's Guide* for information on this feature.
- 6551247 SAML v2 performance fixes
- 6551522 SAML v2 Service needs to do Certificate Revocation List (CRL) checking before validating the signing entity in the XML message. See "Certificate Revocation List Checking" in *Sun Java System SAML v2 Plug-in for Federation Services User's Guide* for information on this feature.
- 6555241 SAML v2 identity provider does not validate the `samlp:AssertionConsumerServiceURL` element
- 6557846 Identity provider single log out HTTP Redirect and service provider single log out HTTP Redirect fail when `LogoutRequest` is signed`samlp:AssertionConsumerServiceURL` element

Additional Information for Microsoft Windows Installations

The following information is applicable when installing the SAML v2 Plug-in for Federation Services on Microsoft Windows.

- "SAML v2 Plug-in for Federation Services Patch 3 Windows Installation Notes" on page 11
- "To Upgrade a SAML v2 Plug-in for Federation Services Windows Deployment on Access Manager 7.0 or Federation Manager 7.0 to Patch 3" on page 11
- "To Cleanup a Failed SAML v2 Plug-in for Federation Services Patch 3 Windows Installation" on page 11

SAML v2 Plug-in for Federation Services Patch 3 Windows Installation Notes

1. **Before installing the SAML v2 Plug-in for Federation Services Patch 3 on Windows, ensure that the LDAP server is running, and the web container is shutdown. The installer needs to modify files held by the web container process.**

2. **When installing the SAML v2 Plug-in for Federation Services Patch 3 on Solaris and Linux, sample metadata templates and a circle of trust will be automatically created. This is not done when installing on Windows. To create metadata templates and a circle of trust on Windows after installation, start your web container and run `saml2meta`. See "The saml2meta Command-line Reference" in** *Sun Java System SAML v2 Plug-in for Federation Services User's Guide* **for more information.**

To Upgrade a SAML v2 Plug-in for Federation Services Windows Deployment on Access Manager 7.0 or Federation Manager 7.0 to Patch 3

Before You Begin You should already have a staging directory from your initial installation. This variable is referred to as *war staging dir* in the following procedure.

1. **Download the Windows patch.**

   See Table 1–3.

2. **Unzip the file into a new directory.**

3. **Copy `saml2.jar` from** *unzip directory*`\saml2\lib` **to** *war staging dir*`\WEB-INF\lib`**.**

4. **Change to the** *unzip directory*`\saml2\samples\useCaseDemo` **directory.**

5. **Copy `init.jspf` to the** *war staging dir*`\samples\saml2\useCaseDemo`**.**

   This action will overwrite the earlier `init.jspf`.

6. **Generate a new WAR from the** *war staging dir***.**

7. **Redeploy the new WAR to your web container.**

To Cleanup a Failed SAML v2 Plug-in for Federation Services Patch 3 Windows Installation

It may be necessary to clean up an attempted installation of Patch 3 if an error is encountered. If this situation occurs, future attempts to install the patch will fail unless this procedure is followed.

1. **Remove the *base_dir*\saml2 directory.**

   This directory contains the SAML v2 binary bits.

2. **Remove the following SAML v2 related properties from the bottom of `AMConfig.properties`.**

   - `com.sun.identity.saml2.am_or_fm`
   - `com.sun.identity.saml2.xmlenc.EncProviderImpl`
   - `com.sun.identity.saml2.xmlenc.SigProviderImpl`
   - `com.sun.identity.common.datastore.provider.default`

3. **Remove the appropriate Access Manager or Federation Manager staging directory and extract new one.**

SAML v2 Plug-in for Federation Services Patch 2

The following patches are now available from SunSolve. For information about applying these patches and the problems they fix, see the `rel_notes.html` included inside the patch binary.

TABLE 1–4 SAML v2 Plug-in for Federation Services Patches

Patch Number	Information
122983-02	For instances of Access Manager 7 2005Q4 and Federation Manager 7.0 on Solaris operating system (SPARC)
122984-02	For instances of Access Manager 7 2005Q4 and Federation Manager 7.0 on Solaris operating system (x86)
122985-02	For instances of Access Manager 7 2005Q4 and Federation Manager 7.0 on Linux application environment

SAML v2 Plug-in for Federation Services Patch 1

The following patches are now available from SunSolve. For information about applying these patches and the problems they fix, see the `rel_notes.html` included inside the patch binary.

TABLE 1–5 SAML v2 Plug-in for Federation Services Patches

Patch Number	Information
122983–01	For instances of Access Manager 7 2005Q4 and Federation Manager 7.0 on Solaris operating system (SPARC)
122984–01	For instances of Access Manager 7 2005Q4 and Federation Manager 7.0 on Solaris operating system (x86)

TABLE 1–5 SAML v2 Plug-in for Federation Services Patches *(Continued)*

Patch Number	Information
122985–01	For instances of Access Manager 7.0 on Linux application environment **Note –** There is no patch for Federation Manager on Linux application environment. Use the recently released bits described in *Technical Note: Sun Java System Federation Manager 7.0 on Linux*

Where to Get the Sun Java System SAML v2 Plug-in for Federation Services

Solaris x86, Solaris (SPARC), Windows and Red Hat Linux versions of the SAML v2 Plug-in for Federation Services can be downloaded from `http://www.sun.com/download/products.xml?id=43e00414`. Installation instructions are in the *Sun Java System SAML v2 Plug-in for Federation Services User's Guide*. Additional information regarding the Linux version can be found in *Technical Note: Sun Java System SAML v2 Plug-in for Federation Services on Linux*, and additional information regarding the Windows version can be found in *Technical Note: Sun Java System SAML v2 Plug-in for Federation Services on Windows*.

Hardware and Software Requirements

There are no hardware requirements for the SAML v2 Plug-in for Federation Services. There are, though, hardware and software requirements for the underlying Access Manager and Federation Manager servers into which the SAML v2 Plug-in for Federation Services must be installed. See the documentation set for the appropriate product to view the respective hardware and software requirements.

- *Sun Java Enterprise System 2005Q4 Release Notes* contains hardware and software requirements for Sun Java System Access Manager 7 2005Q4.
- *Sun Java System Federation Manager 7.0 Release Notes* contains hardware and software requirements for Sun Java System Federation Manager 7 2005Q4.

A general overview of the plug-in can be found in the *Sun Java System SAML v2 Plug-in for Federation Services User's Guide*.

Known Issues and Limitations

This section describes known issues and workarounds, if available, at the time of release. It includes information for the following:

- "Uninstalling the SAML v2 Plug-in for Federation Services" on page 14
- "SAML v2 Plug-in for Federation Services Patch 3 Release" on page 14
- "SAML v2 Plug-in for Federation Services Product Release" on page 18

Uninstalling the SAML v2 Plug-in for Federation Services

After uninstalling the SAML v2 Plug-in for Federation Services, you must manually remove the *base_dir*\saml2 directory to complete the process.

SAML v2 Plug-in for Federation Services Patch 3 Release

The following sections contain information regarding known issues, limitations, and accompanying workarounds noted at the time of the release of the SAML v2 Plug-in for Federation Services Patch 3.

Windows: Single Sign-On Failure Returns Page Not Found Error Instead of Single Sign On Failed

When single sign-on fails, a Page Not Found error is thrown rather than the Single Sign On Failed error thrown on Solaris versions of the software.

WORKAROUND: None

6574265

Modify web.xml When Installing SAML v2 Plug-in for Federation Services Patch 3 on Access Manager 7.0 patch 5

After installing the SAML v2 Plug-in for Federation Services Patch 3 on Access Manager 7.0 patch 5, the web.xml file has been unnecessarily modified. This will not allow you to access the server after deployment. Uncomment the following code in the web.xml file.

```
<!--
<filter>
   <filter-name>amlcontroller</filter-name>
```

```
   <filter-class>com.sun.mobile.filter.AMLController</filter-class>
</filter>
<filter-mapping>
   <filter-name>amlcontroller</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

WORKAROUND: The SAML v2 Plug-in for Federation Services will try to comment out this code again. To alleviate this from happening, edit the `web.xml` file in the staging directory AFTER installation is complete, and regenerate the WAR using the `jar` command.

Enable XML Encryption for Access Manager or Federation Manager using the Bouncy Castle JAR

If you want to enable the XML encryption feature and your web container is running JDK 1.4, or you are running IBM Websphere (JDK 1.4 and 1.5) as your web container, follow this procedure to use Bouncy Castle to generate a transport key.

Note – The Bouncy Castle Crypto API is a Java implementation of cryptographic algorithms.

---

1. Download the Bouncy Castle provider from Bouncy Castle.

   For example, if using JDK 1.4, download the `bcprov-jdk14-136.jar`.
2. Copy the downloaded file to the *jdk_root*`/jre/lib/ext` directory.
3. **OPTIONAL:** If using the domestic version of the JDK, download the appropriate JCE Unlimited Strength Jurisdiction Policy Files from java.sun.com.

   Note – If using IBM WebSphere, go to `http://www.ibm.com` to download additional required files.

   ---

4. **OPTIONAL:** Copy the downloaded `US_export_policy.jar` and `local_policy.jar` files to the *jdk_root*`/jre/lib/security` directory.
5. Edit the *jdk_root*`/jre/lib/security/java.security` file to add Bouncy Castle as one of the providers.

   For example,
   `security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider`
6. Set the `com.sun.identity.jss.donotInstallAtHighestPriority` property in the `AMConfig.properties` file to `true`.
7. Restart the web container.

6344530

Web Browser Artifact Profile Fails When SAML v2 Plug-in for Federation Services Patch 3 Installed on Federation Manager and WebSphere

When Federation Manager is deployed in WebSphere Application Server, federation using the Web Browser Artifact Profile fails when the service provider attempts to send an artifact back to the identity provider.

WORKAROUND: You must override WebSphere's default SOAP factory by doing the following:

1. Edit WebSphere's `server.xml` file (located in *WebSphere-base*`/WebSphere/AppServer/config/cells/`*cell-name*`/nodes/`*node-name*`/servers/`*server-i*
   by replacing

   ```
   <jvmEntries xmi:id="JavaVirtualMachine_1" classpath=""
   bootClasspath="" verboseModeClass="false" verboseModeGarbageCollection="false"
   verboseModeJNI="false" runHProf="false" hprofArguments=""
   debugMode="false" debugArgs="-Djava.compiler=NONE -Xdebug -Xnoagent
   -Xrunjdwp:transport=dt_socket,server=y,suspend=n, address=7777"
   genericJvmArguments="">
   ```

   with

   ```
   <jvmEntries xmi:id="JavaVirtualMachine_1" verboseModeClass="false"
   verboseModeGarbageCollection="false" verboseModeJNI="false"
   initialHeapSize="256" maximumHeapSize="256" runHProf="false"
   hprofArguments="" debugMode="false" debugArgs="-Djava.compiler=NONE
   -Xdebug -Xnoagent
   -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=7777"
   genericJvmArguments="-Dcom.iplanet.am.serverMode=true">
   <classpath>/usr/share/lib/saaj-api.jar:/usr/share/
   lib/saaj-impl.jar</classpath>
   ```

   Note – The *cell-name*, *node-name*, and *server-instance* variables identify the name of the cell, node, and server in which Federation Manager is deployed.

2. Restart the WebSphere instance.

6320498

`saml2meta` Does Not Return Error When `-m` Option is Used for Extended Metadata

When the `-m` option is used with the `saml2meta` command line interface to import extended metadata, it does not return an error message even though the `-m` option should be used for standard metadata imports only.

WORKAROUND: None. See “The saml2meta Command-line Reference” in *Sun Java System SAML v2 Plug-in for Federation Services User’s Guide* for correct usage and syntax.

6559482

`saml2meta template` Subcommand Throws Exception in Access Manager Single WAR Install

When the SAML v2 Plug-in for Federation Services is installed on an instance of Access Manager that was installed using the single WAR, `saml2meta` throws a `MissingResourceException` when using the `template` subcommand with the certificate alias option.

WORKAROUND: Edit `saml2meta` by appending *war_staging_dir*`/WEB_INF/classes` to the value of the `AM_DIRS` variable.

6563751

`saml2meta` Throws Exception When Access Manager or Federation Manager is SSL Enabled

When the Access Manager or Federation Manager server is SSL enabled, `saml2meta` throws a `java.lang.NoClassDefFoundError` exception.

WORKAROUND: Edit `saml2meta` by doing the following:

1. Remove the `${BOOTCLASSPATHOPTION}` option when running the `java` command for `com.sun.identity.saml2.meta.SAML2Meta` (line 123).
2. Add the following properties when running the `java` command for `com.sun.identity.saml2.meta.SAML2Meta` (line 123).
   - **`-Djavax.net.ssl.trustStore=`***full path for the key store file*
   - **`-Djavax.net.ssl.trustStoreType=`***JKS* where JKS is a Java key store file containing the certificate authority certificates of the SSL certificate for the server's web container.

SAML v2 Logout Fails After a Session Upgrade

SAML v2 Logout fails after a session upgrade.

WORKAROUND: None

6563739

Extended Metadata Attribute Doesn't Work

The `wantLogoutResponseSigned` attribute in the extended metadata configuration file doesn't work.

WORKAROUND: None

6559732

SSO With POST Binding Fails if User Has No Attributes

SSO with POST binding fails if `wantAttributeEncrypted` is on but the identity provider user doesn't have any attributes.

WORKAROUND: Include at least one attribute if `wantAttributeEncrypted` is on.

6563280

Increase Directory Server Values When Installed on Federation Manager

After installing the SAML v2 Plug-in for Federation Services on an instance of Federation Manager running on Directory Server, increase the value of `nsslapd-sizelimit` to, for example `4000`, and set `nsslapd-lookthroughlimit` to unlimited; for example `-1`. This will avoid hitting the Directory Server search and size limit.

SAML v2 Plug-in for Federation Services Product Release

The following sections contain information regarding known issues, limitations, and accompanying workarounds noted at the time of the initial release of the SAML v2 Plug-in for Federation Services.

SAML v2 Authentication Module is not Automatically Registered in Access Manager Legacy Mode

When installing the SAML v2 Plug-in for Federation Services on an instance of Access Manager in legacy mode, the SAMLv2 authentication module is not automatically enabled in the default organization.

Workaround: After installing the SAML v2 Plug-in for Federation Services on an instance of Access Manager in legacy mode, use the `amadmin` command line tool to load the following XML file in order to register the SAMLv2 authentication module.

```
<Requests>
<OrganizationRequests DN="<root_suffix>">
   <RegisterServices>
       <Service_Name>sunAMAuthSAML2Service</Service_Name>
   </RegisterServices>
</OrganizationRequests>
</Requests>
```

This step is necessary for service providers only.

(6431995)

Exception Thrown During Installation if Web Container Has Not Been Started

If the underlying web container running an instance of Access Manager or Federation Manager is not started, a harmless exception concerning the creation of the circle of trust is thrown during installation of the SAML v2 Plug-in for Federation Services. The circle of trust is successfully created in the data store (flat file or LDAP) despite this message and the SAML v2 Plug-in for Federation Services will work correctly after the web container has been started.

Workaround: None

(6371281)

Schema Loading Fails on Sun Java System Federation Manager

When installing the SAML v2 Plug-in for Federation Services on the Solaris™ 8 Operating System (OS) and the Solaris 9 OS, set the `LOAD_SCHEMA` property in the `saml2silent` installation configuration properties file to `false` before running the `saml2setup` installer.

Workaround: After the SAML v2 Plug-in for Federation Services has been successfully installed, you must load the schema manually.

- On Sun Java System Directory Server, run the following two commands:

  `/usr/bin/ldapmodify -h` *directory-host* **`-p`** *directory-port* **`-a -D`** *administratorDN* **`-w`** *administratorPW* **`-f`** *FederationManager-base*`/`*product-directory*`/saml2/ldif/saml2_sds_index.ldif`

  `/usr/bin/ldapmodify -h` *directory-host* **`-p`** *directory-port* **`-D`** *administratorDN* **`-w`** *administratorPW* **`-f`** *FederationManager-base*`/`*product-directory*`/saml2/ldif/saml2_sds_schema.ldif`

- On Microsoft® Active Directory, run the following command:

  `/usr/bin/ldapmodify -a -h` *directory-host* **`-p`** *directory-port* **`-D`** *administratorDN* **`-w`** *administratorPW* **`-f`** *FederationManager-base*`/`*product-directory*`/saml2/ldif/saml2_ad_schema.ldif`

(6374746)

Exception Thrown During Single Sign-on BEA WebLogic® Server

During single sign-on (after a successful log in to the identity provider), an exception is thrown and written to the WebLogic Server logs. This is an issue related to the `idpArtifactResolution.jsp`.

Workaround: Remove or comment out the following lines in `idpArtifactResolution.jsp`:

```
out.clear();
out = pageContext.pushBody();
```

(6375283)

`saml2setup` Doesn't Generate Metadata Against Federation Manager Running on Microsoft Active Directory

By default, `saml2setup` uses `amadmin` as the administrator identifier to log in during installation. A deployment incorporating Federation Manager and Microsoft Active Directory requires a full distinguished name to be passed.

Workaround: After the SAML v2 Plug-in for Federation Services has been successfully installed, you can run `saml2meta`:

- To generate metadata for a hosted identity provider on Federation Manager:

  Federation Manager`/SUNWam/saml2/bin/saml2meta/saml2meta template [-i` *staging-directory*`] -u` *full-DN-admin-user* `-w` *admin-user-password* `-d` *idp-metaAlias* `-e` *idp-entityID* `-m idpMeta.xml -x idpExtended.xml`

- To generate metadata for a hosted service provider on Federation Manager:

  Federation Manager`/SUNWam/saml2/bin/saml2meta/saml2meta template [-i` *staging-directory*`] -u` *full-DN-admin-user* `-w` *admin-user-password* `-d` *sp-metaAlias* `-e` *sp-entityID* `-m spMeta.xml -x spExtended.xml`

(6377631)

`saml2setup` Installs Older Mobile Access Packages

`saml2setup` installs old versions of the `SUNWamma` and `SUNWammae` packages. Because of this the following lines in the `web.xml` file in Access Manager are commented out.

```
<filter>
    <filter-name>amlcontroller</filter-name>
    <filter-class>com.sun.mobile.filter.AMLController</filter-class>
</filter>

<filter-mapping>
    <filter-name>amlcontroller</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

Note – This is not an issue for Access Manager 7.1 or Federation Manager 7.0 installations.

Workaround: Before uncommenting the filter properties in `web.xml`, you need to download from Sunsolve (`http://sunsolve.sun.com/`) and apply the following patches to upgrade your

mobile access packages. (If newer patches have become available use them.) See the Access Manager procedure called *Upgrade Access Manager mobile access software* in the *Sun Java Enterprise System 5 Upgrade Guide for UNIX* for more information.

TABLE 1–6 Mobile Access Packages

Description	Software
Solaris Patch ID	■ 119530-01 (SPARC) ■ 119531-01 (x86)
Linux Patch ID	119532-01 contains ■ `sun-identity-mobileaccess-6.2-25.i386.rpm` ■ `sun-identity-mobileaccess-config-6.2-25.i386.rpm`

Afterwards, the lines can be uncommented and `services.war` can be redeployed.

(6377668)

Redistributable Files

Sun Java System SAML v2 Plug-in for Federation Services does not contain any files that you can redistribute to non-licensed users of the product.

How to Report Problems and Provide Feedback

If you have problems with the Sun Java System SAML v2 Plug-in for Federation Services, contact Sun customer support using one of the following mechanisms:

- Sun Support Resources (SunSolve)

  This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.
- The telephone dispatch number associated with your maintenance contract.

So that we can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs, and its impact on your operation.
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem.
- Detailed steps on the methods you have used to reproduce the problem.
- Any error logs or core dumps.

Related Third-Party Web Sites

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun Microsystems is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Feedback

Sun Microsystems is interested in improving its documentation and welcomes your comments and suggestions. To share your thoughts, go to `http://docs.sun.com` and click the Send Comments link at the top or bottom of the page. In the online form provided, include the document title and part number. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the title of this book is *Sun Java System SAML v2 Plug-in for Federation Services Release Notes*, and the part number is 819–5210.

Additional Sun Resources

For product downloads, professional services, patches, support, and additional developer information, go to the following locations:

- Download Center (`http://wwws.sun.com/software/download/`)
- Sun Software Service Plans (`http://www.sun.com/service/support/software/`)
- Sun Java Systems Services Suite (`http://www.sun.com/service/sunjavasystem/sjsservicessuite.html`)
- Sun Enterprise Services, Solaris Patches, and Support (`http://sunsolve.sun.com/`)
- Developer Information (`http://developers.sun.com/prodtech/index.html`)

If you have technical questions about any Sun products, contact Sun Support and Services (`http://www.sun.com/service/contacting`).