Sun Java System Access Manager 7.1 Release Notes

Part No: 819–4683–24
October 2010

ORACLE

101018@24999

Contents

Sun Java System
Access Manager 7.1 Release Notes

October 2010

Part Number 819-4683-24

The Sun Java System Access Manager 7.1 Release Notes contain important information available for the Sun Java Enterprise System (Java ES) release, including new Access Manager features and known issues with workarounds, if available. Read this document before you install and use this release.

To view the Java ES product documentation, including the Access Manager collection, see `http://docs.sun.com/prod/entsys.5`.

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

Revision History

The following table shows the Access Manager 7.1 Release Notes revision history.

TABLE 1 Revision History

Date	Description of Changes
July 2006	Beta release.
March 2007	Java Enterprise System 5 release.
May 2007	Updated with new Known Issues 6555040, 6550261, 6554379, 6554372, 6480354.
June 2007	Updated with new Known Issues 6562076, 6490150.
July 2007	Updated with new Known Issue 6485695.
January 2008	Added information about "Access Manager 7.1 Patch 1" on page 22.
February 2008	Updated with new information for the "Documentation Updates" on page 75 section; Missing information when configuring Access Manager in SSL mode and Access Manager supports non-ASCII character passwords if Directory Server is configured to support them.
December 2008	Added information about "Access Manager 7.1 Patch 2" on page 18.
January 2009	Added support for Red Hat Enterprise Linux 5.0 Server.
June 2009	Added information about "Access Manager 7.1 Patch 3" on page 13.
July 2009	Added "Account Locking feature fails to send email notification when the user's account is locked (6760137)" on page 57 and revised the workaround for "Password Reset service reports notification errors when a password is changed (6455079)" on page 57.
August 2009	Updated the Directory Server supported versions in Table 2 and added "Required Services not supported in Access Manager 7.1 Console in Realm Mode (6615838)" on page 53.
April 2010	Added the "Access Manager 7.1 Patch 4" on page 10 and "Support for the Java SecurID Authentication Module" on page 75 sections.
October 2010	Added the "Access Manager 7.1 Patch 5" on page 8 section.

About Sun Java System Access Manager 7.1

Sun Java System Access Manager is part of the Sun Identity Management infrastructure that allows an organization to manage secure access to Web applications and other resources both within an enterprise and across business-to-business (B2B) value chains.

Access Manager provides these main functions:

- Centralized authentication and authorization services using both role-based and rule-based access control
- Single sign-on (SSO) for access to an organization's Web-based applications
- Federated identity support with the Liberty Alliance Project and Security Assertions Markup Language (SAML)
- Logging of critical information including administrator and user activities by Access Manager components for subsequent analysis, reporting, and auditing.

Access Manager 7.1 Patch Releases

The latest revisions of the Access Manager 7.1 patches are available for download from SunSolve Online: `http://sunsolve.sun.com`. The most recent patch IDs are:

- Solaris SPARC systems: 126356-05
- Solaris x86 systems: 126357-05
- Linux: 126358-05
- Windows: 126359-05
- WAR file deployments (all platforms): 140504-05

Note – Access Manager 7.1 patches are cumulative. You can install the latest patch without first installing an earlier patch. However, if you did not install an earlier patch, review the new features and issues in the earlier patch sections to determine if any of the features and issues apply to your deployment.

Information about Access Manager 7.1 patches includes:

- "Access Manager 7.1 Patch 1 Single WAR Deployment" on page 36

Sun Alerts. Occasionally, Sun releases Alerts for Access Manager 7.1. Consider periodically checking SunSolve (`http://sunsolve.sun.com/`) to determine if there are any Sun Alerts that affect your deployment.

Sun Java System LDAP JDK Patches

Sun provides the following LDAP JDK patches for security and performance related fixes:

- Solaris SPARC and x86 systems: 119725
- Linux: 120834
- Windows (and platforms other than Solaris and Linux systems): 138905

Check SunSolve (`http://sunsolve.sun.com/`) for the latest version of these patches. For more information, see Sun Alert `http://sunsolve.sun.com/search/document.do?assetkey=1-26-242246-1`.

Note – For most deployments, Sun recommends that you apply the latest version of these patches. However, in the following situations, these patches are required:

- Your current LDAP JDK is version 4.21 or earlier.
- Access Manager 7.1 is deployed on WebLogic Server. The `weblogic.jar` file bundles an older `ldapjdk.jar`. For more information, see "Access Manager 7.1 on WebLogic Server requires new `ldapjdk.jar` File (6774634)" on page 18.

Access Manager 7.1 Patch 5

Access Manager 7.1 patch 5 fixes a number of problems, as listed in the README file included with the patch. For a list of the patch IDs, see "Access Manager 7.1 Patch Releases" on page 7. Patch 5 also includes the following new features and changes:

- "Time to Live (TTL) is implemented for the Service Management (SMS) cache (6973683)" on page 9
- "Retry mechanism is implemented in the PLL server (6963531)" on page 9
- "Access Manager 7.1 patch Readme lists the required LDAP JDK patches (6959325)" on page 9
- "HttpServletRequest and HttpServletResponse are available with Distributed Authentication User Interface (6677966)" on page 9

Time to Live (TTL) is implemented for the Service Management (SMS) cache (6973683)

Patch 5 includes the following new properties to implement the TTL for the SMS cache. The TTL is the period of time before data in the SMS cache is discarded.

- `com.sun.identity.sm.cache.ttl.enable` enables the TTL function for the SMS cache, if set to `true`.
- `com.sun.identity.sm.cache.ttl` specifies the time in minutes before data in the cache is discarded. The default is 30 minutes.

To use these new properties, add them with appropriate values to the `AMConfig.properties` file and then restart the Access Manager web container.

Retry mechanism is implemented in the PLL server (6963531)

Patch 5 includes the following new properties to implement the retry mechanism in the PLL server:

- `com.sun.identity.notification.retry.limit` enables the Access Manager 7.1 server to repeat sending notifications until the notification is delivered successfully. The default is 3 retries, if the value is set to any nonnumeric character. A value of 0 (zero) specifies that no retries are sent.
- `com.sun.identity.notification.retry.interval` species the time interval in milliseconds between re-sending the retries, if `com.sun.identity.notification.retry.limit` is set to a nonnumeric character (or not set). The default is 500 milliseconds.

To use these new properties, add them with appropriate values to the `AMConfig.properties` file and then restart the Access Manager web container.

Access Manager 7.1 patch Readme lists the required LDAP JDK patches (6959325)

The Access Manager 7.1 Readme file included with the patch now lists the required LDAP JDK patches. For more information, see the patch 5 Readme file.

HttpServletRequest and HttpServletResponse are available with Distributed Authentication User Interface (6677966)

Patch 5 allows you to access the `HttpServletRequest` object and modify the `HttpServletResponse` object through a custom authentication module for Access Manager 7.1 server deployments with the Distributed Authentication User Interface (DAUI), as well as for Access Manager 7.1 server deployments without the DAUI.

To use this new feature, you must modify your existing custom authentication modules using the authentication SPI framework. (If you don't want to use this feature, your existing custom authentication modules do not need to be modified. The current APIs for `getHttpServletRequest` and `getHttpServletResponse` will continue to be supported but only for Access Manager 7.1 server deployments without the DAUI.)

Changes to custom authentication modules include both JAVA class files and callback XML files. No UI changes are required. Patch 5 adds these new callbacks:

- `HttpRequestCallback`: equivalent to the container `HttpServletRequest` object
- `HttpResponseCallback`: equivalent to the container `HttpServletResponse` object

For more information, see the *Sun Java System Access Manager 7.1 Developer's Guide*.

Access Manager 7.1 Patch 4

Access Manager 7.1 patch 4 fixes a number of problems, as listed in the README file included with the patch. Patch 4 also includes the following changes and known issues:

New Features and Changes in Access Manager 7.1 Patch 4

New property prevents "Too many authentication attempts" error (6883136)

If you open multiple browser tabs in the same browser instance to access the Access Manager login page, the new `com.sun.identity.authentication.mutiple.tabs.used` property prevents the "Too many authentication attempts" error.

To use this new property, add it with a value of `true` to the `AMConfig.properties` file and restart the Access Manager web container.

New property sets idle time out for policy agent sessions (6697260)

The new `com.iplanet.am.session.agentsessionidletime` property sets the maximum idle timeout in minutes for policy agent sessions. The default value is 0, which causes policy agent sessions to never time out. The minimum value is 30 minutes. A value between 0 and 30 minutes will be reset to 30.

To use this new property, add it with a value appropriate for your deployment to the `AMConfig.properties` file and restart the Access Manager web container.

Access Manager session cookies can be marked as HTTPOnly (6843487)

The new `com.sun.identity.cookie.httponly` property allows Access Manager session cookies to be marked as `HTTPOnly`, in order to prevent scripts or third-party programs from accessing the cookies. Specifically, session cookies marked as `HTTPOnly` can help to prevent cross-site scripting (XSS) attacks.

By default, the value for `com.sun.identity.cookie.httponly` is `false`. To use this new property, add it with a value of `true` to the `AMConfig.properties` file and restart the Access Manager web container

You must also set this property on the client side. For example, for a Distributed Authentication UI server deployment, set it to `true` in the `AMDistAuthConfig.properties` file.

ampassword utility has new options to hash and encrypt a password (6850818)

In patch 4, the `ampassword` utility has the following new options:

```
ampassword -s | --hash [ password ]
ampassword -c | --hashencrypt [ password ]
```

where:

`-s` or `--hash` hashes the password.

`-c` or `--hashencrypt` both hashes and encrypts the password.

Windows Desktop SSO authentication is added for Distributed Authentication UI Server deployment (6888820)

Support for Windows Desktop SSO authentication is added for a Distributed Authentication UI server deployment and the Access Manager 7.0 and later Client SDK. This CR was verified for the following Access Manager 7.1 deployment scenarios:

- Access Manager 7.1 server with a version 7.1 Distributed Authentication UI server deployment from a browser (both Internet Explorer and Firefox)
- Access Manager 7.1 server with a version 7.1 Distributed Authentication UI server deployment with the Access Manager 7.0 and later Client SDK on Windows XP and Windows 2003

CDC Servlet inserts custom HTTP response header (6800246)

In patch 4, if you integrate Cross-Domain Single Sign-On (CDSSO) with programmatic clients, the CDC Servlet inserts an extra HTTP response header (which is not configurable). For example, with a web agent installed in CDSSO mode, viewing a response on "Live HTTP Headers", you will see the `Cdcservlet_auto_post: true` header. This change allows custom applications to easily distinguish the auto submitting form and to process the information accordingly.

Changes to the updateschema.sh script (6870576)

Patch 4 includes the following changes to the `updateschema.sh` script:

- Removes the restriction of requiring the user to be superuser (`root`) to execute the script.
- Allows the user to specify whether Directory Server has SSL enabled.
- Validates the path of the `ldapsearch` and `ldapmodify` commands and prompts the user to specify the path if they are incorrect.
- Corrects the path to the `amadmin` utility in an Access Manger 7.1 single WAR file deployment.

Known Issues in Access Manager 7.1 Patch 4

- "`updateschema.pl` script fails with older version of `ldapjdk.jar` (6934848)" on page 12
- "`updateschema` script cannot run successfully under certain circumstances in WAR file deployment (6934844)" on page 12

updateschema.pl script fails with older version of ldapjdk.jar (6934848)

On Windows, the `updateschema.pl` script in Access Manager 7.1 patch 3 and later requires the version 4.21 or later `ldapjdk.jar` file. In some old `ldapjdk.jar` files, the version is not even defined in the `META-INF/MANIFEST.MF` file. If the LDAP JDK version is older than 4.21 or not defined, the `updateschema.pl` script exits with an error.

Workaround. Download and install the latest LDAP JDK patch, as described in "Sun Java System LDAP JDK Patches" on page 8.

updateschema script cannot run successfully under certain circumstances in WAR file deployment (6934844)

If Access Manager 7.1 patch 4 is deployed from a WAR file, the `updateschema` script cannot run successfully for the following reasons:

- On Solaris systems, the `-B` option is not available for the version of the `ldapsearch` utility that is called by the `updateschema.sh` script.
- On Linux systems, the `-Z` option is not available for the version of the `ldapsearch` utility that is called by the `updateschema.sh` script.

- On Windows, if you are running the `updateschema.pl` script, you cannot specify that the Directory Server is SSL enabled.

Workarounds

- On Solaris or Linux systems, edit the `updateschema.sh` script and change the path for the `ldapsearch` utility to point to a version that supports the `-B` and `-Z` options. You might need to download a version of `ldapsearch` that supports these options. Then, rerun the `updateschema.sh` script.
- On Windows, enable non-SSL access to Directory Server and rerun the `updateschema.pl` script.

Access Manager 7.1 Patch 3

Access Manager 7.1 patch 3 fixes a number of problems, as listed in the README file included with the patch. Patch 3 also includes changes and known issues:

New Features and Changes in Access Manager 7.1 Patch 3

Sun Java System LDAP JDK Patches are Available

Check the "Sun Java System LDAP JDK Patches" on page 8 section to determine if you need to apply these patches.

Running the updateschema Script is Required

Beginning with patch 3 (and any subsequent patches unless specifically noted), you must run the `updateschema.sh` script on Solaris and Linux systems or the `updateschema.pl` script on Windows. The `updateschema` script updates the Sun Java System Directory Server schema with any new attributes required by the patch.

Requirements for the `updateschema.sh` or `updateschema.pl` script include:

- The `updateschema.sh` or `updateschema.pl` script requires JDK 1.5 or later. Therefore, set your `JAVA_HOME` environment variable to a JDK installation of 1.5 or later.
- On Windows systems, the `updateschema.pl` script requires AcivePerl 5.8 or later.

Access Manager 7.1 WAR File Deployment

To locate the `updateschema` script:

1. After you unzip the `140504-05.zip` file, unzip the `AccessManager7_1Patch4.zip` file.
2. In the `140504-05/patch` directory, unzip the `AM7_1Patch4.zip` file.

   The `updateschema.sh` and `updateschema.bat` scripts are in the `140504-05/patch/bin` directory.

For an Access Manager 7.1 WAR file deployment, run the `updateschema` script after you add the patch. The script prompts you for paths to the following items:

- Access Manager 7.1 WAR file deployment directories (which must already exist):
  - Staging directory
  - Configuration directory
  - Tools directory
- Sun Java System Directory Server information:
  - Fully-qualified hostname. For example: `ds.example.com`
  - Port number, Default is 389.
  - Directory Manager DN and password. Default is `cn=Directory Manager`.
  - Top-level administrator and password. For example: `uid=amadmin,ou=People,dc=example,dc=com`

Access Manager 7.1 Installer (Package-Based) Deployment

After you unzip the *patchID*`.zip` file, the `updateschema.sh` or `updateschema.bat` script is in the *patchID* directory, where *patchID* is 126356-05, 126357-05, 126358-05, or 126359-05, depending on your platform.

For an Access Manager 7.1 installer (package-based) deployment, run the `updateschema` script after you add the patch. The script prompts you for the same Directory Server information as requested for a WAR file deployment.

Limitation is Removed for Creation of Data Store Authentication Module Instance in Legacy Mode

Patch 3 removes the limitation for "Creation of Data Store authentication module instance fails in Legacy mode (6764919)" on page 19.

In patch 2, the amadmin user was prevented from logging in to any authentication module other than the Data Store and Application authentication modules. CR 6811036 in patch 3 removes this restriction, but at the same time re-implements the original security fix to protect the authentication for the amadmin user, which is considered as a special or "internal" user.

An internal user such as amadmin must first authenticate internally to the OpenSSO configuration data store before it can authenticate to any authentication module. Hence you can login as amadmin to any authentication module only if you can first successfully authenticate to the configuration data store.

Note. Due to CR 6811036, if you log in as amadmin to the Access Manager Admin Console and provide an incorrect password, the "Your authentication module is denied' message will be displayed instead of "Authentication Failed" (which was displayed prior to patch 2).

Backward Compatibility Issue Between Access Manager 7.1 and amclientsdk.jar is Fixed

Patch 3 fixes the "Backward compatibility issue between Access Manager 7.1 and amclientsdk.jar File (6754863)" on page 20. If you apply patch 3, the workaround documented for patch 2 is not needed.

Sun Java Web Console 3.1 Patches Are Required

The fix for CR 6804294 requires that the following Java Web Console 3.1 patches be applied:

- Solaris SPARC systems: 125950-18
- Solaris x86 systems: 125951-18
- Linux: 125954-18
- Windows: 125955-18 and 127534-18

These patches are available on SunSolve (http://sunsolve.sun.com/).

New Property Prevents Sessions From Being Destroyed After Session Upgrade

For a Distributed Authentication UI server deployment, Access Manager 7.1 patch 3 (CR 6700722) includes the new com.sun.identity.authentication.destroySessionAfterUpgrade property to prevent old sessions from being destroyed after a session upgrade. Values for this property can be:

- true (default): Old sessions are destroyed immediately after a session upgrade.
- false: Old sessions are not destroyed after a session upgrade.

Note. This new property applies only to a Distributed Authentication UI server and not to Access Manager 7.1 server.

To prevent sessions from being destroyed after a session upgrade:

1. Add this new property with a value of false in the AMConfig.properties file. For example:

```
com.sun.identity.authentication.destroySessionAfterUpgrade=false
```

2. Restart the Distributed Authentication UI server.

New Property Allows SSO Token Restriction Other Than an IP Address

Access Manager 7.1 patch 3 (CR 6496155) includes the new `com.iplanet.dpro.session.dnRestrictionOnly` property to enforce the DN as the SSO token restriction rather then the IP address in cross-domain single sign-on (CDSSO) deployments and cookie-hijacking prevention mode. Values for this property can be:

- `true`: Access Manager 7.1 server enforces that an agent send the DN as the SSO token restriction.
- `false` (default): Access Manager 7.1 server uses whatever SSO token restriction is sent by the agent. The token restriction can be the IP address (for older agents that have `amclientsdk.jar` from Access Manager 7 2005Q4 patch 5 and earlier) or the DN (for newer agents that have `amclientsdk.jar` from Access Manager 7 2005Q4 patch 6 and later).

Note: Older agents that use `amclientsdk.jar` from Access Manager 7 2005Q4 patch 5 and earlier should not set this property to `true`.

To require Access Manager 7.1 server to enforce that an agent send the DN as the SSO token restriction:

1. Add this new property with a value of `true` in the `AMConfig.properties` file. For example:

   ```
   com.iplanet.dpro.session.dnRestrictionOnly=true
   ```

2. Restart Access Manager 7.1 server.

Distributed Authentication UI Server Works With Basic Authentication

An Access Manager 7.1 patch 3 Distributed Authentication UI server now works with basic authentication (CR 6754852).

SecurID Authentication Support is Added for Linux Systems

Access Manager 7.1 patch 3 includes support for the SecurID authentication module on Linux systems (CR 6767780).

SecurID authentication support is also available on Solaris SPARC systems and Solaris x86 systems (since patch 2). See "SecurID authentication is supported on Solaris x86 systems (6621802)" on page 21.

Known Issues in Access Manager 7.1 Patch 3

- "Single WAR Access Manager Deployment Cannot Use `https` Protocol Handler (6810092)" on page 17

Single WAR Access Manager Deployment Cannot Use https Protocol Handler (6810092)

If Access Manager 7.1 patch 3 is deployed from a single WAR file, the `https` protocol handler cannot be used.

Workaround. None.

If config Directory Path on Windows Contains a Space, Patch 3 updateschema.pl Fails (6852463)

If Access Manager 7.1 patch 3 is deployed from a single WAR file on Windows, running the `updateschma.pl` script fails if the path to the config directory contains a space.

For example: `c:\Documents and Settings\Administrator\AMConfig`

Workaround. In the `updateschema.pl` file, add a double quote (") around the filename path in the following lines and then rerun the script:

```
$XMLFILE="$AM_ETCDIR/add_cert_org_serverconfig.xml";
$XMLFILE="$AM_ETCDIR/add_cert_org.xml";
$XMLFILE="$AM_ETCDIR/add_choice_none_org.xml";
$XMLFILE="$AM_ETCDIR/add_choice_none_org_serverconfig.xml";
$XMLFILE="$AM_ETCDIR/add_delegation_default_SubjectIdType.xml";
$XMLFILE="$AM_ETCDIR/add_auth_attr.xml";
```

For example:

```
$XMLFILE="\"$AM_ETCDIR/add_cert_org_serverconfig.xml\"";
$XMLFILE="\"$AM_ETCDIR/add_cert_org.xml\"";
$XMLFILE="\"$AM_ETCDIR/add_choice_none_org.xml\"";
$XMLFILE="\"$AM_ETCDIR/add_choice_none_org_serverconfig.xml\"";
$XMLFILE="\"$AM_ETCDIR/add_delegation_default_SubjectIdType.xml\"";
$XMLFILE="\"$AM_ETCDIR/add_auth_attr.xml\"";  Entry 1
```

Hard-coded Path Should be Removed from Patch 3 updateschema.pl Script on Windows (6852467)

If Access Manager 7.1 patch 3 is deployed from a single WAR file on Windows, running the `updateschma.pl` script fails because the path to the tools directory is hard-coded.

Workaround. Remove `/amAdminTools` from the following line of the `updateschema.pl` file and then rerun the script:

```
$AM_ADMIN_CMD="$WAR_TOOLS_DIR/amAdminTools/$DEPLOY_URI/bin/amadmin.bat";
```

Access Manager 7.1 Patch 2

Note – Considerations for patch 2 include:

- **Access Manager 7.1 WAR file deployments**. Patch 140504 is available on `http://sunsolve.sun.com/` for Access Manager 7.1 WAR file deployments. See the patch README file for more information. (For consistency with other Access Manager 7.1 patches, "02" is the first release of this patch.)
- **LDAP JDK patches**. Sun provides LDAP JDK (`ldapjdk.jar`) patches for security and performance related fixes, as described in "Sun Java System LDAP JDK Patches" on page 8.
- **Legacy mode**. If you plan to use Access Manager 7.1 patch 2 in Legacy mode, see "Creation of Data Store authentication module instance fails in Legacy mode (6764919)" on page 19.

Access Manager 7.1 patch 2 fixes a number of problems, as listed in the README file included with the patch. Patch 2 also includes these changes:

Access Manager 7.1 on WebLogic Server requires new `ldapjdk.jar` File (6774634)

Sun provides a new `ldapjdk.jar` file that includes security and performance related fixes for Access Manager 7.1 patch 2. However, the Sun `ldapjdk.jar` won't be effective on WebLogic Server because `weblogic.jar` bundles an older `ldapjdk.jar` file.

Workaround. Put the Sun `ldapjdk.jar` ahead of `weblogic.jar` in the `CLASSPATH`, as follows:

1. Download the new Sun LDAP JDK patch (`ldapjdk.jar`) for your platform, as described in the note under "Access Manager 7.1 Patch 2" on page 18.
2. Copy the Sun `ldapjdk.jar` to the WebLogic `lib` directory.

   For example, on Windows:*BEA_HOME*`\weblogic92\server\lib`
3. Prefix the path to this `ldapjdk.jar` to the existing `classpath`. by editing the startup script used to start WebLogic Server. In the following examples, *BEA_HOME* is where WebLogic Server is installed.

   On Windows, edit:

   BEA_HOME`\weblogic92\samples\domains\wl_server\bin\startWebLogic.cmd`

   Change `set CLASSPATH=%CLASSPATH%;%MEDREC_WEBLOGIC_CLASSPATH%` to:

```
set CLASSPATH=BEA_HOME\weblogic92\server\lib\ldapjdk.jar;%CLASSPATH%;%MEDREC_WEBLOGIC_CLASSPATH%
```

   On Solaris or Linux, edit:

   `/bea/weblogic92/samples/domains/wl_server/bin/startWebLogic.sh`

   or

   `/usr/local/bea/user_projects/domains/base_domain/bin/startWebLogic.sh`

   Change `CLASSPATH="${CLASSPATH}${CLASSPATHSEP}${MEDREC_WEBLOGIC_CLASSPATH}"` to:

```
CLASSPATH="BEA_HOME/weblogic92/server/lib/ldapjdk.jar${CLASSPATH}${CLASSPATHSEP}${MEDREC_WEBLOGIC_CLASSPATH}"
```

4. Restart WebLogic Server.

Creation of Data Store authentication module instance fails in Legacy mode (6764919)

If you install Access Manager 7.1 patch 2 in Legacy mode and you create a Data Store authentication module instance in the Console, an error occurs while the module instance is created.

Note: This problem applies only to Access Manager 7.1 patch 2 and previous releases.

Workaround for Access Manager 7.1 in Legacy Mode. On systems running Access Manager 7.1 in Legacy Mode, in Directory Server, add the `sunRegisteredServiceName` attribute to the Data Store service and set the `sunAMAuthDataStoreAuthLevel` attribute to the minimum value (zero), to ensure the creation of the Data Store authentication module instance. For example, using `ldapmodify`:

```
ldapmodify -D "cn=Directory Manager" -w dm-password -h ds-host -p ds-port
dn: ds-rootdn
changetype: modify
add: sunRegisteredServiceName
```

```
sunRegisteredServiceName: sunAMAuthDataStoreService

ldapmodify -D "cn=Directory Manager" -w dm-password -h ds-host -p ds-port
dn: ou=default,ou=OrganizationConfig,ou=1.0,ou=sunAMAuthDataStoreService,ou=services, ds-rootdn
changetype: modify
add: sunkeyvalue
sunkeyvalue: sunAMAuthDataStoreAuthLevel=0
```

Sub-realm administrator can log in as `amadmin` in root realm (6761627)

If Access Manager 7.1 is installed in Realm mode and a sub-realm administrator creates another `amadmin` user in the sub realm, the second `amadmin` can also log in to the root (top-level) realm.

Access Manager 7.1 patch 2 fixes this problem. As the consequence of this fix, `amadmin` can log in to the Console using this URL:
`http://amhost.example.com:`*port*`/amserver/UI/Login?module=DataStore`

New `com.sun.identity.appendSessionCookieInURL` property (6740071)

The new `com.sun.identity.appendSessionCookieInURL` property determines whether Access Manager appends the session cookie to the URL for zero page authentication. Set this property to `false` to prevent Access Manager from appending the session cookie to the URL. For example, if an application is filtering incoming URLs for special characters for security reasons and a cookie contains a special character, then access is denied The default value is `true` (cookie is appended).

Backward compatibility issue between Access Manager 7.1 and `amclientsdk.jar` File (6754863)

A backward compatibility issue exists between Access Manager 7.1 (all patch levels) and the `amclientsdk.jar` bundled with the policy agent 2.2 Hotpatch 5 and 7.

Workaround. If Access Manager 7.1 does **not** have cookie hijacking prevention enabled, add the following property to the policy agent `AMAgent.properties` file:

```
com.sun.identity.enableUniqueSSOTokenCookie=false
```

Note: If Access Manager 7.1 does have cookie hijacking prevention enabled, this workaround will not work.

Access Manager JAR files should include version number in `MANIFEST.MF` file (6693152)

Access Manager JAR files now have the version and build timestamp added to the `MANIFEST.MF` file. For example:

```
Specification-Version: "7.1"
Implementation-Version: "AM_7.1_20080917:05:27:19"
```

Security permission is missing for CRL validation (6673538)

Certificate-based authentication is not working if it is configured with Certificate Revocation list (CRL) checking.

Workaround. For an existing Access Manager instance, add the following security permission to the web container server policy file and then restart the web container:

```
permission java.security.SecurityPermission "getProperty.ocsp.*";
```

For Sun Java System Application Server and IBM WebSphere Application Server, the security policy file is `server.policy`. For BEA WebLogic Server, the file is `weblogic.policy`.

For new Access Manager instances, the respective web container `amconfig` script has been revised to add this security permission to the security policy file.

SecurID authentication is supported on Solaris x86 systems (6621802)

SecurID authentication is now supported on Solaris x86 systems (as well as on Solaris SPARC systems).

Access Manager Key Provider needs option to use types other than JKS format (6603228)

The default Key Provider implementation (`JKSKeyProvider`) uses JKS format. Access Manager now includes the following new configuration property that allows the keystore type to be changed. For example, for PKCS12 format:

```
com.sun.identity.saml.xmlsig.storetype=PKCS12
```

To use this new property, add it the `AMConfig.properties` file and restart the Access Manager web container.

Delegation privileges cannot be defined for a filtered role (6486843)

If you create a new filtered role, it does not appear under the Privileges tab in the Admin Console.

Workaround. After you apply patch 2, follow these steps to update the Delegation Service (`sunAMDelegationService`) in the Directory Server schema:

1. Create an XML file with the `FILTEREDROLE` subject type. For example:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE Requests
    PUBLIC "-//iPlanet//Sun Java System Access Manager 2005Q4 Admin CLI DTD//EN"
    "jar://com/iplanet/am/admin/cli/amAdmin.dtd">
<Requests>
   <SchemaRequests serviceName="sunAMDelegationService"
```

```
        SchemaType="Global" i18nKey="">
        <AddDefaultValues>
            <AttributeValuePair>
                <Attribute name="SubjectIdTypes"/>
                <Value>FILTEREDROLE</Value>
            </AttributeValuePair>
        </AddDefaultValues>
    </SchemaRequests>
</Requests>
```

Note: The XML encoding used in this example is ISO-8859-1. You might need to use a different encoding depending on your environment.

2. Use the `amadmin` command to load the XML file you created in Step 1 into Directory Server. For example:

```
# cd /opt/SUNWam/bin
# ./amadmin -u amadmin -w pwfile -t new-filteredrole.xml
```

where:

- `pwfile` contains the `amadmin` password.
- `new-filteredrole.xml` is the new XML file you created in Step 1.

3. Restart the Access Manager server web container.

Now, when you log in to the Administration Console, the filtered role will appear under the Privileges tab.

Persistent cookie support is added (6600325)

Persistent cookie support is added for Access Manager session cookies if:

- The `com.iplanet.am.cookie.timeToLive` property is set to a non-zero value in the `AMConfig.properties` file.

  and

- The Access Manager Console is accessed with `PersistAMCookie=true`, as follows:

  `http://`*amhost*`:`*port*`/amserver/UI/Login?PersistAMCookie=true`

Access Manager 7.1 Patch 1

Access Manager 7.1 patch 1 fixes a number of problems, as listed in the README file included with the patch. Patch 1 also includes the following new features and known issues:

- "Support for specific application idle session timeout values" on page 23
- "Web Proxy Agent 2.2-01 in CDSSO mode does not work with Access Manager 7.1 Patch 1 (CR 6611841)" on page 25
- "Distributed Auth UI does not work with a WebSphere Application Server 5.1.1.12 server (CR 6625928)" on page 25
- "Password file exposed in a temporary directory after Patch 1 re-deployment (CR 6640377)" on page 25

Support for specific application idle session timeout values

Patch 1 allows different applications to have different session idle timeout values. In an enterprise, some applications might require session idle timeout values that are less than the session idle time out specified in the session service. For example, you have specified session the idle timeout value in the session service as 30 minutes, but an HR application should timeout if a user has been idle for more than 10 minutes.

This feature is not currently supported for Distributed Authentication and Cross Domain Single Sign-on scenarios

Requirements to use this feature are:

- Agents protecting the application must be configured to enforce URL policy decisions from Access Manager.
- Agents must be configured to run in self policy decision cache mode. See the following properties:
  - For web agents: `com.sun.am.policy.am.fetch_from_root_resource`
  - For J2EE agents: `com.sun.identity.policy.client.cacheMode`
- The Access Manager `AMConfig.properties` file must specify a policy component evaluation order such that Condition is evaluated last. See the following property:

  `com.sun.identity.policy.Policy.policy_evaluation_weights`
- The application access allowed by the agent based on a locally cached decision will not be known to the Condition on Access Manager. Therefore, the actual application idle timeout will be between the application idle timeout to the application idle timeout minus the agent cache duration.

To use this feature:

- Add an Authentication Scheme Condition to the policies protecting the application that requires the application specific session idle timeout.
- Specify the Application Name and Timeout Value in the Authentication Scheme Condition.
- Use the same Application Name and Time Out value in all the policies that apply to the resources for the application.
- Specify the Timeout Value in minutes. If the value is 0 or greater than the session idle timeout value specified in the session service, the value is ignored, and the timeout from session service will apply.

For example, consider a policy `http://host.sample.com/hr/*`, with this Authentication Scheme Condition:

- Authentication Scheme: LDAP
- Application Name: HR
- Timeout Value: 10

If there are multiple policies defined to protect resources of the HR application, you must add the Condition to all of the policies.

When a user in a distinct session attempts to access the HR application protected by the Access Manager agent, that user is prompted to authenticate for the LDAP scheme (if the user is not yet authenticated).

If the user has already authenticated to the LDAP scheme, that user is allowed access only if the time is less than 10 minutes since the time the last authentication or if the time is less than 10 minutes since that user's last access time to the HR application. Otherwise, the user is prompted to authenticate to the LDAP scheme again to access the application.

The Idle Session Timeout for a realm is configured for the highest value required by all applications. Shorter Idle Session Timeout requirements are enforced by the Policy Condition protecting the appropriate applications. However, if you define explicit "deny" policies to protect the application, it would break this protection. This is because the new the new Condition extends the idle timeout for the application, assuming that the access to the application is allowed if this Condition is satisfied. If the other "deny" policy is satisfied, the user can not access the application.

Application idle timeout of value 0 is treated as `Integer.MAX_VALUE` for the purposes of idle timeout enforcement.

Web Proxy Agent 2.2-01 in CDSSO mode does not work with Access Manager 7.1 Patch 1 (CR 6611841)

The Web Proxy Agent 2.2-01 in Cross Domain Single Sign-on mode does not work with Access Manager 7.1 Patch . The agentRootURL requirement was added as a security measure to ensure that CDC is handing off ssotoken cookie to trusted agents running at known URLs.

Workaround

1. Create a new agent profile in the Access Manager server using the administration console.
2. Set the Agent Key `agentRootURL=http://<agenthost>:<agentport>/`using the console.
3. Get the encrypted password for the new agent profile using `cryp_util`on the Agent
4. Use the new agent username and corresponding encrypted password in the `AMAgent.properties` file.

Distributed Auth UI does not work with a WebSphere Application Server 5.1.1.12 server (CR 6625928)

In Patch 1, the

Distributed Authentication user interface does not work with a WebSphere Application Server 5.1.1.12 server.

Password file exposed in a temporary directory after Patch 1 re-deployment (CR 6640377)

After Access Manager Patch 1 applied to Access Manager 7.1 and re-deployed, several`/tmp` directories are created. In one of them, the permissions are incorrectly set so that the `sun_ad_dirmgrpasswd` is readable. These directories are automatically deleted when the deployment is completed, but they are exposed for a matter of time before hand. This is a potential security risk.

Workaround

Before re-deploying the patch, set `umask 077`. The files will then be created with the correct permissions.

LDAP Failover not working properly (CR 6611627)

LDAP failover does not work if the primary LDAP failover server is set to SSL and the secondary server is set to non-SSL. There is no workaround at this time.

amconfig does not tag-swap and re-register the monitoring framework descriptor (CR 6636710)

When Patch 1 is applied to a full Access Manager installation using the `amconfig` script to redeploy all of the web applications, `amconfig` does not tag swap the monitoring framework descriptor. As a result, the monitoring framework description at `$CONFIG_DIR/com.sun.cmm.am.xml` only contains tags.

Workaround

Back up the monitoring framework descriptor (Solaris locatoin is `/etc/opt/SUNWam/config/com.sun.cmn.am.xml`, Linux location is `/etc/opt/sun/identity/config/com.sun.am.xml`) before applying the patch. Once the patch is applied, replace the patched file with the original file in the same location.

amtune does not work if installed in a non-default directory (CR6640673)

The `amtune` script will not work if installed in a non-default directory. This occurs on all platforms. The script is defaulting to the LDAP installation directory when the package is not found on the system.

Workaround

Modify the `amtune-directory` so that `LDAP_DIR` points to the DSEE base directory:

```
DSADMIN=$LDAP_DIR/ds6/bin/dsadm
```

amtune does not delete the world readable password file (CR 6640672)

The `amtune` script does not delete the password file after it completes. The file should be deleted after the completion of the script.

Workaround

Modify the set `DSADMIN_PASSFILE` attribute, or any directory that only the root user can read, in the `amtune-env` file before running the `amtune` script. For example:

```
DSADMIN_PASSFILE=/var/tmp/dspassfile
```

amtune should set thread pool size at 3 times the number of CPUs or cores for CMT servers (CR 6631123)

The optimal size of Access Manager's notification thread pool size (`com.iplanet.am.notification.threadpool.size` in `AMConfig.properties`) was 3 times the number of CPU's where Access Manager is deployed or the number of cores in cases of CMT servers like Niagara I and II (Sun Fire T1000/2000 and T5120/T5220 servers). The current `amtune-identity` sets the maximum number of thread pools at 28 regardless of number of CPU's and calculates the optimal value based on the available amount of memory.

Workaround

Increase the value in the `com.iplanet.am.notification.threadpool.size` property in `AMConfig.properties` by three times the number of CPU's or cores in cases of CMT servers (e.g., T1000/T2000 or T5210/T5220 servers), overriding the recommended values by `amtune-identity` script.

amsfo.pl does not work for Windows (CR 6629189)

For Access Manager Patch 1 for Windows, the `amsfo.pl` script does not work properly. There is no workaround at this time.

Not able to deploy WAR file generated by patch.bat if -l option is used for Windows (CR 6636474)

If you are deploying the WAR file using `patch.bat`, do not use the `-l` option as it will cause errors and fail to deploy.

amserveradmin.bat throwing errors for Access Manager 7.1 Patch for Windows (CR 6631526)

Executing the `amserveradmin.bat` batch file produces the following error message:

```
The system cannot find the path specified.
Loading amAdminConsole.xml
The system cannot find the path specified.
Loading amAuth.xml
The system cannot find the path specified.
Loading amAuthAnonymous.xml
The system cannot find the path specified.
Loading amAuthCert.xml
The system cannot find the path specified.
```

This is because after reconfiguring, tokens in this file are not getting tag swapped.

Workaround

In the `amserveradmin.bat.template`, set the value for `AM_DIR` to `AM_DIR=c:\sun\identity`. Rename the template file to `amserveradmin.bat`.

amsfo.pl script does not work for Session Failover in a Single War deployment for Windows (CR 6646519)

In a single WAR deployment for Windows, the session failover script, `amsfo.pl`, fails to start the `amsessiondb` client. In order to fix this, perform all of the steps described in the following workaround.

Workaround

1. Edit the `amsfo.conf`file to replace the `AMSESSIONDB_ARGS=` parameter with `AMSESSIONDB_ARGS=""`.
2. Edit the `amsfo.conf` file to replace the `$AM_HOME_DIR/.password` with the absolute value of the `.password` file. For example:

   ```
   PASSWORDFILE=c:/was_session/sfo/.password
   ```

3. Edit the `amsfo.pl` script to include the `-javahome` option for the following argument:

   ```
   $jmq_args = "-bgnd $broker_options -vmargs $broker_vm_args -name
   $broker_instance_name -port $broker_port -cluster $cluster_list -javahome
   $java_home";
   ```

   Set the `java_home` as defined in your environment, as it does not read it from the environment even though it is set there.
4. Remove the `/logs/jmq pid` file.

Access Manager classpath not pointing to xml.sec.jar in Patch 1 for Windows (CR 6644461)

In Access Manager Patch 1 for Windows, the Access Manager classpath is not pointing to the patched version of the `xmlsec.jar`.

Workaround

Copy *jes-install-dir*`\identity\lib\xmlsec.jar` to *jes-install-dir*`\share\lib\xmlsec.jar`.

Post authentication plug-in supports Microsoft SharePoint (CR 6541695)

The Access Manager post-authentication plug-in (`ReplayPasswd.java`) has been modified in this patch release to read the `com.sun.am.sharepoint_login_attr_name=`*sharepoint-login-value* property. The value of this property indicates the user token that SharePoint uses for authentication.

For example, if "login" is the LDAP attribute that is mapped in both the places (Access Manager and SharePoint), then the property should be `com.sun.am.sharepoint_login_attr_name=login`.

The post-authentication plug-in will read this property and retrieve the corresponding value from Directory Server. It will then replace this value as a session property. The IIS6 authentication plug-in is modified to read this new property and set authorization headers for Sharepoint to work.

Retrieving schema from Active Directory data store fails (CR 6542686)

Access Manager 7.1 would not successfully retrieve the schema if you are using the Active Directory datastore. Installing patch 1 will fix this issue. To incorporate the fix, load the `am_remote_ad_schema.ldif` file. This file is located at `/etc/opt/SUNWam/config/ldif` for Solaris systems, `/etc/opt/sun/identity/config/ldif` for Linux systems, and `\identity\config\ldif` for Windows systems.

Access Manager supports the JDK 1.5 HttpURLConnection setReadTimeout method (CR 6536635)

To support the `setReadTimeout` method, the `AMConfig.properties` file has the following new property for you to set the read timeout value:

```
com.sun.identity.url.readTimeout
```

If the web container is using JDK 1.5, set this property to an appropriate value to cause connections to time out, in order to avoid having too many open HttpURLConnections that might cause the server to hang. The default is 30000 milliseconds (30 seconds).

The `setReadTimeout` method is ignored if `com.sun.identity.url.readTimeout` is not present in the `AMConfig.properties` file or is set to an empty string.

saml samples will not work if the saml module instance is created with lower case name "saml" (CR 6648342)

If a SAML instance is created with the name "saml", the `amSAML` authentication fails and the sample will not work.

G11n: CLI commands amhasetup and amserver are not localized (CR 6567135)

For EMEA locales, the amhasetup and amserver command line utilities return unlocalized output. For other languages, the output is localized.

G11n: The User sub-tab incorrectly translated in French language (CR 6633529)

After you have created a user in the User sub-tab of the Realm tab in the French language, the edited user message is incorrectly displayed as `Modification de Utilisateur`.

Web Security Service Issues Fixed

6543625 — UserName token authentication can authenticate against a configured LDAP module

The UserName token authentication is able to authenticate against a configured LDAP module. In previous releases, the UserName token authentication could only use the Access Manager file-based authentication realm.

6543626 — SOAPRequestHandler returns the SSOToken set in the Subject

SOAPRequestHandler now returns the SSOToken set in the Subject, in addition to X509 or UserName token that was used for authentication. The SSOToken is in the format usable to the PolicyEvaluator API.

6544177 — When using X509 token with an invalid certificate AM always accepts the cert even without root CA

When using X509 token with an invalid certificate, Access Manager always accepts the certificate, despite the fact that the root CA is not in the Keystore. this problem has been fixed.

6559603 — Boolean configuration flag for "request" signing

A web service user can now choose boolean configuration for SOAP request signing.

6543620 Access Manager Policy Agent profiles able to apply a digital signature to the service request for UserName token

Access Manager Policy Agent profiles can apply a digital signature to the service request and the service response. In previous releases, digital signature could be used only in case when X509 token is included into SOAP message for authentication.

6543623 Access Manager Policy Agent profiles able to encrypt SOAP request body and SOAP response body

Access Manager Policy Agent profiles are now able to encrypt SOAP request body and SOAP response body.

6570021 Encryption supports SOAP messages with extra spaces.

Access Manager now supports the encryption of SOAP message with extra spaces and new lines between XML elements of SOAP message. It is common to see SOAP messages with extra spaces and new lines inserted for better readability.

Removed ACIs that cause unnecessary performance degradation (CR 6484947)

The `amtune` script has been changed to enhance the performance of AM 7.1 by removing unnecessary ACI checks. You must run `amtune` after the patch installation to remove the ACIs.

6.3–based console online help not displayed win Application Server 8.2 (CR 6587213)

If you have installed Access Manager from the Java ES 5 update 1, and have it deployed with Application Server 8.2, the Access Manager console online help will not display. This only occurs in the 6.3–based Access Manager console, accessed by `/amconsole`.

Multiple passwords not required for amtune script

In Access Manager 7.1 Patch 1 you do not need to enter multiple passwords when executing individual `amtune` scripts. Only the wrapper `amtune` script which calls individual scripts needs multiple passwords. For instance, `amtune-os` and `amtune-identity` do not require any password. `amtune-directory` requires only Directory Manager password, while `amtune-ws6`, `-ws7` and `-as8` require the corresponding web container admin passwords.

amtune-os will not run in local zone

`amtune-os` will not run if the wrapper `amtune` script is run in a local zone on Solaris 10, or higher, but other individual `amtune` scripts will still run.

Pre-Installation Considerations

Review the following section before applying the patch.

Installing and Configuring Access Manager

The Access Manager patches described in this document do not install Access Manager. Before you install the patch, Access Manager 7.1 must be installed on the server. For information about installation for Sun Java Enterprise System 5, see following documents:

- If you are installing the patch on a Solaris or Linux system, see the *Sun Java Enterprise System 5 Installation Guide for UNIX*
- If you are installing the patch on a Windows system, see the *Sun Java Enterprise System 5 Installation Guide for Microsoft Windows*.

For information about installation for Sun Java Enterprise System 5 Update 1, see following documents:

- *Sun Java Enterprise System 5 Installation Guide for UNIX*

- *Sun Java Enterprise System 5 Upgrade Guide for Microsoft Windows*

You should also be familiar with running the `amconfig` script to deploy, re-deploy, and configure Access Manager, as described in the Chapter 2, "Running the Access Manager amconfig Script," in *Sun Java System Access Manager 7.1 Postinstallation Guide*.

For a list of the Access Manager patches that are made obsolete by this patch and any patches that you must install before you install this patch, refer to the README file included with this patch.

Caution – Access Manager patches (as with any other patches) should be tested on a staging or pre-deployment system before you put them into a production environment. Also, the patch installer might not update your customized JSP files properly, so you might need to make manual changes in these files in order for Access Manager to function properly.

Patch Installation Instructions

Note – Beginning with patch 3 (and any subsequent patches unless specifically noted), you must run the `updateschema.sh` script on Solaris and Linux systems or the `updateschema.pl` script on Windows. The `updateschema` script updates the Sun Java System Directory Server schema with any new attributes required by the patch.

For more information see "Running the `updateschema` Script is Required" on page 13.

Patch Installation Instructions For Solaris Systems

Before you install the Solaris patch, make sure that you have backed up the files listed in "Pre-Installation Considerations" on page 31.

To add and remove patches on Solaris systems, use the `patchadd` and `patchrm` commands, which are provided with the OS.

patchadd Command

Use the `patchadd` command to install a patch on a standalone system. For example:

```
# patchadd /var/spool/patch/126356-05
```

Note – If you are installing the Solaris patch on a Solaris 10 global zone, invoke the `patchadd` command with the `-G` argument. For example:

```
patchadd -G /var/spool/patch/126356-05
```

The `postpatch` script displays a message about redeploying the Access Manager applications, except on a system that has only the Access Manager SDK component installed.

The `postpatch` script creates the `amsilent` file in the following directory:

- Solaris systems: *AccessManager-base*`/SUNWam`

AccessManager-base is the base installation directory. The default base installation directory is `/opt` on Solaris systems and `/opt/sun` on Linux systems.

The `amsilent` is based on the `amsamplesilent` file, but with some required parameters set according to the Access Manager configuration files on the system. The password parameters, however, contain default values. Uncomment and modify the value of each password parameter and carefully check values of other parameters in this file, as needed for your deployment.

The `COMMON_DEPLOY_URI` parameter, the URI prefix for the common domain web application, also contains a default value. If you have chosen a non-default value for this URI, make sure to update this value. Otherwise, the redeployment of the web applications with `amconfig` and the patch generated `amsilent` file will fail.

Then, run the following command (shown with Access Manager installed in the default directory):

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

Caution – The `amsilent` file contains sensitive data such as administrator passwords in plain text, so make sure you secure the file as appropriate for your deployment.

patchrm Command

Use the `patchrm` command to remove a patch from a standalone system. For example:

```
# patchrm 126356-05
```

The `backout` script displays a message similar to the `patchadd` command, except on a system that has only the Access Manager SDK component installed.

After the patch is removed, redeploy the Access Manager applications using the `amsilent` file in the *AccessManager-base*`/SUNWam` directory, where *AccessManager-base* is the base installation directory. The default base installation directory is `/opt` on Solaris systems.

Set the parameters in the `amsilent` file, as needed for your deployment.

Then, run the following command, which is shown with Access Manager installed in the default directory on Solaris systems:

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

For additional information and examples about the `patchadd` and `patchrm` commands, see the appropriate Solaris `man` pages.

Solaris 10 Zones

The Solaris 10 operating system introduced the new concept of "zones." Consequently, the patchadd command includes the new `-G` option, which adds a patch only to the global zone. By default, the patchadd command looks for the `SUNW_PKG_ALLZONES` variable in the pkginfo of packages to be patched. However, for all Access Manager packages, the `SUNW_PKG_ALLZONES` variable is not set, and the `-G` option is required if Access Manager 7.1 is installed in the global zone. If Access Manager is installed in a local zone, the `patchadd -G` option has no effect.

If you are installing Access Manager 7.1 patches on a Solaris system, it is recommended that you use the `-G` option. For example:

```
 # patchadd -G AM7_patch_dir
```

Similarly, if Access Manager is installed in the global zone, the `-G` option is required to run the `patchrm` command. For example:

```
# patchrm -G 126356-05
```

Patch Installation Instructions For Linux Systems

Before you install the Linux patch, make sure that you have backed up the files listed in "Pre-Installation Considerations" on page 31.

The `installpatch` installs a patch on a standalone Linux system. For example:

```
# ./installpatch
```

The `postpatch` script prints messages similar to the messages on a Solaris system. However, the procedure to back out a patch on a Linux system is different than on a Solaris system. There is no generic script to back out a Linux patch. If a lower version of the patch was previously installed, you can re-install that version and then follow the postpatch instructions to redeploy the Access Manager applications by running the `amconfig` script.

If the patch is installed on the Access Manager 7.1 RTM release and you want to remove the patch and restore the system to the RTM state, you must reinstall the Access Manager RTM bits using the `reinstallRTM` script. This script takes the path where the Access Manager RTM RPMs are stored and installs the RTM RPMs over the patched RPMs. For example:

```
# ./scripts/reinstallRTM path_of_AM71_RTM_RPM_directory
```

After you run the `reinstallRTM` script, redeploy the Access Manager applications by running the `amconfig` script and the restart the web container.

Patch Installation Instructions For Windows Systems

The requirements to install the Windows patch include:

- Access Manager 7.1 must be installed on the Windows system. For information about installation, see the *Sun Java Enterprise System 5 Installation Guide for Microsoft Windows*.
- To run the patch scripts, ActivePerl 5.8 (or later) is required on the Windows system.

Installing the Windows Patch

Before you install the Windows patch, make sure that you have backed up the files listed in "Pre-Installation Considerations" on page 31.

In the base directory path for input to the patch scripts, use a forward slash (`/`). For example: `c:/sun`

To install the Windows patch:

1. Logon to the Windows system as a member of the Administrators group.
2. Create a directory to download and unzip the Windows patch file. For example: `AM71p1`
3. Download and unzip the `126359-05.zip` file in the directory from the previous step.
4. Stop all Java Enterprise System 5 services.
5. Run the `AM71p1\scripts\prepatch.pl` script.
6. Run `AM71p1\126359-05.exe` to install the patch.
7. Run the `AM7p5\scripts\postpatch.pl` script.
8. Restart the Java ES 5 services.
9. Redeploy the Access Manager applications.

Note – If Access Manager is deployed to Web Server 7.0, make sure that Web Server administration server is up and running

---

Backing Out the Windows Patch

To back out the Windows patch:

1. Logon to the Windows system as a member of the Administrators group.
2. Run the `Uninstall_126359-05.bat` file.
3. Run the `AM71p1\scripts\postbackout.pl` script.

4. Redeploy the Access Manager applications.
5. Restart the Java ES 5 services.

Access Manager 7.1 Patch 1 Single WAR Deployment

Note – Sun provides patch functionality for Access Manager 7.1 WAR deployments on all platforms in patch 140504, which is available on `http://sunsolve.sun.com/`. See the patch README file for more information. (For consistency with other Access Manager 7.1 patches, "02" is the first release of this patch.)

This section describes new features, installation instructions and known problems for Access Manager 7.1 patch 1 single WAR deployment.

New Container Versions Supported

The Access Manager 7.1 patch 1 now supports the following containers:

- IBM WebSphere Application Server 6.1
- BEA WebLogic Server 9.2

The version of Access Manager single web-application (WAR) supported on these containers is located in *zip_install_directory*`/applications/jdk14`. *zip_install_directory* is the directory to which you downloaded the .ZIP file for the WAR.

Note – Even though WebLogic 9.2 is compatible with Sun's JDK version 1.5_04, not all of the classes required by Access Manager are present. Access Manager single web-application, when deployed from *zip_install_directory*`/applications/jdk15`, will result in exceptions thrown of missing classes. The deployment succeeds and the console is accessible, but this causes issues with the clients. In general, *zip_install_directory*`/applications/jdk14` should be used for non-Sun or third party containers, even if their run time environment is JDK 1.5.x.

Considerations for Single WAR Deployment with WebSphere 6.1

After you obtain the Access Manager 7.1 patch 1 single WAR, see "Adding Access Manager Permissions to the Server Policy File" in *Sun Java System Access Manager 7.1 Postinstallation Guide* for information on configuring the permissions to the server policy file for the web container on which Access Manager will be deployed.

In addition to the policy changes, follow the steps described in "Deploying an Access Manager 7.1 WAR File in IBM WebSphere Application Server" in *Sun Java System Access Manager 7.1 Postinstallation Guide*.

Considerations for Single WAR Deployment with Weblogic 9.2

For BEA WebLogic Server 9.2, the following JVM property needs to be added in the BEA WebLogic Server instance start script, `startWebLogic.sh`:

```
JAVA_OPTIONS= "-Djavax.xml.soap.MessageFactory=com.sun.xml.

messaging.saaj.soap.ver1_1.SOAPMessageFactory1_1Impl"
```

After you obtain the Access Manager 7.1 patch 1 single WAR, see "Adding Access Manager Permissions to the Server Policy File" in *Sun Java System Access Manager 7.1 Postinstallation Guide* for information on configuring the permissions to the server policy file for the web container on which Access Manager will be deployed.

Applying Patch 1 for Single WAR Deployment

The application of patch 1 is required if you already have an RTM version of the Access Manager single web-application deployed and wish to redeploy the Access Manager patch 1 web application. If there is no prior deployment of Access Manager, then Access Manager single web-application (WAR) provided under the *zip_install_dir*`/applications` directory can be used.

The patch is provided in a separate directory, *zip_install_dir*`/patch`. In this directory, there is a README provided with instructions on running the patch utility.

The patch utility and related files provided in the ZIP file are only for applying the patch to Access Manager single web-application downloaded from the SUN's download site. This patch will not operate with the Access Manager single WAR web-application generated by using the Java Enterprise Systems 5 "Configure Later" option with `DEPLOY_LEVEL=10`.

After you have successfully applied the patch, copy the following property in the configured instance's `AMConfig.properties` file and then restart the container:

```
com.sun.identity.url.readTimeout=30000
```

This patch does not support the patch application to the JavaEE SDK Access Manager WAR file.

Known Issues with Patch 1 WAR Deployment

This section lists the known issues with the Access Manager 7.1 patch 1 WAR deployment.

Modifying SAML source ID in WAR deployment for Access Manager 7.1 Patch 1 (CR 6582972)

This issue will only occur when you already have a RTM version of Access Manager single web-application deployed and would now want to redeploy Access Manager patch 1 web-application. After you have successfully un-deployed the RTM version of Access Manager

and redeployed the patch 1 version of Access Manager, follow the steps outlined under the "Workaround" section. If you are deploying Access Manager patch 1 web-application without any prior installation of Access Manager in your environment, then the outlined workaround is not required. Additionally, this workaround is applicable only when using SAML v.1.

Workaround

1. Extract the Access Manager 7.1 patch 1 ZIP file into a directory, for example `am71_patch1_dir`.
2. Run the following command to generate the SAML source ID:

   ```
   java --classpath am71_patch1_dir/sdk/amclientsdk.jar
   com.sun.identity.saml.common.SAMLSiteID/server_protocol://server_host:server_port/server_deploy
   ```

   A Base64 encoded SAML source ID is displayed. Keep this display open.
3. Log into the Access Manager console as the top-level administrator.
4. Go to Federation > SAML > Site Identifiers and click the Instance ID link for the server
5. In the Site ID field, replace the old value (`SAML_SITEID`) with the source ID generated in the previous step and click Save when finished.
6. Click Save again.

amAdmin from amAdminTools.zip Single WAR does not work with IBM JDK WebSphere 6.1 (CR 6618861)

Currently there is no support to run Access Manager's CLI tools with a non-Sun JDK.

What's New in This Release

This release includes the following new features:

Java ES Monitoring Framework Integration

Access Manager 7.1 integrates with the Java Enterprise System monitoring framework through Java Management Extensions (JMX). JMX technology provides the tools for building distributed, Web-based, modular, and dynamic solutions for managing and monitoring devices, applications, and service-driven networks. Typical uses of the JMX technology include:

consulting and changing application configuration, accumulating statistics about application behavior, notification of state changes and erroneous behaviors. Data is delivered to centralized monitoring console.

Access Manager 7.1 uses the Java ES Monitoring Framework to capture statistics and service-related data such as the following:

- Number of attempted, successful, and failed authentications
- Policy caching statistics
- Policy evaluation transaction times

Web Service Security

Access Manager 7.1 extends authentication capabilities to web services in the following ways:

- Inserts tokens to outgoing messages
- Evaluates incoming messages for security tokens
- Enables point-and-click selection of Authentication providers for new applications

Single Access Manager WAR file deployment

Access Manager includes a single WAR file you can use to deploy Access Manager services consistently to any supported container on any supported platform. The Access Manager WAR file can coexist with the Java Enterprise System installer, which deploys multiple JAR, XML, JSP, HTML, GIF, and various properties files.

For more information about staging, configuring, and deploying the Access Manager WAR file, see the *Sun Java System Access Manager 7.1 Postinstallation Guide*.

Enhancements to Core Services

Web Containers supported

- Sun Java System Web Server 7.0
- Sun Java System Application Server 8.2
- BEA WL 8.1 SP4
- IBM WebSphere 5.1.1.6

Monitoring Framework Integration

Access Manager can use the Java Enterprise System Monitoring Framework to monitor the following:

1. Authentication

- Number of authentications attempted
- Number of remote authentications attempted (optional)
- Number of successful authentications
- Number of failed authentications
- Number of successful logout operations
- Number of failed logout operations
- Transaction time for each module if possible (running and waiting states)

2. Sessions
   - Size of the session table (hence maximum number of sessions)
   - Number of active sessions (incremental counter)
3. Profile Service
   - Maximum cache size
   - Transaction time for operations (running and waiting)
4. Policy
   - Policy evaluation in and out requests
   - Policy connection pool statistics for the subject's plug-in's LDAP server

Authentication module

- Distributed Authentication service not required to stick to one server for load-balanced deployments
- Authentication service and server not required to stick to one server for load-balanced deployments
- Composite advices support among Authentication service, Policy Agents, and Policy service. Includes `AuthenticateToRealm` condition, AuthenticateToService condition, and realm qualification to all conditions.
- Advising organization (realm qualified Authentication conditions)
- Authentication configurations / authentication chains (`AuthServiceCondition`)
- Module-based authentication can now be disallowed if Authentication chaining is enforced
- Distributed Authentication service supports Certificate authentication module
- Added `CertAuth` to Distributed Authentication UI to make it a full featured credential extractor presentation
- New Datastore authentication module as an out-of-box module which authenticates against the configured datastore for a given realm
- Account lockout configuration now persistent across multiple AM server instances
- Chaining of post-processing SPI classes

Policy module

- A new policy condition `AuthenticateToServiceCondition` added, to enforce the user is authenticated to specifc authentication service chain.

- A new policy condition `AuthenticateToRealmCondition` added, to enforce the user is authenticated to a specific realm.
- A new policy condition `LDAPFilterCondition` is added, to enforce the user matches the specified ldap filter.
- Support for one level wild card compare to facilitate protecting the contents of the directory without protecting sub-directory.
- Policies can be created in subrealms without explicit referral policies from parent realm if organization alias referral is enabled in global policy configuration.
- `AuthLevelCondition` can specify the realm name in addition to authentication level.
- `AuthSchemeCondition` can specify the realm name in addition to authentication module name .

Service Management module

- Support for storing Service Management/Policy configuration in Active Directory

Access Manager SDK

- Support APIs for authenticating users to a default Identity Repository framework database

Web Services support

- Liberty ID-WSF SOAP provider: Authentication provider that encapsulates the Liberty ID-WSF SOAP binding as implemented by Access Manager. This consists of a client and service provider.
- HTTP layer SSO provider: HttpServlet layer authentication provider that encapsulates server-side Access Manager-based SSO

Installation module

- Repackaging Access Manager as J2EE Application resulting in a single WAR file to become web deployable
- Support for 64-bit SJS Web Server 7.0 - to support the 64-bit JVM

Delegation module

- Support for grouping of delegation privileges

Upgrade

- Supports upgrade to Access Manager 7.1 from the following versions: Access Manager 7.0 2005Q4, Access Manager 6.3 2005Q1, and Identity Server 6.2 2004Q2.

Logging

- Support for delegation in logging module - controlling which Identities are authorized to write to or read from the log files.

- Support JCE Based `SecureLogHelper` - making it possible to use JCE (in addition to JSS) as a security provider for Secure Logging implementation

Deprecation Notification and Announcement

Sun Java(TM) System Access Manager 7.1 identity management APIs and XML templates enable system administrators to create, delete, and manage identity entries in Sun Java System Directory Server. Access Manager also provides APIs for identity management. Developers use the public interfaces and classes defined in the `com.iplanet.am.sdk` package to integrate management functions into external applications or services to be managed by Access Manager. Access Manager APIs provide the means to create or delete identity-related objects as well as to get, modify, add, or delete the objects' attributes from Directory Server.

The Access Manager `com.iplanet.am.sdk` package, commonly known as AMSDK, will not be included in a future Access Manager release. This includes all related APIs and XML templates. No migration options are available now, and no migration options are expected to be available in the future. The user provisioning solutions provided by Sun Java System Identity Manager are compatible replacements that you can start to use now. For more information about Sun Java System Identity Manager, see `http://www.oracle.com/us/products/middleware/identity-management/oracle-identity-manager/index.html`.

Hardware and Software Requirements

The following table shows the hardware and software that are required for this release.

TABLE 2 Hardware and Software Requirements

Component	Requirement
Operating system (OS)	■ Solaris10 on SPARC, x86, and x64 based systems, including support for whole root local and sparse root zones. ■ Solaris 9 on SPARC and x86 based systems. ■ Red Hat Enterprise Linux 5.0 Server, 32 and 64-bit versions, all updates ■ Red Hat Enterprise Linux 3 and 4, all updates Advanced Server (32 and 64-bit versions) and Enterprise Server (32 and 64-bit versions) ■ Windows Windows 2000 Advanced Server, Data Center Server version SP4 on x86 Windows 2003 Standard (32 and 64–bit versions), Enterprise (32 and 64–bit versions), Data Center Server (32–bit version) on x86 and x64 based systems Windows XP Professional SP2 on x86 based systems HP-UX 11i v1 (11.11 from uname), 64–bit on PA-RISC 2.0. Access Manager 7.1 Patch 1 is not available for HP-UX. For the most updated list of supported operating systems, see "Platform Requirements and Issues" in *Sun Java Enterprise System 5 Release Notes for UNIX* in the *Sun Java Enterprise System 5 Release Notes for UNIX*, or "Hardware and Software Platform Information" in *Sun Java Enterprise System 5 Release Notes for Microsoft Windows* in the *Sun Java Enterprise System 5 Release Notes for Windows.*
Java 2 Standard Edition (J2SE)	J2SE platform 6.0, 5.0 Update 9 (HP-UX: 1.5.0.03), 1.4.2 Update 11, and 5.0 Update 12 (as of Java Enterprise System 5 update 1)

TABLE 2 Hardware and Software Requirements *(Continued)*

Component	Requirement
Directory Server	Access Manager Information Tree (configuration data store): ■ Sun Java System Directory Server Enterprise Edition 6.3 (requires Access Manager 7.1 Patch 2 or later) ■ Sun Java System Directory Server Enterprise Edition 6.1 and 6.2 (requires Access Manager 7.1 Patch 1 or later) ■ Sun Java System Directory Server 5.2 2005Q4 and 6.0 Access Manager Identity Repository (user data store): ■ Sun Java System Directory Server Enterprise Edition 6.3 (requires Access Manager 7.1 Patch 2 or later) ■ Sun Java System Directory Server Enterprise Edition 6.1 and 6.2 (requires Access Manager 7.1 Patch 1 or later) ■ Sun Java System Directory Server 5.2 2005Q4 and 6.0 ■ Microsoft Active Directory
Web containers	Sun Java System Web Server 7.0 and 7.0 Update 1. On supported platform/OS combinations you may elect to run the Web Server instance in a 64 bit JVM. Support platforms: Solaris 9/SPARC, Solaris 10/SPARC, Solaris 10/AMD64, Red Hat AS or ES 3.0/AMD64, Red Hat AS or ES 4.0/AMD64 Sun Java System Application Server Enterprise Edition 8.2 BEA WebLogic 8.1 SP4, and 9.2 for (Patch 1). WebLogic is not supported with Access Manager for HP-UX. IBM WebSphere Application Server 5.1.1.6 and 6.1(for Patch 1). WebSphere is not supported with Access Manager for HP-UX.
RAM	Basic testing: 512 Mbytes Actual deployment: 1 Gbyte for threads, Access Manager SDK, HTTP server, and other internals
Disk space	512 Mbytes for Access Manager and associated applications

If you have questions about support for other versions of these components, contact your Sun Microsystems technical representative.

Supported Browsers

The following table shows the browsers that are supported by the Sun Java Enterprise System 5 release.

TABLE 3 Supported Browsers

Browser	Platform
Firefox 1.0.7, 1.5, 2.0 and later	Windows XP
	Windows 2000
	Solaris OS, versions 9 and 10
	Red Hat Linux 3 and 4
	Mac OS X
Microsoft Internet Explorer7	Windows XP
	Supported for Patch 1 onwards.
Microsoft Internet Explorer 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows 2000
Mozilla 1.7.12	Solaris OS, versions 9 and 10
	Windows XP
	Windows 2000
	Red Hat Linux 3 and 4
	Mac OS X
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000
Netscape Communicator 7.1	Solaris OS, versions 9 and 10

General Compatibility Information

AMSDK intersystem incompatibility with Access Manager server

The following combinations are not compatible between the AMSDK and the Access Manager server in the following Java Enterprise System releases:

- Java Enterprise System 2004Q2 AMSDK is not compatible with the Java Enterprise System 5 Access Manager server (this release).
- Java Enterprise System 5 AMSDK (this release) is not compatible with the Java Enterprise System Access Manger 2004Q2 (formerly Identity Server) server.

Upgrade not supported for Access Manager HPUX version

There is no support for an upgrade path from Access Manager 7 2005Q4 to Access Manger 7.1 (this release) for the HPUX version.

Access Manager Legacy Mode

If you are installing Access Manager with any of the following products, you must select the Access Manager Legacy (6.x) mode:

- Sun Java System Portal Server
- Sun Java System Communications Services servers, including Messaging Server, Calendar Server, Instant Messaging, or Delegated Administrator

You select the Access Manager Legacy (6.x) mode, depending on how you are running the Java ES installer:

To determine the more for an Access Manager 7.1 installation, see "Determining the Access Manager Mode" on page 47.

Java ES Silent Installation Using a State File

Java ES installer silent installation is a non-interactive mode that allows you to install Java ES components on multiple host servers that have similar configurations. You first run the installer to generate a state file (without actually installing any components) and then edit a copy of the state file for each host server where you plan to install Access Manager and other components.

To select Access Manager in Legacy (6.x) mode, set the following parameter (along with other parameters) in the state file before you run the installer in silent mode:

```
...
AM_REALM = disabled
...
```

For more information about running the Java ES installer in silent mode using a state file, see the Chapter 5, "Installing in Silent Mode," in *Sun Java Enterprise System 5 Installation Guide for UNIX*.

"Configure Now" Installation Option in Graphical Mode

If you are running the Java ES Installer in graphical mode with the "Configure Now" option, on the "Access Manager: Administration (1 of 6)" panel, select "Legacy (version 6.x style)", which is the default value.

"Configure Now" Installation Option in Text-Based Mode

If you are running the Java ES Installer in text-based mode with the "Configure Now" option, for `Install type (Realm/Legacy) [Legacy]` select `Legacy`, which is the default value.

"Configure Later" Installation Option

If you ran the Java ES Installer with the "Configure Later" option, you must run the `amconfig` script to configure Access Manager after installation. To select Legacy (6.x) mode, set the following parameter in your configuration script input file (`amsamplesilent`):

```
...
AM_REALM=disabled
...
```

For more information about configuring Access Manager by running the `amconfig` script, refer to the *Sun Java System Access Manager 7.1 Administration Guide*.

Determining the Access Manager Mode

To determine whether a running Access Manager 7.1 installation has been configured in Realm or Legacy mode, invoke:

`http(s)://`*host*`:`*port*`/amserver/SMSServlet?method=isRealmEnabled`

Results are:

- true: Realm mode
- false: Legacy mode

Access Manager Policy Agents

The following table shows the compatibility of Policy Agents with the Access Manager 7.1 modes.

TABLE 4 Policy Agents Compatibility With Access Manager 7.1 Modes

Agent and Version	Compatible Mode
Web and J2EE agents, version 2.2	Legacy and Realm modes
Web and J2EE agents, version 2.1 are not supported in Access Manager 7.1	

Known Issues and Limitations

This section describes the following known issues and workarounds, if available, at the time of the Access Manager 7.1 release.

Installation Issues

Information about Java System Enterprise installation issues is contained in the Java Enterprise System 5 Release Notes. See the section "Access Manager Installation Issues" in *Sun Java Enterprise System 5 Release Notes for UNIX*.

This section contains the following Known Issues:

Access Manager single WAR deployment on WebLogic requires JAX-RPC 1.0 JAR files to communicate with client SDK (6555040)

There is a known issue with the single WAR deployed on Weblogic 8.1, with JAX-RPC initialization. In order for Access Manager to communicate with the client SDK, you need to replace the JAX-RCP 1.1 jar files with JAX-RPC 1.0 jar files.

Workaround:

There are two ways to obtain the WAR file. One is through the Java Enterprise System 5 installer with Access Manager set to the Configure Later option, the other is from Sun's download site.

If you have generated the WAR file through the Java Enterprise System 5 installer with the Configure Later option:

1. Remove the following JAXRPC 1.1 `.jar` files from *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib`:
   - `jaxrpc-api.jar`
   - `jaxrpc-spi.jar`
   - `jaxrpc-impl.jar`
2. Copy the following `.jar` files from their respective locations to *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib`:
   - `jaxrpc-api.jar` from `/opt/SUNWam/lib/jaxrpc 1.0`
   - `jaxrpc_ri.jar` from `/opt/SUNWam/lib/jaxrpc 1.0`
   - `commons-logging.jar` from `/opt/SUNWmfwk/lib`

3. Goto *AccessManager-base*/SUNWam/bin/ and run the following command:

   amconfig –s *samplesilent*

   For more information on configuring Access Manager using the amconfig script, see Running the Access Manager amconfig Script in the *Access Manager Post Installation Guide*.

If you have obtained the WAR file through the Oracle download site (http://www.oracle.com/technetwork/indexes/downloads/index.html):

1. Acquire the *ZIP_ROOT*/applications/jdk14/amserver.war file and explode it into a staging area, such as /tmp/am-staging.
2. Remove the following JAXRPC 1.1 .jar files from /tmp/am-staging/WEB-INF/lib:
   - jaxrpc-api.jar
   - jaxrpc-spi.jar
   - jaxrpc-impl.jar
3. Copy the following JAXRPC 1.0 .jar files and the commons logging .jar file, located in the *ZIP_ROOT*/applications/jdk14/jarFix directory to /tmp/am-staging/WEB-INF/lib:
   - jaxrpc-api.jar
   - jaxrpc-ri.jar
   - commons-logging.jar
4. Recreate and deploy the Access Manager WAR. For more information, see Deploying Access Manager as a Single WAR File in the *Access Manager Post Installation Guide*.

Additional .jar file is required for single WAR generated by the Java Enterprise System 5 installer for Websphere 5.1 (6550261)

If the Access Manager single WAR is generated using the Java Enterprise System 5 installer with the Configure Later option, additional .jar files are required before you deploy Websphere 5.1.

Workaround:

1. Copy jsr173_api.jar from /usr/share/lib to the *AcessManager-base*/opt/SUNWam/web-src/WEB-INF/lib directory.
2. Goto *AccessManager-base*/SUNWam/bin/ and run the following command:

   amconfig –s *samplesilent*

   For more information on configuring Access Manager using the amconfig script, see Running the Access Manager amconfig Script in the *Access Manager Post Installation Guide*.

Single WAR deployment for Webshpere requires changes to server.xml to communicate with client SDK (6554379)

In order for the Access Manager single WAR deployment with Websphere 5.1 to successfully communicate with the client SDK, you must make changes to the server.xml file.

Workaround:

To correctly change the `server.xml` file, see the following steps:

1. Acquire the `amserver.war` file. There are two ways to get the single WAR file; through the Java Enterprise System 5 installer with the Configure Later option, or through the sun download site.

   Note – If you have generated the WAR file through the Java Enterprise System 5 installer, make sure that you complete the steps outlined in Known Issue #6550261.

   ---

2. Explode the Access Manager WAR into a staging area, for instance `/tmp/am-staging`.
3. Copy the following shared `.jar` files from `/tmp/am-staging/WEB-INF/lib` to a shared location, such as`/export/jars`:

jaxrpc-api.jar	jaxrpc-spi.jar	jaxrpc-impl.jar	saaj-api.jar
saaj-impl.jar	xercesImpl.jar	namespace.jar	xalan.jar
dom.jar	jax-qname.jar	jaxb-api.jar	jaxb-impl.jar
jaxb-libs.jar	jaxb-xjc.jar	jaxr-api.jar	jaxr-impl.jar
xmlsec.jar	swec.jar	acmecrypt.jar	iaik_ssl.jar
iaik_jce_full.jar	mail.jar	activation.jar	relaxngDatatype.jar
xsdlib.jar	mfwk_instrum_tk.jar	FastInfoset.jar	jsr173_api.jar

4. Remove the same `.jar` files from the `/tmp/am-staging/WEB-INF/lib` in the staging area.
5. Update the Webshpere instance's `server.xml`. Make the changes to *jvmEntries* in `server.xml` if your default instance location is`/opt/WebSphere/AppServer/config/cells/`*node-name*`/nodes/`*node-name*`/servers/server1`, as shown below:

   ```
   <classpath>/export/jars/jaxrpc-api.jar:/export/jars/jaxrpc-spi.jar:
   /export/jars/jaxrpc-impl.jar:/export/jars/saaj-api.jar:
   /export/jars/saaj-impl.jar:/export/jars/xercesImpl.jar:
   /export/jars/namespace.jar:/export/jars/xalan.jar:/export/jars/dom.jar:
   /export/jars/jax-qname.jar:/export/jars/jaxb-api.jar:/export/jars/jaxb-impl.jar:
   /export/jars/jaxb-libs.jar:/export/jars/jaxb-xjc.jar:/export/jars/jaxr-api.jar:
   /export/jars/jaxr-impl.jar:/export/jars/xmlsec.jar:/export/jars/swec.jar:
   /export/jars/acmecrypt.jar:/export/jars/iaik_ssl.jar:
   /export/jars/iaik_jce_full.jar:/export/jars/mail.jar:
   /export/jars/activation.jar::/export/jars/relaxngDatatype.jar:
   /export/jars/xsdlib.jar:/export/jars/mfwk_instrum_tk.jar:
   /export/jars/FastInfoset.jar:/export/jars/jsr173_api.jar</classpath>
   ```

6. Restart the container.

7. Recreate and deploy the Access Manager WAR from /tmp/am-staging. For more information, see Deploying Access Manager as a Single WAR File in the *Access Manager Deployment Planning Guide*.

Changes required for Distributed Authentication to work with Access Manager single War for Weblogic and Webshpere (6554372)

The Distributed Authentication WAR requires additional jar files for parsing for both Weblogic 8.1 and Websphere 5.1 because the container is version JDK14. The JDK14 `.jar` files are located in the following directory of the `.zip` file:

ZIP-ROOT`/applications/jdk14/jarFix`

Workaround:

For Weblogic 8.1:

1. Configure Distributed Authentication using the setup scripts. See Deploying a Distributed Authentication UI Server in the *Access Manager Post Installation Guide*.
2. Explode the updated Distributed Authentication WAR into a temporary location, such as `/tmp/dist-auth`.
3. Copy `xercesImpl.jar`, `dom.jar` and `xalan.jar` to the `/tmp/dist_auth/WEB-INF/lib` directory from *ZIP-ROOT*`/applications/jdk14/jarFix`.
4. Regenerate the Distributed Authentication WAR from the temporary location and deploy it. For more information, see Deploying a Distributed Authentication UI Server WAR File in the *Access Manager Post Installation Guide*.

For Websphere 5.1:

1. Configure Distributed Authentication using the setup scripts. See Deploying a Distributed Authentication UI Server in the *Access Manager Post Installation Guide*.
2. Explode the updated Distributed Authentication WAR into a temporary location, such as `/tmp/dist_auth/`.
3. Copy `xercesImpl.jar`, `dom.jar` and `xalan.jar` to the `/tmp/dist_auth/WEB-INF/lib` directory from *ZIP-ROOT*`/applications/jdk14/jarFix`.
4. Edit the`WEB-INF/web.xml file` and replace `jar://web-app_2_3.dtd` with `http://java.sun.com/dtd/web-app_2_3.dtd`.
5. Regenerate the Distributed Authentication WAR from the temporary location and deploy it. For more information, see Deploying a Distributed Authentication UI Server WAR File in the *Access Manager Post Installation Guide*.

Single WAR Configurator fails against DS (6562076)

Access Manager deployed as a single WAR fails to configure on Directory Server 6 with a single component root suffix, for example. `dc=example`. However, it works with multi component root suffix, for example `dc=example,dc=com`. After running the configurator with configuration datastore as Sun Java System Directory server, it is always advised to go and edit the `serverconfig.xml` to replace the `cn=directory` manager with less privileged user, such as `cn=dsameuser`. This user should be available in the directory server with proper access permissions to the Access Manager service tree.

Workaround: Use the multi component root suffix, for example `dc=example,dc=com`.

Multi-server configuration of AM Single WAR on same host throws exception (6490150)

When configuring the second instance of Access Manager single WAR on the same host against Directory Server, it throws an exception while updating the Organization Alias. This issue does not occur if the second instance configured is on a different host.

Upgrade Issues

- "Required Services not supported in Access Manager 7.1 Console in Realm Mode (6615838)" on page 53

For additional information, see "Upgrade Issues" in *Sun Java Enterprise System 5 Release Notes for UNIX*.

Required Services not supported in Access Manager 7.1 Console in Realm Mode (6615838)

The Required Services functionality is not supported in Realm Mode. Required Services are services that are dynamically added to user entries when the entries are created. Required Services are not supported for users created under the Access Control tab (that is, using the realm feature) because these users will be under the services node. This scenario applies to an Access Manager 7.1 installation in Legacy Mode or the coexistence of Access Manager 7.1 in Legacy Mode with Sun OpenSSO Enterprise 8.0.

However, the Required Services functionality is supported as follows:

- Access Manager 7.1 Legacy Mode with the old Console.
- Access Manager 7.1 Legacy Mode with the new Console for users created under the Directory Manager tab (that is, using the legacy feature) and for users dynamically created using the `amadmin` CLI under the User Management DIT and not the realm DIT.

Compatibility Issues

Access Manager Single Sign-On fails on Universal Web Client (6367058, 6429573)

The problem occurs after you install Access Manager, Messaging Server, and Calendar Server and configure them to work together, and then install the Java Enterprise System 5 120955-01 patch. The user encounters a login error. The error is due to an incompatibility between Policy Agent 2.1 properties and AMSDK. There is no workaround at this time.

StackOverflowError occurs on Web Server 7.0 running in 64–bit mode (6449977)

If Access Manager is configured on a Web Server 7.0 instance using a 64–bit JVM, the user encounters a Server Error message when accessing the console login page. The Web Server error log contains a `StackOverflowError` exception.

Workaround: Modify the Web Server configuration by following these steps:

1. Log in to the Web Server administration console as the Web Server administrator.
2. Click Edit Configuration.

   In the Platform field, select 64, then click Save.
3. Click the Java tab, and then click the JVM Settings tab.
   - Under Options, look for the minimum heap size entry (for example : -Xms). The minimum heap size value should be at least 512m. For example, if the heap size value is not -Xms512m or greater, then change the value to at least -Xms512m.
   - The maximum heap size value should be at least 768m. If the maximum heap size is not -Xmx768m or greater, then change the value to at least -Xmx768m.
   - Set the Java stack size to 512k or 768k by using `-Xss512k` or `-Xss768k`. You can leave it at the default size for 64-bit JVM on Solaris Sparc (1024k) by leaving it blank.
4. Click the Performance tab, then click the link "Thread Pool Settings."

   Change the stack size value to at least 261144, and then click Save.

5. Click the "Deployment Pending" link in the upper right corner of the screen.

   In the Configuration Deployment page, click the Deploy button.

6. In the Results window, click OK to restart the Web Server instance.

   Click the Close in the Results window after the Web Server has been restarted.

Incompatibilities exist in core authentication module for legacy mode (6305840)

Access Manager 7.1 legacy mode has the following incompatibilities in the core authentication module from Access Manager 6 2005Q1:

- Organization Authentication Modules are removed in legacy mode.
- The presentation of the “Administrator Authentication Configuration” and “Organization Authentication Configuration” has changed. In the Access Manager 7.1 Console, the drop-down list has `ldapService` selected by default. In the Access Manager 6 2005Q1 Console, the Edit button was provided, and the LDAP module was not selected by default.

Workaround: None.

Delegated Administrator `commadmin` utility does not create a user (6294603)

The Delegated Administrator `commadmin` utility with the `-S mail,cal` option does not create a user in the default domain.

Workaround: This problem occurs if you upgrade Access Manager to version 7.1 but you do not upgrade Delegated Administrator.

If you do not plan to upgrade Delegated Administrator, follow these steps:

1. In the `UserCalendarService.xml` file, mark the `mail`, `icssubcribed`, and `icsfirstday` attributes as optional instead of required. This file is located by default in the `/opt/SUNWcomm/lib/services/` directory on Solaris systems.
2. In Access Manager, remove the existing XML file by running the `amadmin` command, as follows:

   ```
   # ./amadmin -u amadmin -w password -r UserCalendarService
   ```

3. In Access Manager, add the updated XML file, as follows:

   ```
   # ./amadmin -u amadmin -w password
   -s /opt/SUNWcomm/lib/services/UserCalendarService.xml
   ```

4. Restart the Access Manager web container.

Delegated Administrator `commadmin` utility does not create an organization (6292104)

The Delegated Administrator `commadmin` utility with the `-S mail,cal` option does not create an organization.

Workaround: See the workaround for the previous problem.

Configuration Issues

Incorrect console redirection behind a load balancer (6480354)

If you have Access Manager instances deployed behind a load balancer, login to the Access Manager Console may be redirected to one of the Access Manager instances rather than to the load balancer. The URL in the browser also changes to the Access Manager instance. For example, this problem can occur if you login into the Console using this URL:

```
http://loadbalancer.example.com/amserver/realm
```

This redirection can occur in both Realm mode and Legacy mode deployments.

There are two workarounds for this issue. You can use either one:

1. Login with either of the following URLs:

   `http://`*loadbalancer*`/amserver/UI/Login`

   `http://`*loadbalancer*`/amserver`

2. In `AMConfig.properties`, set the `com.sun.identity.loginurl` property to the name of the loadbalancer. This needs to be done on each Access Manager Instance behind the load balancer.

Notification URL needs to be updated for Access Manager SDK installation without web container (6491977)

If you install the Access Manager SDK without a web container by running the Java ES 5 installer with the Configure Now option, the `com.iplanet.am.notification.url` property in the AMConfig.properties file is set to `NOTIFICATION_URL`. If you don't perform any additional web container configuration, users will not receive notifications from the remote Access Manager server.

Workaround: Reset this property as follows: `com.iplanet.am.notification.url=""`

Password Reset service reports notification errors when a password is changed (6455079)

When a password is changed, Access Manager submits the email notification using an unqualified sender name `Identity-Server`, which results in errors entries in the `amPasswordReset` logs. For example:

```
07/19/2006 10:26:04:010 AM PDT: Thread[service-j2ee,5,main]
ERROR: Could not send email to user [Ljava.lang.String;@999262
com.sun.mail.smtp.SMTPSendFailedException: 553 5.5.4 <Identity-Server>...
Domain name required for sender address Identity-Server
```

Workaround: The following workaround is for Solaris systems. For other platforms such as Linux, Windows, or HP-UX, adjust the base installation directory for the specific platform.

1. In `/opt/SUNWam/locale/amPasswordResetModuleMsgs.properties`, change `fromAddress.label=<Identity-Server>` to `fromAddress.label=<IdentityServer@myhost.company.com>`.
2. In `/opt/SUNWam/locale/amAuth.properties`, change the `lockOutEmailFrom` property from `Password-Administrator` to `Password-Administrator@myhost.company.com`.
3. Restart Access Manager server.

Account Locking feature fails to send email notification when the user's account is locked (6760137)

If the Account Locking feature is enabled and a user is locked out after a defined number of failures, an email notification is not sent.

Workaround. Change the `lockOutEmailFrom` property as described in Step 2 of the workaround for "Password Reset service reports notification errors when a password is changed (6455079)" on page 57 and then restart Access Manager server.

Platform server list and FQDN alias attribute are not updated (6309259, 6308649)

In a multiple server deployment, the platform server list and FQDN alias attribute are not updated if you install Access Manager on the second (and subsequent) servers.

Workaround: Add the Realm/DNS aliases and platform server list entries manually. For the steps, see the section "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" in *Sun Java System Access Manager 7.1 Postinstallation Guide*.

Data validation for required attributes in the services (6308653)

Access Manager 7.1 enforces required attributes in service XML files to have default values.

Workaround: If you have services with required attributes that do not have values, add values for the attributes and then reload the service.

Document workaround for deployment on a secure WebLogic 8.1 instance (6295863)

If you deploy Access Manager 7.1 into a secure (SSL enabled) BEA WebLogic 8.1 SP4 instance, an exception occurs during the deployment of each Access Manager web application.

Workaround: Follow these steps:

1. Apply the WebLogic 8.1 SP4 patch JAR `CR210310_81sp4.jar`, which is available from BEA.
2. In the `/opt/SUNWam/bin/amwl81config` script, (Solaris systems) or `/opt/sun/identity/bin/amwl81config` script (Linux systems), update the `doDeploy` function and the `undeploy_it` function to prepend the path of the patch JAR to the `wl8_classpath`, which is the variable that contains the `classpath` used to deploy and un-deploy the Access Manager web applications.

   Find the following line containing the `wl8_classpath`:

   ```
   wl8_classpath= ...
   ```
3. Immediately after the line you found in Step 2, add the following line:

   ```
   wl8_classpath=path-to-CR210310_81sp4.jar:$wl8_classpath
   ```

The `amconfig` script does not update the realm/DNS aliases and platform server list entries (6284161)

In a multiple server deployment, the `amconfig` script does not update the realm/DNS aliases and platform server list entries for additional Access Manager instances.

Workaround: Add the Realm/DNS aliases and platform server list entries manually. For the steps, see the section "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" in *Sun Java System Access Manager 7.1 Postinstallation Guide*.

Default Access Manager mode is realm in the configuration state file template (6280844)

By default, the Access Manager mode (`AM_REALM` variable) is enabled in the configuration state file template.

Workaround: To install or configure Access Manager in Legacy mode, reset the variable in the state file:

```
AM_REALM = disabled
```

Performance Issues

In Realm mode, creation of a new group generates Group Admin with ACIs that never get used (6485695)

If Access Manager is installed in Realm mode, whenever a new group is created, Access Manager dynamically creates a new Group Admin with the ACIs necessary to manage the group. In Realm mode, these Group Admin ACIs are not used. Directory Server, however, still evaluates them while processing entries under the suffix, which can degrade Access Manager performance, particularly if a deployment creates a large number of groups.

Workaround: The workaround for this problem involves two parts:

- Preventing Access Manager from creating a Group Admin and corresponding ACIs whenever a new group is created
- Removing any existing Group Admin ACIs from Directory Server

Preventing Group Admin ACIs From Being Created

The following procedure prevents Access Manager from creating a Group Admin and corresponding ACIs whenever a new group is created.

Note – This procedure permanently prevents the creation of Group Admins and corresponding ACIs whenever a new group is created. Use this procedure only if this behavior is appropriate for your specific deployment.

---

1. Backup the `amAdminConsole.xml` file. This file is located in the following directory, depending on your platform:
   - Solaris systems: `/etc/opt/SUNWam/config/xml`
   - Linux and HP-UX systems: `/etc/opt/sun/identity/config/xml`
   - Windows systems: *javaes-install-dir*`\identity\config\xml`

     javaes-install-dir represents the Java ES 5 installation directory. The default value is `C:\Program Files\Sun\JavaES5`.

2. In the `amAdminConsole.xml` file, remove the following Group Admin entry, shown between the comment lines:

```
<AttributeSchema name="iplanet-am-admin-console-dynamic-aci-list"
    type="list"
    syntax="string"
    i18nKey="g111">
    <DefaultValues>
...
# Beginning of entry to delete
                <Value>Group Admin|Group Admin Description|ORGANIZATION:aci:
(target="ldap:///GROUPNAME")(targetattr = "*")
(version 3.0; acl "Group and people container admin role";
allow (all) roledn = "ldap:///ROLENAME";)##ORGANIZATION:aci:
(target="ldap:///ORGANIZATION")
(targetfilter=(&amp;FILTER(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Policy Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Organization Admin Role,ORGANIZATION)
(nsroledn=cn=Container Admin Role,ORGANIZATION)
(nsroledn=cn=Organization Policy Admin Role,ORGANIZATION)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members"; allow (read,write,search)
roledn = "ldap:///ROLENAME";)</Value>
# End of entry to delete
...
    </DefaultValues>
</AttributeSchema>
```

3. Use `amadmin` to delete the Admin Console service from Access Manager. For example, on Solaris systems:

```
# cd /opt/SUNWam/bin
# ./amadmin -u amadmin -w amadmin_password
--deleteservice iPlanetAMAdminConsoleService
```

4. Use `amadmin` to reload the Admin Console service into Access Manager from the edited `amAdminConsole.xml` file from Step 2. For example:

```
# ./amadmin -u amadmin -w amadmin_password
-s /etc/opt/SUNWam/config/xml/amAdminConsole.xml
```

5. Restart the Access Manager web container. (If you plan to remove ACIs from Directory Server, as described in the next procedure, wait and restart the web container after you finish that procedure.)

Removing Existing Group Admin ACIs

Note – The following procedure uses the `ldapsearch` and `ldapmodify` utilities to find and remove the Group Admin ACIs. If your deployment is using Directory Server 6.0, you can also use the Directory Server Control Center (DSCC) or the `dsconf` command to perform these functions. For more information, see the Directory Server 6.0 documentation:

`http://docs.sun.com/app/docs/coll/1224.1`

The following procedure removes Group Admin ACIs that already exist in Directory Server.

1. Create an LDIF file to use with `ldapmodify` to remove the Group Admin ACIs. To find these ACIs, use `ldapsearch` (or another directory search tool, if you prefer).

   For example, the following entries in the sample LDIF file named `Remove_Group_ACIs.ldif` will remove the ACIs for a group named New Group:

```
dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///cn=New Group,ou=Groups,o=isp")(targetattr = "*")
(version 3.0; acl "Group and people container admin role"; allow (all)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///ou=People,o=isp")(targetattr="nsroledn")
(targattrfilters="add=nsroledn:(!(nsroledn=*)),
del=nsroledn:(!(nsroledn=*))") (version 3.0;
acl "Group admin's right to add user to people container"; allow (add)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///o=isp")
(targetfilter=(&(|(memberof=*cn=New Group,ou=Groups,o=isp)
(iplanet-am-static-group-dn=*cn=New Group,ou=Groups,o=isp))
(!(|(nsroledn=cn=Top-level Admin Role,o=isp)
(nsroledn=cn=Top-level Help Desk Admin Role,o=isp)
(nsroledn=cn=Top-level Policy Admin Role,o=isp)
(nsroledn=cn=Organization Admin Role,o=isp)(
nsroledn=cn=Container Admin Role,o=isp)
(nsroledn=cn=Organization Policy Admin Role,o=isp)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list ||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members";
allow (read,write,search)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)
aci: (target="ldap:///o=isp")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the root suffix";
allow (all) userdn = "ldap: ///cn=dsameuser,ou=DSAME Users,o=isp"; )
```

2. Use `ldapmodify` with the LDIF file from the previous step to remove the Group ACIs from Directory Server. For example:

```
# ldapmodify -h ds-host -p 389 -D "cn=Directory Manager"
-w ds-bind-password -f Remove_Group_ACIs.ldif
```

3. Restart the Access Manager web container.

Access Manager Console Issues

New Access Manager Console cannot set the CoS template priorities (6309262)

The new Access Manager 7.1 Console cannot set or modify a Class of Service (CoS) template priority.

Workaround: Login to the Access Manager 6 2005Q1 Console to set or modify a CoS template priority.

Old console appears when adding Portal Server related services (6293299)

Portal Server and Access Manager are installed on the same server. With Access Manager installed in Legacy mode, login to the new Access Manager Console using `/amserver`. If you choose an existing user and try to add services (such as NetFile or Netlet), the old Access Manager Console (`/amconsle`) suddenly appears.

Workaround: None. The current version of Portal Server requires the Access Manager 6 2005Q1 Console.

Console does not return the results set from Directory Server after reaching the resource limit (6239724)

Install Directory Server and then Access Manager with the existing DIT option. Login to the Access Manager Console and create a group. Edit the users in the group. For example, add users with the filter `uid=*999*`. The resulting list box is empty, and the console does not display any error, information, or warning messages.

Workaround: The group membership must not be greater than the Directory Server search size limit. If the group membership is greater, change the search size limit accordingly.

Add `ContainerDefaultTemplateRole` attribute after data migration (4677779)

In Legacy mode, he user's role does not display under an organization that was not created in Access Manager. In debug mode, the following message is displayed:

```
ERROR: DesktopServlet.handleException()
com.iplanet.portalserver.desktop.DesktopException:
DesktopServlet.doGetPost(): no privilige to execute desktop
```

This error becomes evident after the Java ES installer migration scripts are run. The `ContainerDefaultTemplateRole` attribute is not automatically added to the organization when the organization is migrated from an existing directory information tree (DIT) or from another source.

Workaround: Use the Directory Server console to copy the `ContainerDefaultTemplateRole` attribute from another Access Manager organization and then add it to the affected organization.

Command Line Issue

Organization Admin role is fails to create a new user with the amadmin command line utility (6480776)

An administrator assigned the Organization Admin role is not able to create a new user with the amadmin command line utility due to incorrect logging privileges.

Workaround: Both the Organization Admin and the Top-level admin may set the permissions. To do so through the Administration Console:

1. Go to the organization to which the Organization Admin belongs.
2. Click on the Privileges tab.
3. Click on the Organization Admin Role link.
4. Select `Read and write access to all log files` or `Write access to all log files`.
5. Click Save.

SDK and Client Issues

Clients do not get notifications after the server restarts (6309161)

Applications written using the client SDK (`amclientsdk.jar`) do not get notifications if the server restarts.

Workaround: None.

SDK clients need to restart after service schema change (6292616)

If you modify any service schema, `ServiceSchema.getGlobalSchema` returns the old schema and not the new schema.

Workaround: Restart the client after a service schema change.

This problem is fixed in patch 1.

Authentication Issues

Distributed Authentication UI server performance drops when application user has insufficient privileges (6470055)

When you deploy the Distributed Authentication UI server using the default application user, performance drops significantly due to the default application user's restricted privileges.

Workaround: Create a new user with appropriate privileges.

To create a new user with the proper ACIs:

1. In the Access Manager console, create a new user. For example, create a user named `AuthUIuser`.
2. In Directory Server console , add the following ACI.

   ```
   dn:ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>
   changetype:modifyadd:aci
   aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>")
   (targetattr = "*"(version 3.0; acl "SunAM client data anonymous access";
   allow (read, search, compare) userdn = "ldap:///<AuthUIuser's DN>";)
   ```

   Notice that the `userdn` is set to `"ldap:///<AuthUIuser's DN>"`.
3. See the instructions in the "To Install and Configure a Distributed Authentication UI Server" in *Sun Java System Access Manager 7.1 Postinstallation Guide* for editing the `amsilent` file, and for running the `amadmin` command.

4. In the amsilentfile, set the following properties:

   APPLICATION_USER Enter `AuthUIuser`.

   APPLICATION_PASSWD Enter a password for `AuthUIuser`.

5. Save the file.
6. Run the `amconfig` script using the new configuration file. For example, on a Solaris system with Access Manager installed in the default directory:

   ```
   # cd /opt/SUNWam/bin
   # ./amconfig -s ./DistAuth_config
   ```

7. Restart the web container on the Distributed Authentication UI server.

Incompatibility for Access Manager default configuration of Statistics Service for legacy (compatible) mode (6286628)

After installation with Access Manager in legacy mode, the default configuration for the Statistics Service has changed:

- The service is turned on by default (`com.iplanet.services.stats.state=file`). Previously, it was off.
- The default interval (`com.iplanet.am.stats.interval`) has changed from 3600 to 60.
- The default stats directory (`com.iplanet.services.stats.directory`) has changed from `/var/opt/SUNWam/debug` to `/var/opt/SUNWam/stats`.

Workaround: None.

Attribute uniqueness broken in the top-level organization for naming attributes (6204537)

After you install Access Manager, login as `amadmin` and add the `o`, `sunPreferredDomain`, `associatedDomain`, `sunOrganizationAlias`, `uid`, and `mail` attributes to the Unique Attribute List. If you create two new organizations with the same name, the operation fails, but Access Manager displays the "organization already exists" message rather than the expected "attribute uniqueness violated" message.

Workaround: None. Ignore the incorrect message. Access Manager is functioning correctly.

Session and SSO Issues

- "System creates invalid service host name when load balancer has SSL termination (6245660)" on page 66
- "Using `HttpSession` with third-party web containers " on page 66

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 Service Pack (SP) releases, edit the `servername` attribute as follows:

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

Web Server 6.1 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.example.com:443" defaultvs="https-sample"
security="false" ip="any" blocking="false" acceptorthreads="1"/>
```

Using `HttpSession` with third-party web containers

The default method of maintaining sessions for authentications is "internal session" instead of `HttpSession`. The default invalid session maximum time value of three minutes is sufficient. The `amtune` script sets the value to one minute for Web Server or Application Server. However, if you are using a third-party web container (IBM WebSphere or BEA WebLogic Server) and the optional `HttpSession`, you might need to limit the web container's maximum `HttpSession` time limit to avoid performance problems.

Policy Issues

- "Deletion of dynamic attributes in Policy Configuration Service causing issues in editing of policies (6299074)" on page 66

Deletion of dynamic attributes in Policy Configuration Service causing issues in editing of policies (6299074)

The deletion of dynamic attributes in Policy Configuration Service causes issues in editing of policies for this scenario:

1. Create two dynamic attributes in the Policy Configuration Service.
2. Create a policy and select the dynamic attributes (from Step 1) in the response provider.
3. Remove the dynamic attributes in the Policy Configuration Service and create two more attributes.
4. Try to edit the policy created in Step 2.

Results are: "Error Invalid Dynamic property being set." No policies were displayed in the list by default. After a search is done, the policies are displayed, but you cannot edit or delete the existing policies or create a new policy.

Workaround: Before removing the dynamic attributes from the Policy Configuration Service, remove the references to those attributes from the policies.

Server Startup Issues

Debug error occurs on Access Manager startup (6309274, 6308646)

Access Manager 7.1 startup returns the debug errors in `amDelegation` and `amProfile` debug files:

- `amDelegation`: Unable to get an instance of plug-in for delegation
- `amProfile`: Got Delegation Exception

Workaround: None. You can ignore these messages.

AMSDK Issues

Error displayed when performing AMIdentity.modifyService (6506448)

When using `AMIdentity.modifyService` to set desktop service dynamic attribute on a realm, Access Manager returns a null pointer exception.

Workaround: Add the following property to `AMConfig.properties` and then restart the server.:

```
com.sun.am.ldap.connnection.idle.seconds=7200
```

Group members don't show up in selected list (6459598)

The problem occurs under the following conditions:

1. Define a realm with the following realm configuration:
   - Top-level realm is `amroot`. A subrealm is `example.com`.
   - The subrealm `example.com` has two data stores: `exampleDB` and `exampledminDB`.
   - The data store `exampleDB` contains all the users starting at `dc=example,dc=com`. Supported LDAPv3 operations is set to `user=read,write,create,delete,service`.
   - The data store `exampleadminDB` contains an admin group for the realm. The admin group is `DN: cn=example.com Realm Administrators,ou=Groups,dc=example,dc=com`. This group has a single member, `scarter`. Supported LDAPv3 operations is set to `group=read,write,create,delete`.
2. Click the Subjects tab, then Groups, then the entry for `example.com Realm Administrators`.
3. Click the User tab.

All the users in the `exampleDB` data store show up as available, but `scarter` does not show up in the Selected field.

Workaround: Add the operation `user=read` to the supported LDAPv3 operations in the `exampleadminDB` data store.

Access Manager Login URL Returns Message "No such Organization found" (6430874)

The problem may be due to the use of mixed-case (both uppercase and lowercase) characters in the fully qualified domain name (FQDN).

Example: `HostName.PRC.Example.COM`

Workaround : After installation, do not use the default Access Manager login URL. Instead, in the login URL, include the LDAP location of the default organization. For example:

```
http://HostName.PRC.Example.COM/amserver/UI/Login?org=dc=PRC,dc=Example,dc=COM
```

Once you've successfully logged in to Access Manager, you can eliminate the need to enter the full path to the user's organization each time you log in to Access Manager. Follow these steps:

1. Go to the Realm tab in Realm mode, or go to the Organization tab in Legacy mode.
2. Click the default realm or organization name.

   In this example, click `prc`.
3. Change all uppercase characters in the `Realm/DNS Alias` value to lowercase characters.

   In this example, add the all-lowercase value `hostname.prc.example.com` to the list, and then remove the mixed-case `HostName.PRC.Example.COM` value from the list.
4. Click Save, and log out of Access Manager Console.

You can now log in using any one of the following URLs:

- `http://hostname.PRC.Example.COM/amserver/UI/Login`
- `http://hostname.PRC.Example.COM/amserver`
- `http://hostname.PRC.Example.COM/amserver/console`

Sub-org creation not possible from Access Manager when using `amadmin` (5001850)

This problem occurs when multi-master replication is enabled between two Directory Servers and you attempt to create a sub-organization using the `amadmin` utility.

Workaround: In both Directory Servers, set the `nsslapd-lookthroughlimit` property to -1.

SSL Issue

- "The amconfig script fails when SSL certificate is expired. (6488777)" on page 69

The amconfig script fails when SSL certificate is expired. (6488777)

If the Access Manager container is running in SSL mode, and the container SSL certificate is expired, `amconfig` fails and may cause classpath corruption.

Workaround: If you have already run `amconfig` with an expired certificate, and the classpath is corrupted, first obtain a valid SSL certificate. Revert to the original `domain.xml` file, or a copy of the `domain.xml` file, in which the classpath is not corrupted. Then rerun the `amconfig` command:

```
/opt/SUNWam/bin/amconfig -s $PWD/amsamplesilent
```

Samples Issue

- "Clientsdk samples directory contains unwanted makefile (6490071)" on page 70

Clientsdk samples directory contains unwanted makefile (6490071)

Sample files are included in the Client SDK. These demonstrate how to write stand-alone programs and how to write web applications. The samples are located under the directory where you generated the `Makefile.clientsdk`, and in the following subdirectories:

```
.../clientsdk-samples/

.../clientsdk-webapps/
```

Clientsdk-samples includes samples for authentication, logging, policy and SAML stand-alone programs. Clientsdk-webapps includes samples for user management, service management, and policy programs. Each sample has a Readme.html file with instructions on compiling and running the sample program.

In order to compile the samples, the makefile should be run in the corresponding sub-directory. The Top-level makefile does not compile the samples in the sub-directories.

Linux OS Issues

- "JVM problems occur when running Access Manager on Application Server (6223676)" on page 70

JVM problems occur when running Access Manager on Application Server (6223676)

If you are running Application Server 8.1 on Red Hat Linux, the stack size of the threads created by the Red Hat OS for Application Server is 10 Mbytes, which can cause JVM resource problems when the number of Access Manager user sessions reaches 200.

Workaround: Set the Red Hat OS operating stack size to a lesser value such as 2048 or even 256 Kbytes, by executing the `ulimit` command before you start Application Server. Execute the `ulimit` command on the same console that you will use to start Application Server. For example:

```
# ulimit -s 256;
```

Windows and HP-UX Issues

- "Access Manager auto configuration failed when installing on zh_TW and es locales (6515043)" on page 71
- "HP-UX needs gettext binary with AM while installing Java Enterprise System full stack (6497926)" on page 71

Access Manager auto configuration failed when installing on zh_TW and es locales (6515043)

Workaround: In `zh_TW` and `es` locales on HP-UX platform, Access Manager has to be configured in "Config Later" mode only. Start the JavaES installer, install the Access Manager product and exit the JavaES installer. Then invoke the Access Manager configurator as shown below:

1. `LANG=C`
2. `export LANG`
3. Edit *accessmanager-base*`/bin/amsamplesilent file`
4. Run *accessmanager-base*`/bin/amconfig -s amsamplesilent`

HP-UX needs gettext binary with AM while installing Java Enterprise System full stack (6497926)

There is no current workaround for this problem.

Federation and SAML Issues

Logout error occurs in Federation (6291744)

In realm mode, if you federate user accounts on an identity provider (IDP) and service provider (SP), terminate Federation, and then logout, an error occurs: Error: No sub organization found.

Workaround: None.

Globalization (g11n) Issues

Administration console components displayed in English in the zh locale (6470543)

When setting the browser locale to `zh`, the Administration console components are displayed in English, for example the Version, Help and Logout buttons.

Workaround: Set browser locale setting to `zh-cn` instead of `zh`.

Current Value and New value are incorrectly displayed in the console (6476672)

In the localized version of the Administration console, the labels for the Current Value and New Value attributes are incorrectly displayed as label.current.value and label.new.value, respectively.

Policy condition date must be specified according to English custom (6390856)

Policy condition date format labels under the Chinese locale are not displayed according to Chinese customs. Labels are proposing a date format like English date format. Related fields also accept English date format values.

Workaround: For each field, follow the date format example given in the field label.

Removing UTF-8 is not working in Client Detection (5028779)

The Client Detection function is not working properly. Changes made in the Access Manager 7.1 Console are not automatically propagated to the browser.

Workaround: There are two workarounds:

- Restart the Access Manager web container after you make a change in the Client Detection section.

  or

- Follow these steps in the Access Manager Console:
  1. Click `Client Detection` under the `Configuration` tab.
  2. Click the `Edit` link for `genericHTML`.
  3. Under the HTML tab, click the `genericHTML` link.
  4. Enter the following entry in the character set list: `UTF-8;q=0.5` (Make sure that the UTF-8 `q` factor is lower than the other character sets of your locale.)
  5. Save, logout, and login again.

Multi-byte characters are displayed as question marks in log files (5014120)

Multi-byte messages in log files in the `/var/opt/SUNWam/logs` directory are displayed as question marks (`?`). Log files are in native encoding and not always UTF-8. When a web container instance starts in a certain locale, log files will be in native encoding for that locale. If you switch to another locale and restart the web container instance, the ongoing messages will be in the native encoding for the current locale, but messages from previous encoding will be displayed as question marks.

Workaround: Make sure to start any web container instances always using the same native encoding.

Documentation Issues

Missing information when configuring Access Manager in SSL mode (6660610)

In Chapter 8, "Configuring Access Manager in SSL Mode," in *Sun Java System Access Manager 7.1 Postinstallation Guide*, the documentation fails to mention that the port number is changed from 80 to 443 if configure SSL for Access Manager with a secure WebServer and did not select the "Enable SSL" checkbox during installation.

Access Manager supports non-ascii character passwords if Directory Server is configured to support them (6661374)

Access Manager supports non-ascii characters in password fields only if the Directory Server is configured to support them. The Sun Java System Directory Server 7-Bit check plug-in should be disabled to let non-ascii characters to be stored. This flag, by default, is enabled in Directory Server 5.2 and should be disabled if non-ascii characters are needed to be entered in the `userPassword` entery. The 7-Bit Check Plug-in is disabled by default in Directory Server versions 6.0 and above.

Document the roles and filtered roles support for LDAPv3 plug-in (6365196)

After applying the respective patch, you can configure roles and filtered roles for the LDAPv3 plug-in, if the data is stored in Sun Java System Directory Server (fixes problem ID 6349959). In the Access Manager 7.1 Administration console, in LDAPv3 configuration for the "LDAPv3 Plug-in Supported Types and Operations" field, enter the values as:

```
role: read,edit,create,delete
filteredrole: read,edit,create,delete
```

You can enter one or both of the above entries, depending on the roles and filtered roles you plan to use in your LDAPv3 configuration.

Document unused properties in the `AMConfig.properties` file (6344530)

The following properties in the `AMConfig.properties` file are not used:

```
com.iplanet.am.directory.host
com.iplanet.am.directory.port
```

Document how to enable XML encryption (6275563)

To enable XML encryption for either Access Manager or Federation Manager using the Bouncy Castle JAR file to generate a transport key, follow these steps:

1. If you are using a JDK version earlier than JDK 1.5, download the Bouncy Castle JCE provider from the Bouncy Castle site (`http://www.bouncycastle.org/`). For example, for JDK 1.4, download the `bcprov-jdk14-131.jar` file.
2. If you downloaded a JAR file in the previous step, copy the file to the *jdk_root*`/jre/lib/ext` directory.
3. For the domestic version of the JDK, download the JCE Unlimited Strength Jurisdiction Policy Files from the Sun site (`http://www.oracle.com/technetwork/java/index.html`) for your version of the JDK. For IBM WebSphere, go to the corresponding IBM site to download the required files.
4. Copy the downloaded `US_export_policy.jar` and `local_policy.jar` files to the *jdk_root*`/jre/lib/security` directory.
5. If you are using a JDK version earlier than JDK 1.5, edit the *jdk_root*`/jre/lib/security/java.security` file and add Bouncy Castle as one of the providers. For example:

   ```
   security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
   ```
6. Set the following property in the `AMConfig.properties` file to true:

```
com.sun.identity.jss.donotInstallAtHighestPriority=true
```

7. Restart the Access Manager web container.

For more information, refer to problem ID 5110285 (XML encryption requires Bouncy Castle JAR file).

Documentation Updates

Access Manager 7.1 Documentation Collection

The Access Manager 7.1 documentation is available in the following collection:

`http://docs.sun.com/coll/1292.2`

Support for the Java SecurID Authentication Module

SecurID has been converted to a Java-based authentication module and is supported on the following platforms:

- Solaris SPARC and x86 systems beginning with Access Manager 7.1 patch 2 (CR 6621802).
- Linux systems beginning with Access Manager 7.1 patch 3 (CR 6767780).

Previously, you had to start the SecurID authentication process (`amsecuridd`) manually. Now, the SecurID authentication process runs similar to the other authentication modules, fully-contained within the Access Manager 7.1 server process.

The Java version of SecurID requires the following files:

- `authapi.jar` (SecurID API) in the following directory:
  - WAR file deployment: `WEB-INF/lib` directory
  - Installer (package-based) deployment: *AccessManager-base*`/SUNWam/lib`
- `log4j.properties`, `rsa_api.properties`, and `sdconf.rec` files in the default `/opt/ace/data` directory.

To configure a SecurID authentication module:

1. Log in to the Access Manager 7.1 Administration console.

2. Under Access Control, click *realm-name* and then Authentication.
3. Under Module Instances, click New and add a New Module Instance with Type as SecurID.
4. Configure the following SecurID Realm Attributes:
   - ACE/Server Configuration Path. Default is `/opt/ace/data`.
   - Helper Configuration Port. Default is `58943`.
   - Helper Authentication Port. Default is `57943`.
   - Authentication Level. Default is `0` (zero).
5. Save your configuration and log out of the console.
6. Restart the Access Manager web container.

Access Manager in an Application Server Cluster

A new document entitled Chapter 1, "Technical Note: Deploying Access Manager Instances to an Application Server Cluster," in *Technical Note: Deploying Access Manager to an Application Server Cluster* has been added to the Access Manager 7 2005Q4 collection.

Policy Agent 2.2 Collection

The Sun Java System Access Manager Policy Agent 2.2 collection has also been revised to document new agents:

`http://docs.sun.com/coll/1322.1`

Redistributable Files

Sun Java System Access Manager 7.1 does not contain any files that you can redistribute to non-licensed users of the product.

System Virtualization Support

System virtualization is a technology that enables multiple operating system (OS) instances to execute independently on shared hardware. Functionally, software deployed to an OS hosted in a virtualized environment is generally unaware that the underlying platform has been virtualized. Sun performs testing of its Sun Java System products on select system virtualization and OS combinations to help validate that the Sun Java System products continue to function on properly sized and configured virtualized environments as they do on non-virtualized

systems. For information about Sun support for Sun Java System products in virtualized environments, see *System Virtualization Support in Sun Java Systems Products* in http://docs.sun.com/coll/1292.2.

How to Report Problems and Provide Feedback

If you have problems with Access Manager or Sun Java Enterprise System, contact Sun customer support using one of the following mechanisms:

- Sun Support Resources (SunSolve) services at http://sunsolve.sun.com/.

  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. Go to http://docs.sun.com/ and click Send Comments.

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 the *Access Manager Release Notes* is 819-4683-24.

Additional Sun Resources

You can find useful Access Manager information and resources at the following locations:

- Sun Java Enterprise System Documentation: http://docs.sun.com/prod/entsys.05q4
- Oracle Services: http://www.oracle.com/us/support/systems/advanced-customer-services/index.html
- Oracle Software Products: http://www.oracle.com/us/sun/sun-products-map-075562.html
- Support Resources http://sunsolve.sun.com/
- Oracle Technology Network: http://www.oracle.com/technetwork/index.html
- Sun Developer Support Services: http://developers.sun.com/services/

Accessibility Features for People With Disabilities

For information about Oracle's commitment to accessibility, visit http://www.oracle.com/us/corporate/accessibility/index.htm.

Related Third-Party Web Sites

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

Note – Oracle is not responsible for the availability of third-party Web sites mentioned in this document. Oracle 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. Oracle 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.
