Sun Java™ System Access Manager Release Notes

Version 6 2005Q1

May 25, 2005

Part Number 817-7642-12

These Release Notes contain important information available at the time of release of Sun Java System Access Manager 6 2005Q1 (formerly Sun Java System Identity Server). New features and enhancements, known issues and limitations, and other information are addressed here. Read this document before you install and use this release.

The most up-to-date version of these release notes can be found at the Sun Java System documentation web site:

`http://docs.sun.com/prod/entsys.05q1`

Check the web site prior to installing and setting up your software and then periodically thereafter to view the most up-to-date release notes and product documentation.

These release notes contain the following sections:

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

NOTE Sun 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.

Release Notes Revision History

Table 1 Revision History

Date	Description of Changes
May 25, 2005	Added problem 6245660 with workaround to the Configuration section of Known Issues and Limitations. Added the Documentation Updates and Errata section.
February 25, 2005	Revised Table 2, “Hardware and Software Requirements” to list the supported versions of Red Hat™ Linux.
February 2, 2005	Access Manager 6 2005Q1 release. First publication of these release notes.

About Access Manager 6 2005Q1

Sun Java System Access Manager is an identity management solution designed to meet the needs of rapidly expanding enterprises. Access Manager enables you to get identities for your employees, your partners and suppliers into one online directory. Then it provides a means for establishing policies and permissions regarding who has access to which information in your enterprise. Access Manager is the key to all your data, your services, and who has access to what—it’s the key to all your internal and external business relationships.

What's New in This Release

Access Manager 6 2005Q1 includes the following features. For more a more detailed explanation of these features, see the *Sun Java System Access Manager Technical Overview*.

- Product name has changed from Identity Server to Access Manager
- Support for Solaris 10
- Support for new web container: Sun Java System Application Server Enterprise Edition 8 2005Q1 (8.1)
- New or revised authentication modules:
    - Java Database Connectivity (JDBC)
    - Mobile Station ISDN (MSISDN)
    - Active Directory
    - Security Assertion Markup Language (SAML): SAML authentication support is released as an authentication module, which allows SAML authentication to be part of the authentication stack.
- Session Failover
    - Two or more instances of Access Manager 6 2005Q1, with each instance running on a supported web container on a different host server.
    - Message Queue broker cluster that manages the session messages between the Access Manager instances and the session store database.
    - Berkeley DB by Sleepycat Software, Inc. (http://www.sleepycat.com/) as the session store database. The Berkeley DB client daemon is amsessiondb.
- Policy Management includes a new Resource Name plug-in: `HttpURLResourceName`.
- Console enhancements:
    - Ability to customize the view of each object type in the navigation pane by displaying one or more of the attributes of the object.
    - Ability to add new object types in the navigation pane drop-down menu (for example, adding an entry for printers or buildings).

- Client SDK:
    - Repackaged SDK (Authentication, Service Management, User Management, SAML, Policy Client, and Session components) so Java application developers can better integrate with Access Manager.
    - Removed the dependency on the serverconfig.xml file and minimized the footprint of the jar files.
- Federation Management:
    - Support for the Liberty Alliance Project (LAP) Name Identifier Mapping Protocol
    - Support for the LAP Identity Web Services Framework (ID-WSF) Discovery Service Specification, Version 1.1
    - Support for the LAP ID-WSF Authentication Service Specification
    - Support for the LAP Metadata Description and Discovery Specification
    - Support for the LAP Liberty Identity Federation Framework (ID-FF) Extended Profiles:
        - Dynamic Identity Provider Proxying
        - Affiliation Federation
        - One-time Federation
        - Name Identifier Mapping Profile
        - Name Identifier Encryption Profile
- A performance tuning script is available to tune Application Server Enterprise Edition 8 2005Q1 (8.1) as a web container

Hardware and Software Requirements

The following hardware and software are required for this release of Access Manager.

Table 2 Hardware and Software Requirements

Component	Requirement
Operating system	Solaris™ Operating System (OS), SPARC® Platform Edition, versions 8, 9, and 10
	Solaris™ OS, x86 Platform Edition, versions 9 and 10
	Red Hat™ Linux, WS/AS/ES 2.1 Update 2
	Red Hat™ Linux, WS/AS/ES 3.0 Update 1
RAM	512 Mbytes
Disk space	250 Mbytes for Access Manager and associated applications

Supported Browsers

This release of Access Manager supports the following browsers:

Broswer	Platforms
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000, Sun Linux, Red Hat™ Linux 8.0
Microsoft Internet Explorer 6.0	Windows 2000, Windows™ XP, Sun Linux, Red Hat Linux 8.0
Mozilla 1.7.1	Windows 2000, Sun Linux, Red Hat Linux 8.0, Solaris™ 9 and 10, Solaris™ OS, x86 Platform Edition, versions 9 and 10
Netscape™ 4.79	Windows NT, Solaris 8 and 9
Netscape™ 6.2.1	Windows NT, Windows 98, Sun Linux, Red Hat™ Linux Advanced Server 2.1, Solaris™ OS, x86 Platform Edition, versions 9 and 10
Netscape™ 7.0	Windows 2000, Sun Linux, Red Hat Linux 8.0, Solaris 9 and 10, Solaris™ OS, x86 Platform Edition, versions 9 and 10

Bugs Fixed in This Release

The table below describes the bugs fixed in Access Manager 6 2005Q1:

Table 3 Bugs Fixed in the Access Manager 6 2005Q1

Bug Number	Description
5050332	On Linux systems, amserver stop does not stop the amunixd process
5049218	Error in Console While Searching for Users When User Management is Disabled
5048378	smtp Server Port Property Incorrect in AMConfig.properties
5043752	Failed message appears when running am2bak
5042100	Policy Admin Cannot Not Modify Own Profile
5041529	BasicEntitySearch Filter Hardcoded to uid
5038600	Users Cannot Be Created With the SAML Service
5037978	Creating roles with defined access permissions as org admin generates error
5026635	Console Samples Do Not Compile
5016725	Modifications in Referral Policy Rule Not Reflected in Suborg
5013994	Authlevel Login Fails for Japanese Browsers
5008960	amadmin returns incorrect error message
4996479	Services With Policy Schema Shows as “Addable” to a User
4961370	“**” Search Mask Does Not Work
4959895	Entity Descriptors Search Filter Does Not Work Properly
4959071	Idle Sessions Are Not Cleaned Up
4931907	Services Disappear With Service Type Role User Login
4931163	Naming Attributes Should Be Lower Case
4930610	am2bak And bak2am Version Messages Only In English
4922030	Conflict Resolution Level In Fixed Locale
4916683	Message for msgid-msgstr Pairs in backup_restore.po Not Localized
4853809	Service Registration Problem
4853809	Registering All Services May Not Register All Available Services

Installation Notes

The amconfig script now supports deployment of additional instances of Access Manager using Application Server Enterprise Edition 8 2005Q1 (8.1) as a web container, after you install the first instance using the Java Enterprise System installer.

For information about running the configuration scripts, see the *Access Manager 6 2005Q1 Administration Guid*e.

See also Installation under Known Issues and Limitations.

Known Issues and Limitations

This section contains a list of the more important known issues at the time of the Access Manager 6 2005Q1 release. This section covers the following topics:

- Installation
- Authentication
- Access Manager Samples
- Command-Line Tools
- Configuration
- Access Manager Console
- Federation
- Logging Service
- Policy
- Single Sign-On
- Access Manager SDK
- Internationalization (i18n)
- Cookies
- Cookie Hijacking

Installation

amadmin on SDK Installations With Secure Server Throws Exceptions (#5107584)

In Access Manager 2005Q1, if you install a full installation of a secure Access Manager and then install an SDK installation to use the full install, exceptions may be thrown. This is because the `com.iplanet.am.admin.sli.cerdb.prefix` property has the wrong value with Web Server.

Workaround

1. Edit `AMConfig.properties`.
2. Change the property `com.iplanet.am.admin.cli.certdb.prefix` to `https-<ws-instance-name>-<ws-hostname>-`.
3. Restart the web server.

AMSDK Installation with Web Containers Contains Broken Links to Shared Components on Linux (#6199933)

If you install the Access Manager SDK on for any web container on the Linux platform, several shared component Links are broken.

Workaround

Remove incorrect links and create correct links.

To remove the links:

```
cd ${AM_INSTALL_DIR}/identity/lib

rm -rf jaxrpc-spi.jar relaxngDatatype.jar xsdlib.jar
```

To create new links:

```
ln -s /opt/sun/private/share/lib/jaxrpc-spi.jar

ln -s /opt/sun/private/share/lib/relaxngDatatype.jar

ln -s /opt/sun/private/share/lib/xsdlib.jar
```

Typo in Argument to Referential Integrity Plugin Impacts Performance (#5029256)

When Access Manager enables the referential integrity plugin for the Directory Server, in argument 11 of the plugin, the attribute name has a typo. The attribute name is given as `iplanet-am-modifable-by`. This causes a `search not indexed` warning in directory error log, when an organization is deleted.

The referential integrity plugin requires all attributes mentioned in its arguments to be indexed, and the attribute which is indexed is `iplanet-am-modifiable-by`. This may impact Access Manager performance.

Application Server xercesImpl.jar Causes the To JVM to Crash (#6223676)

Application Server 8.1 EE's `xercesImpl.jar` in `/opt/sun/appserver/lib` for RedHat Linux (or `/opt/SUNWappserver/appserver/lib`) for Solaris gets loaded before the shared component version of `xercesImpl.jar` in `/opt/sun/share/lib` for RedHat Linux (or `usr/share/lib` for Solaris).

The Application Server version gets loaded by the class loader before the shared component version. When this happens, the outdated version from the Application Server cannot keep up with thousands of JSPs waiting to be processed. The JVM either hangs or crashes.

Workaround

Rename the `xercesImpl.jar` in `opt/sun/appserver/lib` for Red Hat AS 2.1 or 3.0 or in `/opt/SUNWappserver/appserve/lib` for Solaris 9 or 10 for both SPARC and x86. The JVM classloader will then be forced to use the shared components' `xerceImpl.jar` in `/opt/sun/share/lib` for Red Hat AS 2.1 or 3.0 or in `/usr/share/lib` for Solaris 9 and 10.

Installer does not allow user to enter protocol during AM SDK installation (#6180090)

If you install the Access Manager SDK, the "Access Manager: Web Container for running Sun Java System Access Manager Services" panel does not ask for the protocol of the web container that is running the Access Manager services. The installer assumes that the web container uses the `http` protocol; however, you might need to specify the `https` protocol to access an SDK installation that uses an SSL enabled Access Manager installation.

Workaround

In the `AMConfig.properties` file, set the protocol associated with the Access Manager server installation to `https`. For example:

```
com.iplanet.am.server.protocol=https
com.iplanet.am.console.protocol=https
```

Access Manager adds servlet.jar to the server CLASSPATH (#5016348)

Access Manager is placing a `servlet.jar` in the server CLASSPATH for its supported web containers. This file can cause unexpected results because each web containers bundles a `servlet.jar` file in its implementation.

Workaround

Remove the `servlet.jar` from the CLASSPATH.

Access Manager Samples

Samples return warnings while compiling with JDK 1.5 (#5102149)

Samples that are included with Access Manager return warnings if they are compiled with JDK 1.5.

Workaround

Avoid these warnings by:

- When using JDK 1.5, add `encoding="ISO-8859-1"` to the compilation command line.

  or

- Use JDK 1.4 to compile the samples.

Omissions in SAML xmlsig sample result in compilation failures (#5090925)

Omissions in the SAML `xmlsig` samples result in compilation failures if they are compiled with JDK 1.5. This problem does not occur if you are compiling with JDK 1.4.2.

Workaround

If you are compiling with JDK 1.5, follow these steps to set up the LD_LIBRARY_PATH:

1. Find the Readme.html or Readme.txt file for the SAML samples in the `xmlsig` directory.
2. Under section 3 “Instructions to set up the XMLSIG sample on Solaris,” in step 4, set the LD_LIBRARY_PATH as *web-server-install-directory*`/bin/https/lib`.
3. Add `/usr/lib/mps/secv1` to LD_LIBRARY_PATH to pick up the JSS library and its dependencies.

Authentication

User Modification Notification Through Email Is Not Working (#6212964)

The User Modification Notification through E-mail mechanism, located in the Administration Service, is not currently working.

SafeWord Connections Are Not Closed (#5073718)

If you try to login to Access Manager, go to the SafeWord challenge response page and never enter a password, there is no timeout out on the connection. If the you closes the browser, the connection never closes with the SafeWord server.

LDAP Authentication Is Doing Anonymous Bind for LDAP Directory Server Connection (#5090018)

Access Manager is not passing the bind DN and password to Directory Server for an LDAP connection, which affects authentication when the anonymous bind in the LDAP Directory Server is disabled.

Workaround

Enable anonymous bind for your Directory Server.

Persistent Cookie Mode Property is Inconsistent (#5038544)

In Persistent Cookie mode, the UserId property set in the token is inconsistent. Because of this, the policy agent, which depends on the UserID property, may fail.

Workaround

Use `UserToken` for a non DN value and `Principal` for the DN value.

Reloading the Session Timeout Page Will Authenticate User with Valid User name and Password (#4697120)

At the login page, if a user waits for the page to timeout and then enters a valid user name and password, the user will see the session timeout page. The user will be authenticated to Access Manager if the user reloads the page without re-entering user name and password.

Different Directories Must Be Specified For Multiple SafeWord Servers (#4756295)

A configuration with multiple organizations using their own respective SafeWord servers have to specify their own `.../serverVerification` directories in their SafeWord Authentication service templates. If you leave the default value, and all servers use the same directory, then the first organization to authenticate with its SafeWord server will be the only one that works.

Command-Line Tools

ldapsearch and ldapmodify utilities in /opt/SUNWam/bin directory do not work correctly (#4954779)

The ldapsearch and ldapmodify utilities in /opt/SUNWam/bin directory return fatal errors.

Workaround

Add the *DirectoryServer-base*`/lib/` path to your LD_LIBRARY_PATH environment variable.

am2bak and bak2am Scripts Not Working for Linux (#5053866)

The `am2bak` and `bak2am` restore scripts do not work if Access Manager is running on a Linux system.

Workaround

1. Correct the path of the following commands:
   - `ECHO=/usr/bin/echo` should be `ECHO=/bin/echo`
   - `uid='/usr/xpg4/bin/id -un'` should be `uid='/usr/bin/id -un'`
   - `/usr/bin/tar` should be `/bin/tar`
   - `/usr/bin/rm` should be `/bin/rm`
   - `/usr/bin/grep` should be `/bin/grep`
   - `/usr/bin/ps` should be `/bin/ps`
   - `/usr/bin/ls` should be`/bin/ls`
2. Modify the `check_for_invalid_chars()` function. For example:

```
check_for_invalid_chars() {
echo "$1" | grep '[^/_.a-zA-Z0-9a-]' > /dev/null
if [ $? = 0 ]; then
return 1
else
return 0
fi
}
```

amadmin Returns Incorrect Error Message (#5008960)

The `import` option of `amadmin` incorrectly throws the same error message for all related errors.

amverifyarchive on Console-Only Install Has Unswapped Tags (#4993375)

If you perform an Access Manager console-only installation, the `amverifyarchive` utility does not have the following tags swapped out in this script: JSSHOME, JDK_HOME, BASEDIR, and PRODUCT_DIR.

Configuration

System creates invalid service host name when load balancer has SSL termination (#6245660)

If Access Manager is deployed with Web Server as the web container using a load balancer with SSL termination, clients are not directed to the correct Web Server page. Clicking the Sessions tab in the Access Manager Console returns an error because the host is invalid.

Workaround

In the following examples, Web Server listens on port 3030. The load balancer listens on port 80 and redirects requests to Web Server.

In the *web-server-instance-name*/`config/server.xml` file, edit the `servername` attribute to point to the load balancer, depending on the release of Web Server you are using.

For Web Server 6.1 2005Q1 Service Pack (SP) releases, edit the `servername` attribute as follows:

```
<LS id="ls1" port="3030" servername="loadbalancer.external.example.com:80"
defaultvs="https-sample" security="false" ip="any" blocking="false" acceptorthreads="1"/>
```

Web Server 6.1 2005Q1 SP2 (or later) can switch the protocol from `http` to `https` or `https` to `http`. Therefore, edit `servername` as follows:

```
<LS id="ls1" port="3030" servername="https://loadbalancer.external.example.com:443"
defaultvs="https-sample" security="false" ip="any" blocking="false" acceptorthreads="1"/>
```

WebSphere Application Server 5.1 Fails to Start After Successful Configuration on Linux (#6204646)

If you install the Access Manager SDK component for WebSphere on Linux and then run `amwas51config` with correct `amsamplesilent` file, WebSphere will fail to start.

Workaround

Add `/opt/sun/private/lib` in the `LD_LIBRARY_PATH` as follows:

```
LD_LIBRARY_PATH="$WAS_LIBPATH":$LD_LIBRARY_PATH:/opt/sun/private/lib

export LD_LIBRARY_PATH ;;
```

In `server.xml`, remove the **“/:”** before `the -Djava.util.logging.config.class` option.

certdb Alias Not Set Correctly For Web Server (#6212532)

If you enable SSL for Web Server with Access Manager, and then run `amadmin`, it throws “namingservice not available” error. Thought the browser, it works as expected.

Indices Are Always Created For userRoot Irrespective of the Backend Name (#5002886)

The `index.ldif` hardcodes the userRoot for creating index for the attributes. It is possible to install Access Manager on a rootsuffix residing on any arbitrary backend database name. The backend name can be obtained by `ldapsearch` with base `cn=config` using `nsslapd-suffix=SUFFIX_NAME` as the filter.

Federation

Federation Management Contact Person Throws Exception (#6213102)

If create a new Provider and then add a new Contact Person to that provider, you may receive the following error:

```
The server encountered an internal error () that prevented it from fulfilling this request
```

Remote Logging is not Working For amFederation.access Logs (#6197608)

When remote logging is configured, all the logs are written properly to the remote Access Manager instance, with the exception of amFederation.access. The log record is not written.

Workaround

Use `AccessController.doPrivileged(AdminTokenAction.getInstance());` in `LogUtils`.

fedCookie Status Does Not Change (#6202574)

If you perform a Federation Termination for federated users on and SP and IDP, the `fedCookie` status will still display `YES`. It should show `NO`.

Personal Profile Containers Fail For Query/Modify (#6189808)

The following Personal Profile containers fail for either a query or modify operation:

```
LegalIdentity/Gender
EmploymentIdentity/AltO
```

Exception Thrown for PP Modify if Attribute Value is Empty (#5047103)

Access Manager throws an exception when you perform a PP Modify with an empty attribute value. For example, if you create the setup to test the `sis-ep` sample and then send the EP Modify page and click on the button without entering any value for the attribute, the exception is incorrectly thrown.

Policy Effect Requires Server Restart (#5045036)

Federation policy implementation does not take effect until you restart the server. This is valid for both Application Server and Web Server. You must restart the server only after a fresh install and when the policy is first implemented.

Access Manager Console

Unable to Create Users With Large Number of People Containers in the DIT (#5079609)

If you create couple a large number of People Containers (over a thousand) and then login to Access Manager console and create a new user, the user will not be created because no people containers are found.

This is because the `UMCreateUserModelImpl.getPeopleContainers()` fails with search time limit errors, even though the Directory Server finds a large number of People Containers before hitting the time limit.

Workaround

Enable Show People Container in the Access Manager console, go to the specific People Container and create users there.

Top-level Help Desk Admin Role With Read Only Access Can Create New Users (#5109348)

Currently, the default for Help Desk Admin role is set to Full Access. Changing it to Modify will disable the New and Delete buttons in the navigation frame but still allow the admin to modify the user entry properties.

Workaround

Bring up the Help Desk Admin properties page, and change the view to available actions. Locate the User row and change the setting from Full Access to Modify.

Exception Thrown When Select Affiliate Option of an Affiliate Entity (#6203563)

In the Federation Management module, an exception will be thrown when you select View>Affiliates in the Affiliate Entity page.

Workaround

Modify the JSP so the height attribute is outside the closing JATO tag. In `FSAffiliateProfile.jsp`, line 104 change to:

```
<td width="1%"><img src="<%consoleImages%>/spacer.gif" width=<jato:text
name="defaultAttrNameWidth" /> height="1" alt=""></td>
```

Note the `/>` coming before the height attribute.

Error in Affiliates Display Option (#6194139)

Access Manager will return an error page when the Affiliates Display option, in the Federation Management module, is the only option in the menu and is set as the default.

Can Not Modify Services for Users as People Admin Role (#6174652)

If you are logged is as the top-level People Admin Role, you can add a new service to a user, but you cannot modify any services.

Workaround

Edit the display profile for the People Admin role and give it the necessary view menus and available actions.

CValues Not Retained When Clicking Back Button (#4992972)

Whenever there is a multiple page process, such as creating a group, role, or adding a condition to a policy, and then the Back button is selected, the values in the previous page will not be restored.

Refresh Problem For Hosted Provider in Federation Management Module (#4915894)

In the Federation Management module, if you modify and save any attributes in the Identity Provider view of a hosted provider, the changes will be saved, but will not be automatically refreshed in the display.

Workaround

Exit the Federation Management module by selecting a different module (for example, Service Configuration) and then return to the Federation Management module. This will refresh the display.

Console Does Not Refresh User Attribute Changes (#4931455)

The Access Manager console Navigation frame does not refresh to indicate changes in User attribute values in made in the Data frame. Refresh the page manually to view the changed values.

Port Problems With Internet Explorer (#4864133)

Due to an incompatibility with Internet Explorer, you should not use port 80 as the Access Manager port number when running http or port 443 when running https.

Logging Service

Logging Problem When Java Security Is Enabled (#4926520)

`jdk_logging.jar` may not work when Java Security is enabled.

Workaround

If Java Security is enabled and you have a JDK version previous to 1.4, include the following permission in the java security file:

```
permission java.lang.RuntimePermission  shutdownHooks
```

Policy

Matching Entries are not Returned When nslookthrough Limit Reached (#5013538)

Matching entries are not returned to the Access Manager console even after reaching the admin limits defined in `nslookthrough`.

Workaround

Tune the `nslookthroughlimit` parameter to compensate for the number of entries.

Policy Not Enforced for Aliased Tokens (#4985823)

If you use user alias a to log in to Access Manager against an authorization module other than LDAP or Membership, and then attempt to access a protected resource, access is denied.

Problem With Policy Sample (#4923898)

The `Readme.html` located in the Policy Sample excludes information that causes the sample not to run.

Workaround

To run the sample, the `LD_LIBRARY_PATH` environment variable must include the path to the `NSPR`, `NSS`, and `JSS` shared libraries.Set `LD_LIBRARY_PATH` to include `/usr/lib/mps/secv1` for Solaris systems or `/opt/sun/private/lib` for Linux systems.

Access Manager SDK

Attribute Uniqueness Broken in the Top Level Org for Naming Attributes (#6204537)

Attribute Uniqueness for naming attributes does not function in the Top Level organization. However, user and organization attribute uniqueness is enforced correctly.

EventService Runs into a Tight Loop When it Does Not Get Persistent Search Connection (#6205443)

The EventService (ES) thread successfully adds the listeners (LDAP JDK successfully adds the listener) even when the number of Persistent Searches is connected. But, when a ES thread attempts to get a response, an LDAPResponse reports (error code 51) that Persistent Search connections are unavailable. The ES then tries to re-establish the listeners again. So, this becomes a tight loop.

Document Use of certutil For Access Manager SDK Installations That Use SSL Servers (#5027614)

Users are experiencing security-related errors and exceptions when trying to communicate from SDK-only machines with SSL-enabled Access Manager servers. In this scenario, the Access Manager SDK is deployed either on no web container or on a third-party web container such as BEA WebLogic Server or IBM WebSphere Application Server.

Workaround

Create a certificate database on the SDK-only machine and install the root CA certificate for the Access Manager server into this database:

1. Log into the SDK-only machine as superuser (`root`).

2. Verify that the required Netscape Security Services (NSS) package is installed:

   - On Solaris systems: SUNWtlsu
   - On Linux systems: sun-nss RPM

3. If the package is not installed, install it. For example:

   On Solaris systems:

   ```
   cd JavaEnterpriseSystem_base/Solaris_arch/Product/shared_components/Packages
   pkgadd -d . SUNWtlsu
   ```

   On Linux systems:

   ```
   cd JavaEnterpriseSystem_base/Linux_x86/Product/shared_components/Packages
   rpm -Uvh sun-nss-3.3.10-1.i386.rpm
   ```

4. Create the password file for the token password for that certificate database. For example:

   On Solaris systems:

   ```
   echo "cert-database-password" > /etc/opt/SUNWam/config/.wtpass
   chmod 700 /etc/opt/SUNWam/config/.wtpass
   ```

On Linux systems:

```
echo "cert-database-password" > /etc/opt/sun/identity/config/.wtpass
chmod 700 /etc/opt/sun/identity/config/.wtpass
```

where *cert-database-password* is the token password.

5. Check the LD_LIBRARY_PATH variable:

   On Solaris systems, check LD_LIBRARY_PATH to see if the `/usr/lib`, `/usr/lib/mps/secv1`, and `/usr/lib/mps` directories are present. If not add any missing directories.

   On Linux systems, check LD_LIBRARY_PATH to see if the `/opt/sun/private/lib` directory is present. If not add the directory.

6. Use the Certificate Database Tool (`certutil`) to create the certificate and key databases. For information about `certutil`, refer to the following Web site:

   `http://mozilla.org/projects/security/pki/nss/tools/certutil.html`

   For example:

   ```
   certutil-home/certutil -N -d cert-database-dir -f config-home/.wtpass
   ```

   where:

   certutil-home is the location of `certutil`:

   - On Solaris systems: `/usr/sfw/bin`
   - On Linux systems: `/opt/sun/private/bin`

   cert-database-dir is the database directory for the certificate and key databases.

   config-home is the location of the Access Manager configuration files:

   - On Solaris systems: `/etc/opt/SUNWam/config`
   - On Linux systems: `/etc/opt/sun/identity/config`

7. In the newly created certificate database, add the root CA certificate for the SSL certificate that is installed on the Access Manager server. For example:

   ```
   certutil-home/certutil -A -n "certificate-nickname" -t "TCu,TCu,TCuw" -d
   cert-database-dir -a -i path-to-file-containing-cert -f config-home/.wtpass
   ```

8. Use an editor to view the `AMConfig.properties` file and verify that the following values

   - Certificate database directory: `com.iplanet.am.admin.cli.certdb.dir`
   - Prefix: `com.iplanet.am.admin.cli.certdb.prefix`

- Password file: `com.iplanet.am.admin.cli.certdb.passfile`

  If not, edit the settings as needed. For example, the prefix setting should be empty (that is, equal to “”).

9. If changes were made to the `AMConfig.properties` and the Access Manager SDK is deployed into a web container, restart the web container.

SSL Handshake Fails With DNSAlias with JCE Provider (#5038876)

SSL handshaking fails when certificates with valid `DNSAlias` names in the `subjectaltname` are used with a JCE provider.

Identity Methods in Init() of Filters Cause Weblogic to Crash (#5016283)

A WebLogic server will not start when the `init()` methods of filters have Access Manager-related code. The Access Manager API is called in the `init` method of the ServletFilter servlet.

Access Manager uses JSS as the security provider, but WebLogic uses JCE by default. When the `init` method is invoked, WebLogic attempts to validate its license using the JCE, but JSS is getting initialized.

Workaround

Change the default security encryption from `JSSEncryption` to `JCEEncryption` in the `AMConfig.properties` file.

Any Password That Starts with “{SSHA}” Symbols is Unusable (#4966191)

Access Manager does not support the use of hashed {SSHA}symbols in passwords.

Group Create Option Adds Only One memberURL Attribute (#4931958)

If you create a group with the multiple LDAP-filter option (`-f`), the group is incorrectly created with only one `memberURL` attribute.

Tuning

amtune And Associated Files Are Not Delivered For Solaris-x86 (#6213019)

In this release, the `amtune` script, and its associated files, are not installed into the appropriate directory for Solaris-x86.

Workaround

Use `amtune` files delivered for Sparc-Solaris.

amtune-as8 Script Contains Error For Password File (#6212380)

Automated tuning for Application Server 8 (`amtune-as8`) with the amtune script does not work, because a temporary password file is created with the `asadmin` password. Currently only the password is put in the file.

Workaround

In `amtune-as8`, use the following syntax to enter the string:

```
"TOKEN=Value"
```

For example:

```
"AS_ADMIN_PASSWORD=11111111"
```

Enter this change `amtune-env:`

```
#ASADMIN=$CONTAINER_BASE_DIR/bin/asadmin
ASADMIN=/opt/SUNWappserver/appserver/bin/asadmin
```

Single Sign-On

Unable To Perform SSO With Different Deploy URIs (#4770271)

If the deployment URIs are different between two different instances of Access Manager, Single Sign-on will not function properly.

Internationalization (i18n)

Group Members Are Not Listed When Group Name is Multibyte (#6197041)

In the internationalized version of Access Manager 6 2005Q1, groups members are not listed in the Access Manager console when the group name is multibyte.

The Start and Stop Messages Are Unreadable on Linux (#6207421)

The Access Manager Start and Stop messages for the zh / zh_TW character set are unreadable. This occurs on the Linux platform.

Cannot Login with HTTPBasic and WindowsDesktopSSO in Non-English Locale (#6209324)

You cannot login to the HTTPBasic and WindowsDesktopSSO authentication modules in a non-English locale.

Workaround

Revert these parameters to English in XML files:

```
HTTPBasic.xml: <HttpHeader>Authorization</HttpHeader>
```

```
WindowsDesktopSSO.xml: HttpHeader>Authorization</HttpHeader>
```

These files are usually installed into the following directory when Access manager is deployed into Application Server:

```
/var/opt/sun/appserver/domains/domain1/applications/j2ee-modules/amserver/config/auth/defa
ult_<lang>
```

These files are usually installed into the following directory when Access manager is deployed into Web Server:

```
/opt/sun/webserver/https-<host>/is-web-apps/services/config/auth/default_<lang>
```

Japanese Online Help Incorrectly Displayed (#5024138)

If you are running the Japanese version of Access Manager and change the language to en_US, the Japanese help context will still display.

Workaround

Create a sym link from `docs_en` to `docs_en_US`.

Client Detection function not working properly (#5028779)

In the Client Detection service, removing UTF-8 is not working properly.

Workaround

If you remove the UTF-8 character set, restart the web container after you have made the change.

G11NSetting Does Not Handle a Space in Q Factor (#5008860)

When the client data has a space in or around `q` factor, the G11NSettings code fails to parse it correctly and returns the following error:

```
ERROR: G11NSettings::Fetchcharset() Unable toparse  charset entry invalid Q  q
```

Login Page Fails With Multi-byte Role Parameter On URL for ja Character Set (#4905708)

If you create a multi-byte role and then try a URL login with a user registered to the multi-byte role, the login page will produce a failure error.

Workaround

In order for the authentication framework to decode a multi-byte role value specified in the URL, you need to specify gx_charset along with the parameter. For example:

```
http://hostname:port/amserver/UI/Login?role=manager?role=%E3%81%82%&gx_charset=utf-8
```

Logfiles are Garbled in Ja Locale (#4882286)

The following log file contains Japanese characters and are garbled when opened:

All the files in the /var/opt/SUNWam/debug directory except deploy.log and undeploy.log.

Locale Parameter In URL Displays Mixed Login Page (#4915137)

If you are using a non-English based browser with an instance of Access Manager installed with Web Server and login to http://*host*:*port*/amserver/UI/Login?locale=en, the login page will display with a mix of English and non-English characters.

Workaround

Change the following symbolic link:

```
AccessManager-base/SUNWam/web-apps/services/config/auth/default
```

to

```
AccessManager-base/SUNWam/web-apps/services/config/auth/default_en
```

Mixed Locale In Login Window When Application Server Is ja (#4932089)

The Access Manager login window will not default back to English when the browser language setting is en and Application Server's locale is set to ja.

Workaround

Run the Application Server with locale set to en.

Lockout Notification Sends Unreadable Email (#4938511)

If you run Access Manager with web container that has the preferred locale set to anything other than C and a user is locked out of the server, lockout notification email will be sent, but it will be unreadable.

Workaround

Set email|local|charset (instead of only the email parameter) in the Email Address to Send Lockout Notification attribute. For example:

```
user1@example.com|zh|GB2312
```

Multi-byte Names Do Not Work in Self Registration (#4732470)

If you create a user in the Self Registration (Membership Authentication service) module with a duplicated user ID and a multi-byte First Name and Last Name, an error will occur. Multi-byte user IDs are not supported.

Workaround

If a user logs in using Self Registration in a multi-byte environment, the administrator must make sure that the User Generator Mode attribute in the Core Authentication is not selected.

or

The user can select the Create My Own option in the Self-Registration login page.

Japanese Version Of Access Manager Does Not Work With Netscape 6.22, 6.23 (#4902421)

In the Japanese version of Access Manager, you can not log into the console with Netscape 6.22 or 6.23.

Time Condition Format Does Not Change (#4888416)

In Time Conditions for policy definitions, the time display does not change from the following format, regardless of locale:

```
Hour:Minute AM/PM
```

Client Detection Screen Not Localized (#4922013)

Portions of the Current Style Properties screen of the Client Detection interface were not localized in this release.

Updated genericHTML Client Property Does Not Get Applied (#4922348)

If you remove UTF-8 from the character set list in the Client Detection service's genericHTML client property, save the changes and then enable Client Detection, and then logout and login again, the login page is still in UTF-8 character set.

Workaround

Restart the server manually with `amserver`.

Log File Headers Not Localized (#4923536)

The first two lines of all log files are not localized, in particular the `Version` and `Fields` sections and their lists of fields.

Data Field Values Are Not Localized In amSSO.access (#4923549)

In the `amSSO.access` log file, all the values under the `Data` field are not localized.

Exception.jsp Has Hard-Coded Messages (#4772313)

`Exception.jsp` is not localized and contains hard-coded title, error messages and copyright information. This exceptional error jsp page is invoked only in extreme cases. Examples are when Directory Server is down, or when no Access Manager services can be brought up and no localization is available for this jsp page.

Cookies

Cookieless Mode is Not Working (#4967866)

If a browser that supports cookies accesses Access Manager and the cookie support is turned off, the browser will then continue to send the older Access Manager cookie. This problem causes access to Access Manager resources to be denied.

Workaround

Choose one of the following workarounds:

- Clear the browser cookie cache to remove all Access Manager cookies.
- Disable cookies in the browser.

Cookie Hijacking

The following information has been incorporated into the English version of the *Sun Java System Access Manager Administration Guide*.

Security may be compromised when applications using the session cookies cannot be trusted.

When single sign-on (SSO) or cross domain single sign-on (CDSSO) is enabled in your Access Manager deployment, `http(s)` session cookies are set on the user's browser. These cookies are validated across multiple applications. When the Access Manager is deploy across multiple DNS domains, the Liberty protocol transfers the `http(s)` session cookies from the authenticated DNS domain to web application's target domain.

Although the user is automatically signed on to web resources, there is a known security weakness when applications using the session cookies cannot be trusted. The weakness may be present when an Identity Provider provides authentication, authorization and profile information about a user to applications (or Service Providers) that are developed by third parties or by unauthorized groups within the enterprise. Possible security issues are:

- All applications share the same `http` session cookie. This makes it possible for a rogue application to hijack the session cookie and impersonate the user to another application.

- If the application does not use the `https` protocol, the session cookie is prone to network eavesdropping.
- If just one application can be hacked, the security of the entire infrastructure is in jeopardy of being compromised.
- A rouge application can use the session cookie to obtain and possibly modify the profile attributes of a user. If the user has administrative privileges, the application would be able to do a lot more damage.

Workaround

Follow these steps:

1. Use the Access Manager administration console to make an entry for each agent.

   a. In the organization that contains the agent to be created, choose Agents from the View menu, and then click New.

   b. Provide the following information:

      Name. Enter the name or identity of the agent. Example: `agent123`

      Password. Enter the agent password. Example: `agent123`

      Confirm Password. Confirm the password.

      Description. Enter a brief description of the agent. For example, you can enter the agent instance name or the name of the application it is protecting.

      Agent Key Value. Set the agent properties with a key/value pair. This property is used by Access Manager to receive agent requests for credential assertions about users.

      Enter a property value for `agentRootURL` with value equal to the agent URL with port number. Note that the `agentRootURL` value is case sensitive.

      Example: `agentRootURL=http://`*server_name:99*`/`

      Device Status. Enter the device status of the agent. If set to Active, the agent will be able to authenticate to and communicate with Access Manager. If set to Inactive, the agent will not be able to authenticate to Access Manager.

   c. Click OK.

2. Run the following command on the password that was entered in step 1b.

   AccessManager-base`/SUNWam/agents/bin/crypt_util agent123`

   This will give the following output:

   ```
   WnmKUCg/y3l404ivWY6HPQ==
   ```

3. Change `AMAgent.properties` to reflect the new value, and then and restart the agent. Example:

```
# The username and password to use for the Application authentication module.


com.sun.am.policy.am.username = agent123
com.sun.am.policy.am.password = WnmKUCg/y3l404ivWY6HPQ==


# Cross-Domain Single Sign On URL
# Is CDSSO enabled.
com.sun.am.policy.agents.cdsso-enabled=true


# This is the URL the user will be redirected to after successful login
# in a CDSSO Scenario.
com.sun.am.policy.agents.cdcservletURL =
http://server.example.com:port/amserver/cdcservlet
```

4. Change `AMConfig.properties` to reflect the new values, and then and restart Access Manager. Example:

```
com.sun.identity.enableUniqueSSOTokenCookie=true
com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer


com.sun.identity.authentication.uniqueCookieDomain=example.com
```

5. In the Access Manager administration console, choose Service Configuration>Platform.

6. In the Cookie Domains list, change the cookie domain name:

   a. Select the default `iplanet.com` domain, and then click Remove.

b. Enter the host name of the Access Manager installation, and then click Add.

Example: server.`example.com`

You should see two cookies set on the browser:

Cookie	Host Name
`iPlanetDirectoryPro`	`server.example.com`
`sunIdentityServerAuthNServer`	`example.com`

Documentation Updates and Errata

The English version of the *Sun Java System Access Manager Administration Guide* has been revised as follows:

- The procedures in Chapter 3, "Configuring Access Manager in SSL Mode" have been revised. Specifically, new procedures for setting up Application Server 8.1 with Access Manager have been added.
- The reference to the high availability database (HADB) has been removed from Chapter 42, "Session Service Attributes."
- The following information has been incorporated as Chapter 3, "Installing and Configuring Third-Party Web Containers."

Installing and Configuring Third-Party Web Containers

This section describes the procedures for installing and configuring third-party web containers deployed with Sun Java™ System Access Manager. For this release, Access Manager supports BEA WebLogic 8.1 (and its current patches) and IBM WebSphere 5.1 (and its current patches).

WebLogic and WebSphere are not part of the Java Enterprise System, so you must install and configure them independently of the Java ES Install program. In general the procedures are:

1. Install, configure, and start the web container instance.
2. Install the Directory Server from the Java ES installer.
3. Install Access Manger from the Java ES Installer in Configure Later Mode, which will leave Access Manager in an unconfigured state.

4. Run the Access Manager configuration scripts to deploy Access Manager in the web container.

5. Restart the web container.

Installing and Configuring BEA WebLogic 8.1

Before you install WebLogic, make sure that your host domain is registered in DNS and verify that you are installing the correct version of the WebLogic software. For more information, go to the BEA product site at `http://commerce.bea.com/index.js`p.

To Install and Configure WebLogic 8.1

1. Unpack the downloaded software image, either in `.zip` or `.gz` format. Make sure that the zip/gzip utility you are using is for the correct platform, or you may receive a checksum error during the unpackaging.

2. Run the installation program from a shell window of your target system.

   Follow the procedures provided by the WebLogic installation utility (detailed installation instructions can be found at `http://e-docs.bea.com/wls/docs81`/).

   During the installation process, make sure that you record the following information, as it will be used later in the Access Manager configuration:

   - FQDN (used in the `WL8_HOST` parameter)
   - installation location
   - port number

3. Once installation is complete, run the WebLogic configuration tool to configure the domain and server instance from the following location:

   WebLogic-base/*WebLogic-instance*/`common/bin/quickstart.sh`

   By default, WebLogic defines the server instance as `myserver` and the domain as `mydomain`, however it is unlikely that you will choose to use these defaults. If you create a new domain and instance, make sure that you record the information for Access Manager configuration and deployment. See the WebLogic 8.1 documentation for instructions.

4. If you are installing on an administration instance, start WebLogic by using the `startWebLogic.sh` utility from the following location:

   WebLogic-base/*WebLogic-Userhome*/`domains`/*WebLogic-domain*/`startWebLogic.sh`

   If you are installing on a managed instance, start WebLogic by using the following command:

   WebLogic-base/*WebLogic-Userhome*/`domains`/*WebLogic-domain*/`startManagedWebLogic` *WebLogic-managed-instancename admin-url*

Installing and Configuring IBM WebSphere 5.1

Before you install WebSphere, make sure that your host domain is registered in DNS and verify that you are installing the correct version of the WebSphere software for your platform. For more information, go to the IBM product support website at `http://www-306.ibm.com/software/websphere/support/`.

To Install and Configure WebSphere 5.1

5. Unpack the downloaded software image, either in `.zip` or `.gz` format. Make sure that the zip/gzip utility you are using is for the correct platform, or you may receive a checksum error during the unpackaging.

6. Run the installation program from a shell window of your target system. If you are planning on installing a patch, install the 5.1 version first and apply the patch later (see Step 9). Detailed installation instructions can be found at `http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp`.

   During the installation process, make sure that you record the following information, as it will be used later in the Access Manager configuration:

   - hostname
   - domain name
   - cell name
   - node name
   - port number
   - installation directory
   - WebSphere instance name

- administration port

  By default, WebSphere defines the server instance as `server1`, however it is unlikely that you will choose to use the default. If you create a new instance, make sure that you record the information for Access Manager configuration and deployment. See the WebSphere 5.1 documentation for instructions.

7. Verify that the installation was successful. To do so:

   a. Make sure the `server.xml` file exists in the following directory:

   `/opt/WebSphere/AppServer/config/cells/cell-name/noes/node-name/servers/`*server1*

   b. Use the `startServer.sh` command to start the server. For example:

   `/opt/WebSphere/AppServer/bin/startServer.sh` *server1*

   c. In a web browser, enter the corresponding URL of the following format to view the sample web application:

   `http://`*fqdn:portnumber/snoop*

8. Once you have verified a successful installation, stop the server using the `stopServer.sh` utility. For example:

   `opt/WebSphere/AppServer/bin/stopServer.sh` *server1*

9. If you are installing WebSphere 5.1 patch, use the `updateWizard.sh` command line utility to install the patch over the original 5.1 instance.

10. Restart WebSphere and verify that the installation was successful (see Step 7).

Using Java ES to Install Directory Server and Access Manager

Access Manager installation involves two separate invocations of the Java Enterprise System (Java ES) Installer.

1. Run the first Java ES invocation to install Directory Server (either local or remote) with the Configure Now option. The Configure Now option allows you to configure the first instance during the installation by the choices (or default values) that you select.

2. Run the second Java ES invocation to install Access Manager with the Configure Later option. This option Installs the Access Manager 2005Q1 components, and then after installation, you must configure them.

   WebLogic and WebSphere are installed independently of Java ES, so the Installer does not contain the necessary configuration data to automatically deploy the containers. Because of this, you must select the Configure Later option when installing Access Manager. This option leaves your Access Manager deployment in the following state:

- The active Directory Server (either Local or Remote) does not have Access Manager DIT data loaded.
- Access Manager configuration files are not automatically loaded.
- Access Manager web application `.war` files are not generated.
- Access Manager deployment and post-installation configuration processes are not automatically started and run.

For detailed installation instructions, refer to the *Sun Java Enterprise System Installation Guide* located at `http://docs.sun.com/doc/819-0056`.

Configuring Access Manager

After you have completed Access Manager installation on the target system's local drive, you need to manually configure Access Manager with either WebLogic 8.1 or WebSphere 5.1. This is a three-step process:

1. Edit the configuration script input file
2. Run the configuration script
3. Restart the web container

Creating the Configuration Script Input File

The Access Manager configuration script input file contains all of the deployment level, Access Manager, web container, and Directory Server variable definitions. Access Manager contains a sample configuration script input file template (`amsamplesilent`), which is available in the *AccessManager-base*`/SUNWam/bin` directory on Solaris systems or the *AccessManager-base*`/identity/bin` directory on Linux systems.

You can use the `amsamplesilent` template to construct your configuration script input file. Instructions for editing the file, as well as the variable definitions, are described in "Access Manager Sample Configuration Script Input File" in Chapter 1 of the *Access Manager Administration Guide*.

Before you edit the file, make sure that you have the following information available from your web container installation:

BEA WebLogic and IBM WebSphere

- installation location
- instance name and location
- hostname
- FQDN

- port number to which it is listening
- administration ID
- protocol used

BEA WebLogic only

- administration password
- shared library location
- domain name and location
- project directory name
- JDK location

IBM WebSphere only

- cell name
- node name
- JDK location

Running the Configuration Script

When you have saved the configuration script input file, you run the `AMConfig` script to complete the configuration process. For example:

```
AccessManager-base/SUMWam/bin/amconfig -s silentfile
```

`silentfile` should be the absolute path to the configuration input file.

Running this script performs the following functions:

1. Loads the Access Manager schema to the active Directory Server instance.
2. Loads the Access Manager service data to the Directory Server instance.
3. Generates the Access Manager configuration files used by the active Access Manager instance.
4. Deploys the Access Manager web application data to the web container.
5. Customizes the web container configuration to match the Access Manager requirements.

The procedures for running the `amconfig` script are described in the *Access Manager Administration Guide*.

Restarting the Web Container

After you have completed the configuration process, you must restart the web container. Refer to your product's documentation for instructions.

For BEA WebLogic 8.1, see `http://e-docs.bea.com/wls/docs81`.

For IBM WebSphere 5.1, see `http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp.`

Redistributable Files

Sun Java System Access Manager 6 2005Q1 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 Sun Java System Access Manager, contact Sun customer support using one of the following mechanisms:

- Sun Software Support services online at
  `http://www.sun.com/supportraining`

  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

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. Use the web-based form to provide feedback to Sun:

http://www.sun.com/hwdocs/feedback/

Please provide the full document title and part number in the appropriate fields. 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 part number of these Release Notes is 817-7642-12.

Additional Sun Resources

Useful Sun Java System information can be found at the following Internet locations:

- Sun Java System Documentation
  http://docs.sun.com/prod/entsys.05q1
- Sun Java System Professional Services
  http://www.sun.com/service/products/software/javaenterprisesystem/
- Sun Java System Software Products and Service
  http://wwws.sun.com/software/
- Sun Java System Software Support Services
  http://www.sun.com/supportraining
- Sun Java System Support and Knowledge Base
  http://sunsolve.sun.com
- Sun Java System Consulting and Professional Services
  http://www.sun.com/service/products/software/javaenterprisesystem
- Sun Java System Developer Information
  http://developers.sun.com/
- Sun Developer Support Services
  http://www.sun.com/developers/support