Sun Java System Access Manager 7 2005Q4 Release Notes

Part No: 819–2134–28
November 9, 2010

ORACLE

Copyright © 2010, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

101109@24999

Contents

Sun Java System Access Manager 7 2005Q4 Release Notes

November 9, 2010

Part Number 819-2134-28

The Sun Java System Access Manager (Access Manager) 7 2005Q4 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.

For information in this edition of the Release Notes, see the "Revision History" on page 8.

To view the Java ES product documentation, including the Access Manager collection, see `http://docs.sun.com/prod/entsys.05q4`.

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

Contents

The Access Manager 7 2005Q4 Release Notes contain the following sections:

Revision History

The following table shows the Access Manager 7 2005Q4 Release Notes revision history.

TABLE 1 Revision History

Date	Description of Changes
November 9, 2010	■ Added information about patch 12 in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section. ■ Revised outdated URLs.
May 10, 2010	Revised "CR# 6564877: Access Manager 7 patch installation overwrites SAML v2 files" on page 24.
December 15, 2009	Added information about patch 11 in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section.
August 7, 2009	Added information about patch 10 in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section.
February 27, 2009	Added information about patch 9 in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section.
November 5, 2008	Added information about patch 8 in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section.
August 19, 2008	Added information about patch 7 for Windows and HP-UX systems in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section.
May 12, 2008	■ Added information about patch 7 in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section. ■ Added the "System Virtualization Support" on page 76 section.
October 16, 2007	Changes for this revision include: ■ Added information about patch 6 in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section. ■ Updated "CR# 6522720: Search in console online help does not work for multibyte characters on Windows and HP-UX systems" on page 50. Patch 6 fixes this problem on Windows systems. However, the problem still exists on HP-UX systems.

TABLE 1 Revision History *(Continued)*

Date	Description of Changes
July 10, 2007	Changes for this revision include: ■ Added information about patch 126371-05 for HP-UX systems in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section. ■ Added the following new issue: "Null attribute LDAP search returns an error when Access Manager points to Directory Proxy (6357975)" on page 92.
March 16, 2007	Changes for this revision include: ■ Added information about patch 5 in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section. ■ Added clarifications and new information under "Documentation Issues" on page 101. ■ Made various other technical and editorial changes from reviewers and Change Requests (CRs).
October 30, 2006	Changes in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section include: ■ Added information about patch 4. ■ Corrected the inconsistent use of *AccessManager-base*. ■ Revised the description for "CR# 6440651: Cookie replay requires `com.sun.identity.session.resetLBCookie` property" on page 59.
August 25, 2006	Changes in the "Access Manager 7 2005Q4 Patch Releases" on page 11 section include: ■ Added information about patch 3. ■ Revised and added new information about patches 1 and 2.

May 25, 2006	Changes for this revision include:
	■ Added the new "Access Manager 7 2005Q4 Patch 2" on page 62 section.
	■ Added information about support for the HP-UX and Microsoft Windows platforms in Table 4.
	■ Added the following issues under "Documentation Issues" on page 101:
	  ■ "Release Notes have wrong workaround for known issue (6422907)" on page 106
	  ■ "Document `com.iplanet.am.session.protectedPropertiesList` in `AMConfig.properties` (6351192)" on page 106

TABLE 1 Revision History *(Continued)*

Date	Description of Changes
February 9, 2006	Revised "Documentation Updates" on page 108 to list the new and revised Access Manager 7 2005Q4 documents that have been published since the initial release.
February 7, 2006	Changes for this revision include: ■ Added the following issues under "Known Issues and Limitations" on page 79: ■ "Authentication service is not initialized when Access Manager and Directory Server are installed on separate machines (6229897)" on page 83 ■ "Access Manager `ampre70upgrade` script does not remove localized packages (6378444)" on page 84 ■ Updated the "Documentation Updates" on page 108 section.
January 18, 2006	Changes for this revision include: ■ Added the new "Access Manager 7 2005Q4 Patch 1" on page 67 section. ■ Clarified the description of "Distributed Authentication" on page 71. ■ Clarified the support for Solaris 10 zones and added support for Solaris 10 OS on AMD64 platforms in "Hardware and Software Requirements" on page 74. ■ Added the following issues under "Known Issues and Limitations" on page 79: ■ "URL signing failed in IBM WebSphere when using RSA key (6271087)" on page 88 ■ "JVM problems occur when running Access Manager on Application Server (6223676)" on page 97 ■ "Running the web services sample returns "Resource offering not found" (6359900)" on page 98 ■ "After applying patch 1, `/tmp/amsilent` file allows read access for all users (6370691)" on page 82 ■ "Add `ContainerDefaultTemplateRole` attribute after data migration (4677779)" on page 86 ■ "Document the roles and filtered roles support for LDAPv3 plug-in (6365196)" on page 107 ■ "Document unused properties in the `AMConfig.properties` file (6344530)" on page 107 ■ "Document how to enable XML encryption (6275563)" on page 108 ■ Added the new "Documentation Updates" on page 108 section.

TABLE 1 Revision History *(Continued)*

Date	Description of Changes
November 8, 2005	Revised the "Identity Repository" on page 69 for the supported LDAP version 3 (LDAP v3) compliant repositories.
October 3, 2005	Initial release.
June 30, 2005	Beta release.

About Sun Java System Access Manager 7 2005Q4

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 2005Q4 Patch Releases

The latest revisions of the Access Manager 7 2005Q4 patches are available for download from SunSolve Online: `http://sunsolve.sun.com`. The most recent patch IDs are:

- Solaris Operating System (Solaris OS) on SPARC based systems: 120954-12
- Solaris OS on x86 platforms: 120955-12
- Linux systems: 120956-12
- Microsoft Windows systems: 124296-12
- HP-UX systems: 126371-12

Note – Patch 12 is the last patch for Sun Java System Access Manager 7 2005Q4. For more information, see the "Lifetime Support Policy: Oracle Fusion Middleware Products" at `http://www.oracle.com/us/support/library/lifetime-support-middleware-069163.pdf`.

Access Manager 7 2005Q4 patches are cumulative. You can install a 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 2005Q4 patches includes:

Access Manager 7 2005Q4 Patch 12

Access Manager 7 patch 12 (revision 12) fixes a number of problems, as listed in the README file included with the patch. Patch 12 also includes these issues and changes:

CR# 6916733: `updateschema` script checks for LDAP JDK version 4.21 or later

Access Manager 7 patch 9 and later requires LDAP JDK (`ldapjdk.jar`) version 4.21 or later.

With patch 12, the `updateschema.sh` or `updateschema.pl` script checks the LDAP JDK version. If the version is older than 4.21 or not defined, the script displays a message that you should install the latest LDAP JDK patch.

For security reasons, it is highly recommended that you download and install the latest LDAP JDK patch from SunSolve Online (`http://sunsolve.sun.com/`), depending on your specific platform:

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

CR# 6770231: Access Manager 7 Patch 12 validates `goto` URLs

After installing patch 12, Access Manager 7 2005Q4 server can validate a `goto` URL after a user logs in. This fix prevents a hacker from sending the user to an imposter site in order to steal the user's personal information.

To set valid `goto` URLs, follow these steps:

1. After you install patch 12, make sure you run the `updateschmema.sh` or `updateschema.bat` script and then restart the Access Manager web container.
2. Log in to the Access Manager Administration Console.
3. Click Configuration, Authentication, and then Core.
4. Under Valid `goto` URL domains, add each valid goto domain name, as follows:
   - A domain name starting with a dot (.) such as `.example.com` allows all hosts in the `example.com` domain to be used in a success redirect URL.
   - A domain name that does not start with a dot (.) such as `example.com` allows the host `example.com` to be used in a success redirect URL. For example, `http://example.com` would be valid, but `http://host.example.com` would not be valid.
   - If you don't add the entire domain to the list, you must add each individual agent host name being used.
   - You do not need to add domains for agents in CDSSO mode, because they are protected automatically.
5. Click Save.
6. Restart the Access Manager web container.

If you subsequently want to disable the `goto` URL validation, remove all entries from the Valid `goto` URL domains list. If a `goto` URL is found to be invalid, the user will be redirected to the default success login URL.

CR# 6926203 Distributed Authentication UI server deployment validates `goto` URLs

In a Distributed Authentication UI (DAUI) server deployment, Access Manager 7 patch 12 validates `goto` URLs on the DAUI server side. This fix is similar to the Access Manager server side fix described previously in CR 6770231. The DAUI server reads the valid domain list from Access Manager server and does not maintain its own list. After you install patch 12, make sure you restart the DAUI server.

Pre-Installation Considerations

Backing Up Files

Important If any of the files in your current installation are customized, back up those files before you install the patch. After you install the patch, compare the backed up files with the new files installed by this patch to identify the customizations. Merge the customizations with the new files and save them. For more information about how to handle customized files, read the following information.

Before you install a patch, also back up the following files.

Solaris Systems	■ *AccessManager-base*/SUNWam/bin/amsfo ■ *AccessManager-base*/SUNWam/lib/amsfo.conf ■ Files in the /etc/opt/SUNWam/config/xml/template/ directory: idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml, amAuth.xml, amSession.xml ■ Files in the *AccessManager-base*/SUNWam/locale/ directory: amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties

Linux and HP-UX Systems	■ *AccessManager-base*/identity/bin/amsfo ■ *AccessManager-base*/identity/lib/amsfo.conf ■ Files in the /etc/opt/sun/identity/config/xml/template/ directory: idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml, amAuth.xml, amSession.xml ■ Files in the *AccessManager-base*/identity/locale/ directory: amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties
Windows Systems	■ *AccessManager-base*\identity\setup\AMConfigurator.properties ■ *AccessManager-base*\identity\bin\amsfo ■ *AccessManager-base*\identity\lib\amsfo.conf ■ Files in the *AccessManager-base*\identity\config\xml\template directory: idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml, amAuth.xml, amSession.xml ■ Files in the *AccessManager-base*\identity\locale directory: amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties

AccessManager-base is the base installation directory. The default base installation directory depends on the platform:

- Solaris systems: /opt
- Linux and HP-UX systems: /opt/sun
- Windows systems: *javaes-install-directory*\AccessManager. For example: C:\Program Files\Sun\AccessManager

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 2005Q4 must be installed on the server. For information about installation, see the *Sun Java Enterprise System 2005Q4 Installation Guide for UNIX*.

If you are installing the patch on a Windows system, see the *Sun Java Enterprise System 2005Q4 Installation 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 1, "Access Manager 7 2005Q4 Configuration Scripts," in *Sun Java System Access Manager 7 2005Q4 Administration 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

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 14.

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/120954-12
```

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/120954-12
```

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`
- Linux systems: *AccessManager-base*`/identity`

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.

After you run the `amconfig` script, execute the `updateschema.sh` script to load the XML and LDIF files. The `updateschema.sh` script is available after you install patch 11 in the following directory:

- Solaris SPARC systems: *patch-home-directory*/120954-09
- Solaris x86 systems: *patch-home-directory*/120955-09

After you run the `updateschema` script, restart the Access Manager processes. For example:

```
# cd /opt/SUNWam/bin
# ./amserver stop
# ./amserver start
```

Then, restart the Access Manager web container.

patchrm Command

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

```
# patchrm 120954-03
```

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.

See also "Post-Installation Considerations" on page 21 for more information.

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 2005Q4 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 2005Q4 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 120954-09
```

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 14.

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.

After you run the `amconfig` script, execute the `updateschema.sh` script (patch 5 and later patches) to load the XML and LDIF files. The `updateschema.sh` script is available after you install patch 11 in the *patch-home-directory*`/120956-09/scripts` directory.

After you run the `amconfig` and `updateschema.sh` scripts, restart the Access Manager web container.

If the patch is installed on the Access Manager 7 2005Q4 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_AM7_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.

See also "Post-Installation Considerations" on page 21 for more information.

Patch Installation Instructions For Windows Systems

The requirements to install the Windows patch include:

- Access Manager 7 2005Q4 must be installed on the Windows system. For information about installation, see the *Sun Java Enterprise System 2005Q4 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 14.

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: `AM7p8`
3. Download and unzip the `124296-09.zip` file in the directory from the previous step.
4. Stop all Java ES 2005Q4 services.
5. Run the `AM7p8\scripts\prepatch.pl` script.
6. Run `AM7p8\124296-09.exe` to install the patch.
7. Run the `AM7p8\scripts\postpatch.pl` script.
8. Restart the Java ES 2005Q4 services.
9. Redeploy the Access Manager applications. See "Post-Installation Considerations" on page 21 for more information.
10. Run the `AM7p8\scripts\updateschema.pl` script to update the Directory Server service schema. The script validates your entries and then loads the files. The script also writes the following log file:

    javaes-install-directory`\AccessManager\AM70Patch-upgrade-schema-`*timestamp*
11. Restart the Java ES 2005Q4 services.

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_124296-09.bat` file.
3. Run the `AM7p8\scripts\postbackout.pl` script.
4. Redeploy the Access Manager applications.
5. Restart the Java ES 2005Q4 services.

Note: If you back out the patch, the schema changes added by the `AM7p8\scripts\updateschema.pl` script are not removed from Directory Server. However, you do not need to remove these schema changes manually because they will not affect Access Manager functionality or usability after the patch is backed out.

Patch Installation Instructions For HP-UX Systems

To install or remove the HP-UX patch, use the `swinstall` and `swremove` commands. For example, to install the patch to a standalone system:

```
# swinstall /var/spool/patch/126371-09
```

Or, to remove the patch from a standalone system:

```
# swremove 126371-09
```

For information about the `swinstall` and `swremove` commands, refer to the `swinstall` and `swremove` man pages.

After you install or remove the patch, you must re-deploy the Access Manager applications as described in the "Post-Installation Considerations" on page 21 section.

After you re-deploy the Access Manager applications, execute the `updateschema.sh` script (patch 5 and later patches) to load the XML and LDIF files. The `updateschema.sh script` is available after you install patch 11 in the *patch-home-directory*`/120956-09/scripts` directory. After you run the `amconfig` and `updateschema.sh` scripts, restart the Access Manager web container.

Note: If you remove the patch, the schema changes added by the `updateschema.sh` script are not removed from Directory Server. However, you do not need to remove these schema changes manually because they will not affect Access Manager functionality or usability after the patch is removed.

For more information about deploying Access Manager on HP-UX systems, see the *Sun Java System Access Manager 7 2005Q4 Release Notes for HP-UX*.

Post-Installation Considerations

Considerations after you install an Access Manager 7 2005Q4 patch include:

CR# 6254355: Access Manager patches do not deploy Access Manager applications in postpatch scripts

The patch installer might not preserve some of the customized WAR files, replacing them with non-customized versions. To help you identify and then manually update the customized contents of a WAR file, consider the following procedure.

In the following examples, *AccessManager-base* is the base installation directory. The default base installation directory is `/opt` on Solaris systems and `/opt/sun` on Linux systems.

On Windows systems, *AccessManager-base* is *javaes-install-directory*`\AccessManager`. For example: `C:\Program Files\Sun\AccessManager`

The WAR files that get patched are:

- `console.war`
- `password.war`
- `services.war`

These files are located in *AccessManager-base*`/SUNWam` on Solaris systems and *AccessManager-base*`/identity` on Linux systems.

On Windows systems: the WAR files that get patched are located in *AccessManager-base*`\`.

The changeable content in a WAR file includes:

- Properties files:
  - Solaris systems: *AccessManager-base*`/SUNWam/locale/*.properties`
  - Linux systems: *AccessManager-base*`/identity/locale/*.properties`
  - Windows systems: *AccessManager-base*`\locale\*.properties`
- Tag library descriptors:
  - Solaris systems: *AccessManager-base*`/SUNWam/web-src/applications/WEB-INF/*.tld`
  - Linux systems: *AccessManager-base*`/identity/web-src/applications/WEB-INF/*.tld`
  - Windows systems: *AccessManager-base*`\web-src\applications\WEB-INF\*.tld`
- The `web.xml` file and the files used to construct it (`WEB-INF/web.xml` and `WEB-INF/*.xml`)
- Application specific files: JSP (`*.jsp`) files, images (`*.gif`) files, and style sheets - background colors, font sizes, etc. (`*.css`) files

To make sure that all custom changes are preserved, follow these steps. Before you make changes to a file, always backup the file first.

1. Install the patch.
2. Expand the WAR files into a temporary directory. For example, with Access Manager installed in the default directory on Solaris systems:

   ```
   # cd temporary-directory
   # jar -xvf /opt/SUNWam/console.war
   # jar -xvf /opt/SUNWam/services.war
   # jar -xvf /opt/SUNWam/password.war
   ```
3. Check the expanded files to see whether the patch installer made any changes to your customized files and manually add your original custom changes to the ones that got changed in the temporary directory. For your changes to the files under the *AccessManager-base*`/web-src/` directory but not included in the patched WAR files, you do not need to redo your changes.
4. Update the WAR files with the modified files. For example, with Access Manager installed in the default directory on Solaris systems:

   ```
   # cd temporary-directory
   # jar -uvf /opt/SUNWam/console.war $path/$modified file
   # jar -uvf /opt/SUNWam/services.war $path/$modified file
   # jar -uvf /opt/SUNWam/password.war $path/$modified file
   ```

For example, for Steps 2-4:

```
# mkdir /tmp/war.tmp
# cd /tmp/war.tmp
# jar -xvf /opt/SUNWam/services.war
# vi index.html
# jar -uvf /opt/SUNWam/services.war index.html
```

5. Reuse the silent configuration file (`amsilent`) generated by the patch or create a new one based on the `amsamplesilent` template file, and then set the appropriate configuration variables in the file, including:

   - `DEPLOY_LEVEL=21`
   - `DIRECTORY_MODE=5`
   - Passwords for `DS_DIRMGRPASSWD`, `ADMINPASSWD`, and `AMLDAPUSERPASSWD`
   - Access Manager Web container variables

   On Windows systems, reuse the silent configuration file (`amsilent`) generated by the `postpatch.pl` script and make sure that *AccessManager-base*`\setup\AMConfigurator.properties-tmp` has valid values. Then rename this file to *AccessManager-base*`\setup\AMConfigurator.properties`.

   For more information about the Web container variables, see the `amsamplesilent` file in the `/opt/SUNWam/bin` directory on Solaris systems or the `/opt/sun/identity/bin` directory on Linux systems.

   On Windows systems, the configuration file is *AccessManager-base*`\setup\AMConfigurator.properties`.

6. Run the `amconfig` script as shown below. Before you run `amconfig`, Directory Server and the Access Manager Web container must be running. For example, to run `amconfig` on a Solaris system, with Access Manager installed in the default base installation directory:

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

7. After you run the `amconfig` script, restart the Access Manager processes. For example:

   ```
   # cd /opt/SUNWam/bin
   # ./amserver stop
   # ./amserver start
   ```

8. Make sure all your customized JSP files reside in the proper subdirectories under the *AccessManager-base*`/SUNWam/web-src/` directory on Solaris systems or the *AccessManager-base*`/identity/web-src/` on Linux systems, and that you have backed up all of your customized files.

   On Windows systems, the files are in *AccessManager-base*`\web-src\`.

9. Restart the Access Manager Web container.

For more information about running the `amconfig` script, see the: Chapter 1, "Access Manager 7 2005Q4 Configuration Scripts," in *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

CR# 6436409: Redeploying the Distributed Authentication and Client SDK WAR Files

If you are using Distributed Authentication or the Client SDK, recreate and redeploy the Distributed Authentication WAR file and/or the Client SDK WAR file after you install the patch. For information, see the following documents:

- Building the Distributed Authentication WAR file: *Technical Note: Using Access Manager Distributed Authentication*
- Building the Client SDK WAR file: "Installing the Client SDK" in *Sun Java System Access Manager 7 2005Q4 Developer's Guide*
- Deploying the Client SDK WAR file: "To Deploy amclientwebapps.war" in *Sun Java System Access Manager 7 2005Q4 Developer's Guide*

Access Manager 7 2005Q4 Patch 11

Access Manager 7 patch 11 (revision 11) fixes a number of problems, as listed in the README file included with the patch. Patch 11 also includes these issues and changes:

CR# 6564877: Access Manager 7 patch installation overwrites SAML v2 files

If the SAML v2 plug-in is installed and you install a new SAML v2 plug-in patch or Access Manager 7 patch, the patch installation overwrites the existing SAML v2 related files, and you must reconfigure your SAML v2 deployment.

Workaround: Run the `saml2setup` installer with the `update` option to update a previously configured staging directory with new files from a patch installation directory and to regenerate a modified WAR file for redeployment. The `update` option prevents the unconfigure and configure routine, which removes your existing SAML v2 files.

Note: The `saml2setup` installer with the `update` option is available in the SAML v2 Plug-in for Federation Services patch 1 or later. Therefore, you must add the SAML v2 plug-in patch 1 or later to use this option. Although the `update` option was first available in patch 1, Oracle recommends that you always install the latest patch. The patch IDs are:

- Solaris SPARC systems: 122983
- Solaris x86 systems: 122984
- Linux: 122985

To use the `saml2setup` installer with the `update` option, follow these steps:

1. Install the new Access Manager or SAML v2 patch.
2. If you installed an Access Manager patch in Step 1:
   a. Run `amconfig` to generate a new `amserver.war`.
   b. Update the SAML v2 staging directory with the new `amserver.war`.
   c. Reapply any necessary customizations for your deployment.
3. Run the `saml2setup` installer with the `update` option as follows:

   `saml2setup update -s` *installation-configuration-properties-file*
4. Redeploy the modified WAR file.
5. Restart the Access Manager or Federation Manager web container.
6. Do any postinstallation tasks required for the Access Manager or Federation Manager instance.

For information about the `saml2setup` installer, see Chapter 2, "Installing the SAML v2 Plug-in for Federation Services," in *Sun Java System SAML v2 Plug-in for Federation Services User's Guide*.

CR# 6872718: Persistent XSS attacks are prevented in Access Manager

Patch 11 prevents potential persistent cross-site scripting (XSS) attacks in Access Manager.

CR# 6843487: Access Manager session cookies can be marked as `HTTPOnly`

Patch 11 includes the new `com.sun.identity.cookie.httponly` property to allow 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 avoid cross site scripting (XSS) attacks.

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

Access Manager 7 2005Q4 Patch 10

Access Manager 7 patch 10 (revision 10) fixes a number of problems, as listed in the README file included with the patch.

Security Fixes. Patch 10 includes several important security fixes. Oracle recommends that you install patch 10 to prevent from being exposed to these security risks. Refer to the patch README file for a list of these fixes.

Patch 10 also includes these changes:

CR# 6813339: Access Manager reregisters Notification URL after a restart

Access Manager now reregisters the notification URL after a server restart if the following property is set in the server's `AMConfig.properties` file:

```
com.sun.identity.agents.reregisterNotificationUrls=true
```

The default value for this property is `false`. In a multi-server deployment, set this property for each Access Manager server.

CR#6804391 and CR#6777889 Access Manager SecurID authentication process no longer crashes

On Solaris SPARC systems, the SecurID authentication process (`amsecuridd`) now avoids crashes because the process no longer writes to a closed connection. These CRs also fix a problem that caused users to be denied access even when authentication was successful. Also, more debug messages are added for better analysis in case other `amsecuridd` process problems occur.

Access Manager 7 2005Q4 Patch 9

Access Manager 7 patch 9 (revision 09) fixes a number of problems, as listed in the README file included with the patch.

Access Manager 7 2005Q4 Patch 8

Access Manager 7 patch 8 (revision 08) fixes a number of problems, as listed in the README file included with the patch. Patch 8 also includes these changes:

CR# 6668882: Cannot access Console that was installed with upper and lower case characters in domain name

If Access Manager is installed with a domain name that contains both upper and lowercase characters, you cannot log in to the Console. For example, if the domain name is `amhost.`*realm-name*`.Example.COM`, you cannot log in using `amhost.`*realm-name*`.example.com`.

Workaround. There are two workarounds:

First, try logging in using the following URL:

`http://amhost.`*realm-name*`.example.com:port/amserver/UI/Login?realm=`*realm-name*

Or, add the *realm-name* to the Realm/DNS aliases:

1. In the Admin Console, go to Realms, Edit Realm - *realm-name*.
2. Add `amhost.`*realm-name*`.example.com` to the Realm/DNS aliases.
3. Restart the Access Manager server.
4. Log in using the following URL:

   `http://amhost.`*realm-name*`.example.com:port/amserver/UI/Login`

CR# 6691106: Multiple SiteMonitor threads could be running for checking the same site

The `amNaming` log sometimes indicates multiple SiteMonitor threads running for checking the same site.

To prevent this problem, patch 8 provides improved synchronization to prevent the creation of the multiple SiteMonitor threads for the same site. Patch 8 also includes these new configuration properties:

- `com.sun.identity.urlchecker.retry.interval` specifies the time interval in milliseconds between retries for a URL connection. Default is 500 milliseconds (0.5 seconds).
- `com.sun.identity.urlchecker.retry.limit` specifies the maximum number of retries for the URL connection if a connection failure occurs. Default is 3 retries.

The fix for this problem also uses the following property, which was added for patch 5:

- `com.sun.identity.urlchecker.sleep.interval` specifies the time interval in milliseconds that the site status check should sleep. Default is 30000 milliseconds (30 seconds).

The patch does not add these new properties to the `AMConfig.properties` file. To use these properties with values other than the default values:

1. For each property that you want to set, add the property and its value to the `AMConfig.properties` file.
2. Restart the Access Manager web container for the values to take effect.

CR# 6697260: New property to set policy agent application session idle timeout

Patch 8 includes this new property:

- `com.iplanet.am.session.agentsessionidletime` sets the maximum idle timeout in minutes for policy agent sessions. The minimum value is 30 minutes.

By default, policy agent sessions never expire unless you set this property. To use this new property, add it with the maximum idle timeout value to the `AMConfig.properties` file and restart the Access Manager web container.

CR# 2151598: Delegation privileges cannot be defined for a filtered role

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

Workaround. After you apply patch 8, 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 Admin Console, the filtered role will appear under the Privileges tab.

Access Manager 7 2005Q4 Patch 7

Access Manager 7 patch 7 (revision 07) fixes a number of problems, as listed in the README file included with the patch.

Patch 7 includes these changes:

- "CR# 6637806: After restart, Access Manager sent an invalid application SSO token to an agent" on page 29
- "CR# 6612609: Session failover works if network cable is disconnected from Message Queue server" on page 30
- "CR# 6570409: Interaction service behind load balancer works correctly as Identity Provider" on page 30
- "CR# 6545176: Redirect URLs can be dynamically set in post authentication processing SPI plug-in" on page 30

CR# 6637806: After restart, Access Manager sent an invalid application SSO token to an agent

After an Access Manager server restart, the Access Manager client SDK now sends a meaningful exception to an agent, so the agent can re-authenticate itself to get a new application session. Previously, after applying Access Manager 7 2005Q4 patch 5, the Access Manager client SDK sent a invalid application SSO token to the agent after an Access Manager server restart.

This problem has been fixed by duplicate CR 6496155. Patch 7 also provides an option (`comp.iplanet.dpro.session.dnRestrictionOnly` property) to send the application SSO token in a restrictive context. By default, agents send the IP address of the server where they are installed, but if strict DN checking is required, set this property in the `AMConfig.properties` file as follows:

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

CR# 6612609: Session failover works if network cable is disconnected from Message Queue server

In a session failover deployment, if each Access Manager instance and Message Queue broker are installed on the same server, session failover now works if a network cable is disconnected from one of the servers. By default the Message Queue `imqAddressListBehavior` connection factory attribute is set to `PRIORITY`, which causes Message Queue to try addresses in the order in which they appear in the broker address list (for example: `localhost:7777,server2:7777,server3:7777`). If the attribute is set to `RANDOM`, the addresses are tried in random order.

To set this attribute to RANDOM, set the following parameter in the `amsessiondb` script:

```
-DimqAddressListBehavior=RANDOM
```

For information about the Message Queue `PRIORITY` and `RANDOM` attributes, see "Broker Address List" in *Sun Java System Message Queue 3.7 UR1 Administration Guide*.

CR# 6570409: Interaction service behind load balancer works correctly as Identity Provider

In a deployment with two servers connected with a load balancer and functioning as a single Identity Provider, you must set the following properties in the `AMConfig.properties` file:

```
com.sun.identity.liberty.interaction.lbWspRedirectHandler
com.sun.identity.liberty.interaction.trustedWspRedirectHandlers
```

The `com.sun.identity.liberty.interaction.interactionConfigClass` is the only class currently supported. Thus, by default, the interaction configuration class bundled with Federation Liberty is used to access the interaction configuration parameters.

CR# 6545176: Redirect URLs can be dynamically set in post authentication processing SPI plug-in

Redirect URLs can now be dynamically set in post authentication processing SPI plug-ins for login success, login failure, and logout. If a post processing plug-in is not executed, the redirect URL set in the post processing SPI is not used, and redirect URLs set by any other means will be executed as before.

For information, see the `com.iplanet.am.samples.authentication.spi.postprocess.ISAuthPostProcessSample.java` sample.

Access Manager 7 2005Q4 Patch 6

Access Manager 7 patch 6 (revision 06) fixes a number of problems, as listed in the README file included with the patch. Patch 6 also includes the following new features, issues, and documentation updates.

New Features in Patch 6

Known Issues and Limitations in Patch 6

Note – Before you install patch 6, it is recommended that you upgrade or patch the following components:

- If you are using Sun Java System Web Server 6.1 SP5 or earlier, upgrade to Web Server 6.1 SP7, which you can download from this site:

  `http://www.sun.com/download/products.xml?id=45c90ca9`

  Follow the upgrade process as described in "Upgrade" in *Sun Java System Web Server 6.1 SP7 Release Notes*.
- Download and install the latest security patch for NSS, JSS, and NSPR from SunSolve Online: `http://sunsolve.sun.com`.
  - Solaris 8 SPARC platforms: 119209
  - Solaris 8 x86 platforms: 119210
  - Solaris 9 SPARC platforms: 119211
  - Solaris 9 x86 platforms: 119212
  - Solaris 10 SPARC platforms: 119213
  - Solaris 10 x86 and AMD64 platforms: 119214
  - Windows systems: 124392
  - HP-UX systems: 124379

Access Manager supports the JDK 1.5 `HttpURLConnection` `setReadTimeout` method

To support the `setReadTimeout` method, the `AMConfig.properties` file has the following new property for you to set the read time-out 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.

Access Manager SDK falls back to primary Directory Server after primary comes back up

If Sun Java System Directory Server is configured for multi-master replication (MMR), the Access Manager SDK now falls back to the primary Directory Server after the primary server goes down and then comes back up. Previously, the Access Manager SDK continued to access the secondary Directory Server even after the primary server came back up.

To support this new behavior, Access Manager has the following new property in the `AMConfig.properties` file:

```
com.sun.am.ldap.fallback.sleep.minutes
```

This property sets the time in minutes that a secondary Directory Server instance sleeps before it falls back to the primary server after the primary server comes back up. The default is 15 minutes.

The `com.sun.am.ldap.fallback.sleep.minutes` property is hidden. To set this property to a value other than the default (15 minutes), explicitly add it to the `AMConfig.properties` file. For example, to set the value to 7 minutes:

```
com.sun.am.ldap.fallback.sleep.minutes=7
```

For the new value to take effect, restart the Access Manager web container.

Multiple Access Manager instances log to separate log files

Multiple Access Manager instances running on the same host server can now log to separate log files in different logging subdirectories by setting the following new property in the `AMConfig.properties` file:

```
com.sun.identity.log.logSubdir
```

Unless you change the default logging directory in the Admin Console, the default logging directories are:

- Solaris systems: `/var/opt/SUNWam/logs`
- Linux and HP-UX systems: `/var/opt/sun/identity/logs`
- Windows systems: `C:\Sun\JavaES5\identity\logs`

The first Access Manager instance always logs to the default logging directory. To specify different logging subdirectories for additional Access Manager instances, set the `com.sun.identity.log.logSubdir` property in the `AMConfig.properties` file for each additional Access Manager instance.

For example, if you have three instances, `am-instance-1`, `am-instance-2`, and `am-instance-3`, all running on the same Solaris host server, set the property as follows:

```
com.sun.identity.log.logSubdir=am-instance-2
com.sun.identity.log.logSubdir=am-instance-3
```

The `com.sun.identity.log.logSubdir` property is hidden. You must explicitly add this property to the `AMConfig.properties` file as needed and restart the Access Manager web container for subdirectory values to take effect.

The Access Manager instances then log to the following directories:

```
/var/opt/SUNWam/logs/log-files-for-am-instance-1
/var/opt/SUNWam/logs/am-instance-2/log-files-for-am-instance-2
/var/opt/SUNWam/logs/am-instance-3/log-files-for-am-instance-3
```

Access Manager 7 allows multiple cookie domains

To support multiple cookie domains, Access Manager has the following new property:

```
com.sun.identity.authentication.setCookieToAllDomains
```

The default is `true`. This new property is hidden. To set the value to `false`, explicitly add the property to the `AMConfig.properties` file, and restart the Access Manager web container.

Microsoft IIS 6.0 post-authentication plug-in supports SharePoint Server

The Microsoft Internet Information Services (IIS) 6.0 authentication plug-in now supports the Microsoft Office SharePoint Server. A user can login to Access Manager with either a user ID or login name. SharePoint Server, however, accepts a login name, which causes problems when the user specifies a user ID.

To allow a login to SharePoint Server, the post-authentication plug-in (`ReplayPasswd.java`) now uses the following new property:

```
com.sun.am.sharepoint_login_attr_name
```

This new property indicates the user attribute that SharePoint Server uses for authentication. For example, the following property species the common name (`cn`) for authentication:

```
com.sun.am.sharepoint_login_attr_name=cn
```

The post-authentication plug-in reads the `com.sun.am.sharepoint_login_attr_name` property and gets the corresponding attribute value for the user from Directory Server. The plug-in then sets the authorization headers to allow the user to access SharePoint Server.

This property is hidden. To set the property, explicitly add it to the `AMConfig.properties` file, and then restart the Access Manager web container for the value to take effect.

Access Manager supports Internet Explorer 7

Access Manager 7 2005Q4 patch 6 now supports Microsoft Windows Internet Explorer 7.

CR# 6379325: Accessing Console during session failover throws null pointer exception

In this scenario, multiple Access Manager servers are deployed in session failover mode behind a load balancer configured for cookie-based sticky request routing. The Access Manager administrator accesses the Access Manager Console through the load balancer. When the administrator logs into the Console, the session is created on one of the Access Manager servers. If that server goes down, the Console session fails over to another Access Manager server, as expected. The administrator, however, sometimes experiences intermittent null pointer exceptions on the browser and in the web-container error log.

The issue affects only the active Access Manager Console session at the time of the failover and not the functioning of the Access Manager servers.

Workaround: To prevent these intermittent null pointer exceptions:

- For a temporary solution, refresh the browser, or log out and then back into the Console.
- For a permanent solution, deploy the Access Manager Console on a separate Access Manager instance that does not participate in the session failover.

CR# 6508103: On Windows, clicking Help in the Admin Console returns an application error

On Windows 2003 Enterprise Edition with Access Manager deployed on Sun Java System Application Server in locales other than English, clicking Help in the Admin Realm Mode Console returns an application error.

Workaround:

1. Copy the *javaes-install-dir*`\share\lib\jhall.jar` file to the `%JAVA_HOME%\jre\lib\ext` directory.

   where *javaes-install-dir* is the Windows installation directory
2. Restart the Application Server instance.

Access Manager 7 2005Q4 Patch 5

Access Manager 7 patch 5 (revision 05) fixes a number of problems, as listed in the README file included with the patch. Patch 5 also includes the following new features, issues, and documentation updates.

New Features in Patch 5

Known Issues and Limitations in Patch 5

Globalization (g11n) Issues

Documentation Updates

- "Document steps to set up Distributed Authentication UI server passwords (6510859)" on page 105
- "Online Help for "To create a new site name" needs more information (2144543)" on page 106
- "Document that administrator password configuration parameter is `ADMIN_PASSWD` on Windows systems (6470793)" on page 106

Support for HP-UX Systems

Patch **126371** provides support for HP-UX systems. For more information see:

- "Patch Installation Instructions For HP-UX Systems" on page 20
- "Post-Installation Considerations" on page 21

For information about installation on HP-UX systems, see the *Sun Java Enterprise System 2005Q4 Installation Guide for UNIX*.

Support for Microsoft Windows Systems

Patch **124296** provides support for Windows systems. For more information see:

- "Patch Installation Instructions For Windows Systems" on page 19
- "Post-Installation Considerations" on page 21
- "Tuning scripts are available for Windows systems" on page 44

For information about installation on Windows systems, see the *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows*.

New `updateschema.sh` script to load LDIF and XML files

Patch 5 (and later) includes the `updateschema.sh` script to load the following files to update the Directory Server service schema:

- `AddLDAPFilterCondition.xml`
- `amPolicyConfig_mod_ldfc.xml`
- `accountLockoutData.xml`
- `accountLockout.ldif`
- `idRepoServiceAddAttrSchemaRequest_Cache.xml`
- `wsf1.1_upgrade.xml`
- `amAuth_mod.xml`
- `amAuthCert_mod.xml`

In previous Access Manager patch releases, you were required to load these files manually.

To run the `updateschema.sh` script:

1. Log in as or become superuser (`root`).
2. Change to the patch directory.

3. Run the script. For example, on Solaris systems:

```
# cd /120954-07
# ./updateschema.sh
```

   On Windows systems, the script is `updateschema.pl`.

4. When the script prompts you, enter these items:
   - Directory Server host name and port number
   - Directory Server admin user DN and password
   - `amadmin` DN and password
5. The script validates your entries and then loads the files. The script also writes the following log file:
   - Solaris systems: `/var/opt/SUMWam/logs/AM70Patch.upgrade.schema.`*timestamp*
   - Linux systems: `/var/opt/sun/identity/logs/AM70Patch.upgrade.schema.`*timestamp*
6. After the script finishes, restart the Access Manager web container.

Note If you back out patch 5, the schema changes added by the `updateschema.sh` script are not removed from Directory Server. However, you do not need to remove these schema changes manually because they will not affect Access Manager functionality or usability after the patch is backed out.

Support for specific application idle session timeout values

Patch 5 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.

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.

CDC Servlet can be deployed on a Distributed Authentication UI server

The CDC Servlet can coexist with a Distributed Authentication UI server in the DMZ to enable Cross-Domain Single Sign-On (CDSSO). The Access Manager server can be deployed behind a firewall, and all access to Access Manager to achieve CDSSO is handled by the CDC Servlet in the Distributed Authentication UI server. To enable CDSSO, refer to the specific policy agent documentation and perform these additional steps:

- Modify the agent's `AMAgent.properties` file to point to the CDC Servlet on the Distributed Authentication side (client). For example, for web agents, change the following property:

```
com.sun.am.policy.agents.config.cdcservlet.url=
    http://DAhost.DAdomain:DAport/DISTAUTH_DEPLOY_URI/cdcservlet
```

- Define policies as necessary in Access Manager for resources that need to be protected by the agent. For example, if agent is at `host.example.com:80`, define a policy for the resource as `http://host.example.com:80/*`.

Realm can be specified when CDC servlet redirects to the Access Manager login URL

You can now specify a realm name to the CDC servlet, so that when the redirect to the Access Manager login URL occurs, the realm name is included, and the user can logo into the specific realm. For example:

```
com.sun.am.policy.agents.config.cdcservlet.url=
    http://lb.example.com/amserver/cdcservlet?org=realm1
```

Certificate Authentication can use UPN value to map user profile

Previously, Certificate Authentication used only the `dn` component in the `subjectDN` to map a user profile. Access Manager now allows the user principal name (UPN) value in `SubjectAltNameExt` for profile mapping.

Post authentication processing of logout occurs in a multiple-server environment

Post authentication processing now occurs when a user logs out of a different server from the one originally logged into in a multiple-server environment, either with or without session failover configured.

SAML supports a new name identifier SPI

SAML now supports a new name identifier service provider interface (SPI), so that a site can customize the name identifier in the SAML assertion. A site can implement the new `NameIdentifierMapper` interface to map a user account to a name identifier in the subject of a SAML assertion.

New Configuration Properties for Site Monitoring

The Access Manager site monitoring feature includes the following new properties to allow you to specify the behavior of the site status check.

Property	Description
`com.sun.identity.urlchecker.invalidate.interval`	Time interval in milliseconds for recognizing a down or non-responding site. Default: 70000 milliseconds (70 seconds).

`com.sun.identity.urlchecker.sleep.interval`	Time interval in milliseconds that the site status check should sleep. Default: 30000 milliseconds (30 seconds).
`com.sun.identity.urlchecker.targeturl`	Different target URL for checking the Access Manager process status. Default: "`/amserver/namingservice`".

The patch does not add these properties to the `AMConfig.properties` file. To use these new properties with values other than the default values:

1. Add the properties and their values to the `AMConfig.properties` file. For Policy Agents, add these properties to the `AMAgents.properties` file.
2. Restart the Access Manager web container for the values to take effect.

User no longer must authenticate twice in authentication chain

Consider the following scenario. A site configures an authentication chain with three LDAP modules. All modules are set to `SUFFICIENT`, and both the `iplanet-am-auth-shared-state-enabled` and `iplanet-am-auth-store-shared-state-enabled` options are set to `true`. For example:

```
<AttributeValuePair>
   <Value>A-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>B-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>C-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
</AttributeValuePair>
```

Patch 5 adds the new `iplanet-am-auth-shared-state-behavior-pattern` option to the module options with two possible values: `tryFirstPass` (default) and `useFirstPass`.

To prevent a user from having to enter the user ID and password twice to get authenticated (as described in the previous scenario), set this new option to `useFirstPass` for all modules in the chain. Previously, a user who existed only in the third LDAP instance was required to enter a user ID and password twice to get authenticated.

Changes to Performance Tuning Scripts

Patch 5 includes these changes to the performance tuning scripts:

- "Tuning scripts support a password file" on page 42
- "Tuning script removes unnecessary ACIs from Directory Server" on page 42
- "Tuning scripts can tune the Distributed Authentication UI server web container" on page 42

- "Single `amtune-os` script tunes both Solaris OS and Linux OS" on page 43
- "Tuning scripts run to completion in a Solaris 10 local zone" on page 43
- "Tuning scripts are available for Windows systems" on page 44
- "Tuning Considerations for Sun Fire T1000 and T2000 Servers" on page 44

See also "CR# 6527663: Default value for `com.sun.identity.log.resolveHostName` property should be `false` instead of `true`" on page 46.

Tuning scripts support a password file

Patch 5 allows you to specify passwords for the tuning scripts in a text file. Previously, you could enter passwords only as a command-line argument, which could cause security issues. To use a password file, set the following variables, as needed, in the file:

```
DS_ADMIN_PASSWORD=DirectoryServer-admin-password
AS_ADMIN_PASSWORD=ApplicationServer8-admin-password
```

For example, to tune Application Server 8:

```
# ./amtune-as8 password-file
```

where *password-file* contains `AS_ADMIN_PASSWORD` set to the Application Server 8 administrator password.

The tuning scripts use the `-j` *password-file* option when they call the `ldapmodify`, `ldapsearch`, `db2index`, and `dsconf` Directory Server utilities.

Tuning script removes unnecessary ACIs from Directory Server

If Access Manager 7 2005Q4 is installed in Realm Mode, delegation privileges are used to determine access permissions, and therefore some Directory Server ACIs are not needed. Access Manager 7 2005Q4 patch 5 allows you to remove the unnecessary ACIs by running the `amtune-prepareDSTuner` script. This script reads a list of ACIs from the `remacis.ldif` file and then calls the `ldapmodify` utility to remove them.

You can run the `amtune-prepareDSTuner` script to remove the unnecessary ACIs on Solaris, Linux, HP-UX, and Windows systems. For more information, including how to run the script, see *Technical Note: Sun Java System Access Manager ACI Guide*.

Tuning scripts can tune the Distributed Authentication UI server web container

After you deploy the Distributed Authentication UI server on a web container, you can tune the web container by running the Access Manager tuning scripts. The following tuning scripts set the JVM and other tuning options for the respective web container:

TABLE 2 Access Manager Web Container Tuning Scripts

Web Container	Tuning Script
`amtune-ws61`	Web Server 6.1
`amtune-as7`	Application Server 7
`amtune-as8`	Application Server Enterprise Edition 8.1

To tune a web container for a Distributed Authentication UI server:

1. Because Access Manager server is not installed on the system where the Distributed Authentication UI server is deployed, copy the appropriate web container tuning script (shown in the previous table), `amtune-env` configuration file, and `amtune-utils` script from an Access Manager server installation. If you want to tune the Solaris or Linux operating system, copy the `amtune-os` script too.
2. Edit the parameters in the `amtune-env` configuration file to specify the web container and tuning options. To run the script in REVIEW mode, set `AMTUNE_MODE=REVIEW` in the `amtune-env` file.
3. Run the web container tuning script in REVIEW mode. In REVIEW mode, the script suggests tuning changes based on values in the `amtune-env` file but does not make any actual changes to the deployment.
4. Review the tuning recommendations in the debug log file. If needed, make changes to the `amtune-env` file based on this run.
5. To make tuning changes, set `AMTUNE_MODE=CHANGE` in the `amtune-env` file.
6. Run the tuning script in CHANGE mode to make the tuning changes to the deployment.

For more information about running the tuning script to tune an Access Manager web container, see Chapter 2, "Access Manager Tuning Scripts," in *Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide*.

Single amtune-os script tunes both Solaris OS and Linux OS

Patch 5 includes a single `amtune-os` script to tune both the Solaris OS and Linux OS. The script determines the OS type from the `uname -s` command. Previously, Access Manager provided separate `amtune-os` scripts to tune each OS.

Tuning scripts run to completion in a Solaris 10 local zone

If Access Manager is installed in a Solaris 10 local zone, all tuning scripts except `amtune-os` can run in the local zone. In a local zone, the `amtune-os` script displays a warning message but does not tune the OS. The script then continues running any other tuning scripts that you have requested. Previously, in a local zone, the `amtune-os` script would abort, and any subsequent tuning scripts that you requested would not run.

In a Solaris 10 global zone, the `amtune` script invokes `amtune-os` to tune the OS as well as any other scripts that you have requested to run.

Tuning scripts are available for Windows systems

Patch 5 includes tuning scripts for Windows systems. Running the tuning scripts on a Windows system is similar to running the scripts on a Solaris system or Linux system, with these differences:

- Windows scripts are written in Perl and require Active Perl 5.8 to run.
- If you are tuning Directory Server, after running `amtune-prepareDSTuner.pl` script, you must copy the `amtune-utils.pl`, `amtune-directory.pl`, `remacis.ldif`, and `amtune-samplepassordfile` files to the Directory Server system, because the script cannot compress these files.
- A script to tune the Windows operating system is not available.
- Support for zones is not provided.
- Before running a script, you must set the `$BASEDIR` parameter to the Access Manager installation directory in the `amtune-env.pl` file.

Tuning Considerations for Sun Fire T1000 and T2000 Servers

If Access Manager is installed on a Sun Fire T1000 or T2000 server, the Patch 5 tuning scripts for Web Server 6.1 and Application Server 8 set the `JVM GC ParallelGCThreads` parameter to 8:

```
-XX:ParallelGCThreads=8
```

This parameter reduces the number of garbage collection threads, which could be unnecessarily high on a 32–thread capable system. However, you can increase the value to 16 or even 20 for a 32 virtual CPU machine such as a Sun Fire T1000 or T2000 server, if it minimizes full garbage collection activities.

Also, for Solaris SPARC systems with a CMT processor with CoolThreads technology, in the `/etc/opt/SUNWam/config/AMConfig.properties` file, it is recommended that you add the following property at the end of the file:

```
com.sun.am.concurrencyRate=value
```

The default *value* is 16, but you can set this property to a lower value, depending on the number of cores in the Sun Fire T1000 or T2000 server.

Basic Authentication in the IIS 6.0 Policy Agent

To enable Basic Authentication in the Microsoft Internet Information Services (IIS) 6.0, the policy agent must obtain the user's name and password. Patch 5 includes the following new classes to enable this functionality using DES encryption of the user's password:

- `DESGenKey.java` generates a unique key used to encrypt and decrypt the user's password.
- `ReplayPasswd.java` reads the encryption key value from the `com.sun.am.replaypasswd.key` property in the `AMConfig.properties` file, encrypts the password, and assigns it to the `sunIdentityUserPassword` session property.

To use the Basic Authentication in IIS 6.0, you must perform steps on both the Access Manager server side and the IIS 6.0 policy agent side.

On the Access Manager server side:

1. Execute `DESGenKey.java` to generate a unique encryption key for password encryption and decryption. On Solaris systems, the `DESGenKey.java` file is located under the `com/sun/identity/common` directory, included in `am_sdk.jar` in the `/opt/SUNWam/lib` directory. For example, the following command generates an encryption key:

   ```
   # cd /opt/SUNWam/lib
   # java -cp am_sdk.jar com.sun.identity.common.DESGenKey
   ```
2. Assign the encryption key value from Step 1 to the `com.sun.am.replaypasswd.key` property in the `AMConfig.properties` file.
3. Deploy `ReplayPasswd.java` as a post authentication plug-in. Use the complete class name when you configure the plug-in: `com.sun.identity.authentication.spi.ReplayPasswd`.

On the IIS 6.0 policy agent side:

1. Assign the encryption key value from the server side to the `com.sun.am.replaypasswd.key` property in the `AMAgent.properties` file. Both the Access Manager server and the IIS 6.0 policy agent must use the same encryption key.
2. Enable Basic Authentication in IIS 6.0 Manager.

The IIS 6.0 policy agent reads the encrypted password from the session response, decrypts the password from the `com.sun.am.replaypasswd.key` property, and sets the authentication headers, to allow the Basic Authentication to work.

For information about the IIS 6.0 policy agent, see the *Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0*.

CR# 6567746: On HP-UX systems, Access Manager patch 5 reports incorrect errorCode value if password retry count is exceeded

When a user's account is locked, Access Manager 7 2005Q4 patch 5 on HP-UX systems reports `errorCode = null` instead of `errorCode = 107` if the password retry count is exceeded.

Workaround. None.

CR# 6527663: Default value for `com.sun.identity.log.resolveHostName` property should be `false` instead of `true`

Before you run the `amtune-identity` tuning script, it is recommended that you add the following property set to `false` to the `AMConfig.properties` file:

```
com.sun.identity.log.resolveHostName=false
```

A value of `false` minimizes the impact of resolving host names and thus can improve performance. However, if you want the client machine's hostname to be printed in the `amAuthentication.access` log, set the value to `true`.

CR# 6527528: Patch removal leaves XML files with `amldapuser` password in clear text

If you remove patch 5 from an Access Manager full server installation, the `amAuthLDAP.xml` and `amPolicyConfig.xml` files contain the `amldapuser` password in clear text. These files are 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`

Workaround: Edit the `amAuthLDAP.xml` and `amPolicyConfig.xml` files and delete the clear text password.

CR# 6527516: Full server on WebLogic requires JAX-RPC 1.0 JAR files to communicate with client SDK

In Access Manager 7 2005Q4 patches, the Access Manager configuration script for BEA WebLogic Server (`amwl81config`) adds the JAX-RPC 1.1 JAR files to the `classpath` for the WebLogic instance. While this modification is beneficial to products such as Sun Java System Portal Server, a full server installation (`DEPLOY_LEVEL=1`) deployed on WebLogic Server cannot communicate with a client SDK installation, and exceptions will subsequently occur.

If Access Manager 7 2005Q4 server is installed on BEA WebLogic Server, the `CLASSPATH` in the `startWebLogic.sh` script must be set to the location of the JAX-RPC 1.0 JAR files to communicate with Access Manager client SDK.

Workaround: Before applying the Access Manager patch, set the `CLASSPATH` in the `startWebLogic.sh` script for the WebLogic Server instance to use the JAX-RPC 1.0 JAR files instead of the JAX-RPC 1.1 JAR files:

1. On the Access Manager server, login as or become superuser (`root`).
2. Edit the `startWebLogic.sh` script and replace the `CLASSPATH` to use the JAX-RPC 1.0 JAR files. For example:

Current value:

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-spi.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-impl.jar:
```

New value:

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc_1.0/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-ri.jar:
```

where *AccessManager-base* is the base installation directory. The default value is `/opt` on Solaris systems and `/opt/sun` on Linux and HP-UX systems. *AccessManager-package-dir* is the Access Manager package directory.

5. Restart the WebLogic Server instance.

CR # 6523499: Patch 5 `amsilent` file is readable by all users on Linux systems

On Linux systems. the `postpatch` script creates the `/opt/sun/identity/amsilent` file with permissions of 644, which allows read access by all users.

Workaround: After executing the `installpatch` script, change the permissions on the `amsilent` file to allow read and write access only to the owner. For example:

```
# chmod 600 /opt/sun/identity/amsilent
```

CR# 6520326: Applying patch 5 to a second Access Manager instance on a server overwrites `serverconfig.xml` for first instance

In this deployment scenario, two Access Manager instances are deployed on the same host server, with each instance on a different web container instance. You then follow these steps:

1. Apply patch 5.
2. Modify the `amsilent` file and redeploy the first Access Manager instance.
3. Modify the `amsilent` again for the second Access Manager instance, and then redeploy that instance.

If `NEW_INSTANCE=false` in the `amsilent` file, the `serverconfig.xml` file for the first Access Manager instance is overwritten with information from the second Access Manager instance. A subsequent restart of the first Access Manager instance fails. The `serverconfig.xml` file is in the following directory depending on your platform:

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

Workaround: When you deploy the second Access Manager, set `NEW_INSTANCE=true` in the `amsilent` file. The `serverconfig.xml` file for the second Access Manager instance is then updated with the correct information, and the `serverconfig.xml` file for the first Access Manager instance is not overwritten.

CR# 6520016: Patch 5 SDK-only install overwrites the samples makefiles

Applying patch 5 to an SDK-only machine overwrites the samples makefiles.

Workaround: Applying patch 5 to an SDK-only machine does not require a reconfiguration; however, if you want to use the samples makefiles, follow these steps to update the LDIF and properties files (that is, perform tag swapping) for the samples makefiles:

1. Run the `amconfig` script with `DEPLOY_LEVEL=14` to uninstall the SDK and unconfigure the web container.
2. Run the `amconfig` script with `DEPLOY_LEVEL=4` to re-install the SDK and reconfigure the web container.

CR#6515502: LDAPv3 repository plug-in does not always handle Alias Search Attribute correctly

For most searches, this problem has been fixed. However, be careful when setting the Alias Search Attribute. The value of the alias search attributes must be unique across an organization. If more than one alias search attribute is set, it is possible that one entry in the data store matches one attribute, and another entry matches with the other attribute. In this situation, Access Manager server throws the following error:

```
An internal authentication error has occurred. Contact your system administrator.
```

Workaround: None

CR# 6515383: Distributed Authentication and J2EE agent do not work in same web container

A Distributed Authentication UI server and a J2EE policy agent do not work if they are installed in the same web container.

Workaround: Create a second web container instance and deploy the Distributed Authentication UI server and J2EE policy agent on different instances of the container.

CR# 6508103: Online help returns application error with Application Server on Windows systems

If you deploy Access Manager on Sun Java System Application Server on a Windows system, clicking Help in the left panel of the help screen for the Realm Mode console returns an application error.

Workaround: Copy the *javaes-install-dir*`\share\lib\jhall.jar` file to the `JAVA_HOME\jre\lib\ext` directory and then restart Application Server.

CR# 6507383 and CR# 6507377: Distributed Authentication requires explicit `goto` URL parameter

If an explicit `goto` URL parameter is not specified, a Distributed Authentication UI server attempts to redirect to the `goto` on a success URL specified in Access Manager. This redirect can fail for these reasons:

- The URL is relative, and no corresponding page is available at the Distributed Authentication UI server
- The URL is absolute, and the browser cannot reach the URL.

Workaround: Always specify an explicit `goto` URL parameter for a Distributed Authentication UI server.

CR# 6402167: LDAP JDK 4.18 causes LDAP client/Directory Server problems

Access Manager 7 2005Q4 was released with LDAP JDK 4.18 as part of the Java ES 2005Q4 release, which resulted in a number of Access Manager and Directory Server connection problems.

Workaround: Apply one of the following Sun Java System LDAP Java Development Kit patches:

- Solaris OS, SPARC and x86 platforms: 119725-04
- Linux OS: 120834-02

The patches are available on SunSolve Online: `http://sunsolve.sun.com`.

CR# 6352135: Distributed Authentication UI server files are installed in incorrect location

On Solaris systems, the Java ES installer installs the Distributed Authentication UI server `Makefile.distAuthUI`, `README.distAuthUI`, and `amauthdistui.war` files in an incorrect location: `/opt/SUNComm/SUNWam`.

Workaround: Copy these files to their correct location: `/opt/SUNWam`.

Note: Any Distributed Authentication UI server problems fixed in a patch will go into the `/opt/SUNComm/SUNWam/amauthdistui.war` file, so whenever you apply a patch to the Access Manager server and then rebuild and deploy the WAR file, you must also copy these files to the `/opt/SUNWam` directory.

CR# 6522720: Search in console online help does not work for multibyte characters on Windows and HP-UX systems

If Access Manager is installed in a locale that uses multibyte characters (such as Japanese) on a Windows or HP-UX system, a search in the console online help with keywords entered using multibyte characters does not work.

Workaround: None

Patch 6 update: Access Manager 7 2005Q4 patch 6 fixes this problem on Windows systems. However, the problem still exists on HP-UX systems.

CR# 6524251: Multibyte characters in output messages are garbled during Access Manager configuration on Windows systems

If Access Manager is installed in a locale that uses multibyte characters (such as Japanese or Chinese) on a Windows system, during Access Manager configuration, words are garbled in output messages at the terminal window.

Workaround: None, but this problem does not affect the configuration itself.

CR# 6526940: Property keys appear instead of message text during patch 5 installation in non-English locales on Windows systems

If you install patch 5 (124296-05) in a non-English locale on a Windows system, some strings in the install panels appear as property keys instead of the actual message text. Examples of property keys are `PRODUCT_NAME`, `JES_Patch_FinishPanel_Text1`, and `JES_Patch_FinishPanel_Text2`.

Workaround: None

CR# 6513653: Issue with `com.iplanet.am.session.purgedelay` property setting

The Access Manager `amtune` script sets the `com.iplanet.am.session.purgedelay` property to 1, in order to allow as many Access Manager sessions as possible. This property specifies the number of minutes to delay the purge session operation. For clients such as Sun Java System Portal Server, however, a value of 1 might not be sufficient.

Workaround: Reset the `com.iplanet.am.session.purgedelay` property after you run the `amtune` script:

1. In the `AMConfig.properties` file, set the property to the new value. For example:

   ```
   com.iplanet.am.session.purgedelay=5
   ```

2. Restart the Access Manager web container for the new value to take effect.

Access Manager 7 2005Q4 Patch 4

Access Manager 7 2005Q4 patch 4 (revision 04) fixes the following problems:

- CR# 6463796: Disabling `iPlanetAMClientDetection` service for `genericHTML` prevents access to any Access Manager HTML page
- CR# 6463779: Distributed Authentication `amProfile_Client` and Access Manager Server `amProfile_Server` get filled with harmless exceptions
- CR# 6463730: Cross-site scripting (XSS) vulnerability exists with the `goto` and `gx-charset` parameters
- CR# 6435889: Method `Session.getSession` fails because `RestrictedTokenContext` is not set

Known Issues and Limitations in Patch 4

- "CR# 6470055: Distributed Authentication UI server performance improvement" on page 51
- "CR# 6455079: Password reset service reports notification errors when a password is changed" on page 52

CR# 6470055: Distributed Authentication UI server performance improvement

To improve performance in reading, searching, and comparing user attributes for a Distributed Authentication UI server user, follow these steps:

1. In the `Makefile.distAuthUI` file, change the application user name from `anonymous` to another user. For example:

   ```
   APPLICATION_USERNAME=user1
   ```

2. In Directory Server, add the new user (`user1` in the example) and ACI to allow reading, searching, and comparing user attributes. The following example adds the new ACI:

   ```
   dn:ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com
   changetype:modify add:aci
   aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com")
   (targetattr = *")(version 3.0;
   acl "SunAM client data access to a Distributed Auth App User";
   allow (read, search, compare)
   userdn =  "ldap:///uid=user1,ou=people,dc=example,dc=com";)
   ```

CR# 6455079: Password reset service reports notification errors when a password is changed

When a password is changed, Access Manager submits the email notification using the unqualified sender name `Identity-Server`, which results in error 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: Change the from address to include the fully qualified domain name of the host server in the `amPasswordResetModuleMsgs.properties` file:

1. Change the from address label. For example:

   ```
   fromAddress.label=<Identity-Server@amhost.example.com>
   ```

2. Change the `lockOutEmailFrom` property to insure that lockout notifications use the correct from address. For example:

   ```
   lockOutEmailFrom=<Identity-Server@amhost.example.com>
   ```

   The `amPasswordResetModuleMsgs.properties` file is in the *AccessManager-base*`/SUNWam/locale` directory on Solaris systems and the *AccessManager-base*`/identity/locale` directory on Linux systems.

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

Access Manager 7 2005Q4 Patch 3

Access Manager 7 patch 3 (revision 03) fixes a number of problems, as listed in the README file included with the patch. Patch 3 also includes the following new features and known issues:

New Features in Patch 3

Known Issues and Limitations in Patch 3

New Configuration Properties for Site Monitoring

The Access Manager site monitoring feature includes these new properties:

Property	Description
`com.sun.identity.sitemonitor.interval`	Interval time in milliseconds for site monitoring. The site monitoring feature checks each site's availability within the specified time interval. Default: 60000 milliseconds (1 minute).
`com.sun.identity.sitemonitor.timeout`	Timeout in milliseconds for site availability checking. The site monitoring feature waits for the specified timeout value for a response from the site. Default: 5000 milliseconds (5 seconds).

The patch does not add these properties to the `AMConfig.properties` file. To use these new properties with values other than the default values:

1. Add the properties and their values to the `AMConfig.properties` file in the following directory, depending on your platform:
   - Solaris systems: `/etc/opt/SUNWam/config`

- Linux systems: `/etc/opt/sun/identity/config`

For Policy Agents, add these properties to the `AMAgents.properties` file.

2. Restart the Access Manager Web container for the values to take effect.

Custom implementation. In addition, the `com.sun.identity.sitemonitor.SiteStatusCheck` class allows you to customize your own implementation for checking site availability using the following interface:

```
package com.iplanet.services.naming.WebtopNaming$SiteStatusCheck
```

Each implementation class must use the `doCheckSiteStatus` method.

```
public interface SiteStatusCheck {
public boolean doCheckSiteStatus(URL siteurl);
}
```

Liberty Identity Web Services Framework (ID-WSF) 1.1 Support

The default version of ID-WSF in Access Manager 7 patch 3 is WSF1.1. There is no separate configuration needed to trigger the ID-WSF, except that the samples need to use the new security mechanisms. The new security mechanisms for the ID-WSF1.1 are:

```
urn:liberty:security:2005-02:null:X509
urn:liberty:security:2005-02:TLS:X509
urn:liberty:security:2005-02:ClientTLS:X509
urn:liberty:security:2005-02:null:SAML
urn:liberty:security:2005-02:TLS:SAML
urn:liberty:security:2005-02:ClientTLS:SAML
urn:liberty:security:2005-02:null:Bearer
urn:liberty:security:2005-02:TLS:Bearer
urn:liberty:security:2005-02:ClientTLS:Bearer
```

New Property for Liberty ID-WSF Support

The `com.sun.identity.liberty.wsf.version` property determines the Liberty ID-WSF framework when the framework cannot determine from the in-bound message or from the resource offering when Access Manager is acting as the WSC. Values can be 1.0 or 1.1. The default is 1.1.

Note The patch installation does not add the `com.sun.identity.liberty.wsf.version` property to the `AMConfig.properties` file (CR# 6458184). To use this new property, add it to the `AMConfig.properties` file with the appropriate value after you install the patch and then restart the Access Manager Web container.

After Access Manager 7 patch 3 is installed, run the following command to load the schema changes, shown with Access Manager installed in the default directory on Solaris systems:

```
# /opt/SUNWam/bin/amadmin -u amadmin -w amadmin_password
-t /etc/opt/SUNWam/wsf1.1_upgrade.xml
```

The ID-WSF discovery registration can use these new security mechanisms when registering. Also, WSCs will automatically detect which version to use while communicating to WSPs. To configure for ID-WSF1.1, follow the Readme files for the Liberty ID-FF sample1 and the ID-WSF samples that are included with the product.

CR# 6463779 Distributed Authentication `amProfile_Client` log and Access Manager server `amProfile_Server` log are filled with harmless exceptions

Requests to Access Manager server via a Distributed Authentication UI triggers exceptions in the `distAuth/amProfile_Client` log and the Access Manager server `debug/amProfile_Server` log. After numerous sessions, the `amProfile_Client` log can grow to several gigabytes, and the Access Manager server `amProfile_Server` log can grow to several megabytes. No loss of functionality is caused by these exceptions in the logs, but they can cause a false alarm for users, and potentially the logs can fill up the hard disk space.

Workaround. Run `cron` jobs that will make the contents of the log files null. For example:

- On the Distributed Authentication UI client machine, run "`cat /dev/null > distAuth/amProfile_Client`" every few hours, depending on the traffic volume.
- On the Access Manager server, run "`cat /dev/null > /var/opt/SUNWam/debug/amProfile_Server`" every few days, instead of every few hours.

CR# 6460974 Default Distributed Authentication Application User should not be `amadmin`

If you are deploying a Distributed Authentication UI server, the Distributed Authentication administrator should not be `amadmin`. The default Distributed Authentication Application User in the `Makefile.distAuthUI` file is `amadmin` and subsequently in the `AMConfig.properties` file after the `distAuth.war` file is deployed on the client side. The `amadmin` user has an `AppSSOToken` that expires after the `amadmin` session time runs out, which can cause a FATAL ERROR in the `amSecurity` log file (located by default in the `/tmp/distAuth` directory).

Workaround. Specify `UrlAccessAgent` as the Distributed Authentication Application User. For example:

Before deploying the `distAuth.war` file in the client Web container, change the following parameters in the `Makefile.distAuthUI` file:

```
APPLICATION_USERNAME=UrlAccessAgent
APPLICATION_PASSWORD=shared-secret-password or amldapuser-password
```

or

After deploying the `distAuth.war` file in the client Web container, change the following properties in the `AMConfig.properties` file for each Access Manager server:

```
com.sun.identity.agents.app.username=UrlAccessAgent
com.iplanet.am.service.password=shared-secret-password or amldapuser-password
```

See also "CR# 6440697: Distributed Authentication should run as non-amadmin user" on page 59.

CR# 6460576 No link for the User Service under Filtered Role in console online Help

The Access Manager Console online Help does not have a link for the User Service under Filtered Role. In the online Help, go to Contents, Filtered Role, and "To Create a Filtered Role". Page down and, depending on the identity type you selected, a list of services is displayed, but a User Service link is not available.

Workaround. None

CR# 6460085 Server on WebSphere is not accessible after running `reinstallRTM` and redeploying Web applications

After applying Access Manager 7 patch 3 for a `DEPLOY_LEVEL=1` deployment on IBM WebSphere Application Server 5.1.1.6 on Red Hat Linux AS 3.0 Update 4, the `reinstallRTM` script was run to restore the RTM RPMs. The Web applications were then redeployed after editing the `amsilent` file generated by the `reinstallRTM` script. WebSphere was restarted using the `stopServer.sh` and `startServer.sh` scripts. When accessing the login page, however, WebSphere displayed a 500 error, related to the `amlcontroller` filter.

This problem occurred because the new `server.xml` file generated by the `reinstallRTM` script was corrupt.

Workaround. The `server.xml` file backed up by the `amconfig` script is still valid. Use this previous copy, as follows:

1. Stop the server.
2. Replace the corrupted `server.xml` with the copy that was backed up by the `amconfig` script.

   The `server.xml` file that was backed up by the `amconfig` script will have the name `server.xml-orig-`*pid*, where *pid* is the process ID of the `amwas51config` script. The file is located in this directory:

   WebSphere-home-directory`/config/cells/`*WebSphere-cell*`/nodes/`*WebSphere-node*`/servers/`*server-name*
3. Restart the server.

CR# 6455757: `sunISManagerOrganization` marker class must be added to an organization before an upgrade

An organization in an Access Manager DIT that was created before the Access Manager 7 release might not have the `sunISManagerOrganization` object class. Also, an organization created by a product other than Access Manager will not have the `sunISManagerOrganization` object class in its definition.

Workaround. Before you upgrade to Access Manager 7 2005Q4, make sure that all organizations in the DIT have the `sunISManagerOrganization` object class in their definition. If necessary, manually add this object class before you upgrade.

CR# 6454489: Access Manager 7 2005Q4 Patch 2 upgrade causes an error in the Console Current Sessions tab

An upgrade caused the following error on the Current Sessions tab in the Access Manager Console:

```
Failed to get valid Sessions from the Specified server
```

This problem applies to deployments that are upgrading from Access Manager 6 versions that have a root suffix of the form `o=orgname`.

Workaround. After installing Manager 7 2005Q4, apply Manager 7 Patch 3 and then run the `amupgrade` script to migrate the data, as follows:

1. Backup your Access Manager 6 DIT.
2. Run the `ampre70upgrade` script.
3. Install Access Manager 7 2005Q4 with the Configure Later option.
4. Undeploy the Access Manager Web applications.
5. Deploy the Access Manager Web applications.
6. Apply Access Manager 7 patch 3, but don't apply the XML/LDIF changes. The XML/LDIF changes must be applied after running the `amupgrade` script in the next step.
7. Run the `amupgrade` script.
8. Redeploy the Access Manager Web applications, because of the Access Manager 7 patch 3 changes.
9. Access the Access Manager Console.

CR# 6452320: Exceptions are thrown when using polling with client SDK

When you deploy the Access Manager client SDK (`amclientsdk.jar`) and enable polling, errors such as the following can occur:

```
ERROR: Send Polling Error:
com.iplanet.am.util.ThreadPoolException:
amSessionPoller thread pool's task queue is full.
```

Such errors can occur after you deploy a Distributed Authentication UI server, J2EE agents, or in any situation where you deploy the Access Manager client SDK on a client machine.

Workaround. If you have only a few hundred concurrent sessions, add following properties and values in either the `AMConfig.properties` file or the `AMAgents.properties` file:

```
com.sun.identity.session.polling.threadpool.size=10
com.sun.identity.session.polling.threadpool.threshold=10000
```

For thousands or tens of thousands of sessions, the values should be set the same as those for notification in the Access Manager `AMConfig.properties` file after running the `amtune-identity` script. For example, for a machine with 4 GB of RAM, the Access Manager `amtune-identity` script sets the following values:

```
com.sun.identity.session.notification.threadpool.size=28
com.sun.identity.session.notification.threadpool.threshold=76288
```

Set similar values on the client side in the `AMAgent.properties` or `AMConfig.properties` file when the Distributed Authentication UI server or the Access Manager client SDK is deployed on a client machine with 4 GB of RAM.

CR# 6442905 `SSOToken` of authenticated user can be unintentionally revealed to rogue sites

An authenticated Access Manager user can unintentionally reveal the `SSOToken` to a rogue site by clicking on a URL from the rogue site.

Workaround. Always create a unique agent user profile in Access Manger for all participating Policy Agents to make sure that the site is not rogue. Also, make sure that none of these unique agent users use the same password as the shared secret password or `amldapuser` password. By default, Policy Agents are authenticated to the Access Manager Application authentication module as the `UrlAccessAgent` user.

For more information about creating an agent using the Access Manager Admin Console, see "Agents" in *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

CR# 6441918: Site monitor interval and time-out properties

Access Manager site failover includes the following new properties:

```
com.sun.identity.sitemonitor.interval
com.sun.identity.sitemonitor.timeout
```

For more information, see "New Configuration Properties for Site Monitoring" on page 53.

CR# 6440697: Distributed Authentication should run as non-amadmin user

To create a Distributed Authentication administrator other than the default administrative user (`amadmin`) for Distributed Authentication application authentication, follow this procedure:

1. Create an LDAP user for the Distributed Authentication administrator. For example:

   ```
   uid=DistAuthAdmin,ou=people,o=am
   ```

2. Add the Distributed Authentication administrator to the list of special users. For example:

   ```
   com.sun.identity.authentication.special.users=cn=dsameuser,
   ou=DSAME Users,o=am|cn=amService-UrlAccessAgent,ou=DSAME Users,
   o=am|uid=DistAuthAdmin,ou=People,o=am
   ```

   Add this property to the `AMConfig.properties` file of all Access Manager servers, so that the Distributed Authentication administrator's `AppSSOToken` does not expire when the session expires.

CR# 6440695: Distributed Authentication UI servers with a load balancer

If your deployment includes a load balancer in front of multiple Distributed Authentication UI servers, set the following properties in the `AMConfig.properties` file after you deploy the WAR file.

```
com.iplanet.am.lbcookie.name=DistAuthLBCookieName
com.iplanet.am.lbcookie.value=DistAuthLBCookieValue
```

CR# 6440651: Cookie replay requires `com.sun.identity.session.resetLBCookie` property

For cookie replaying to work properly for Access Manager session failover, add the `com.sun.identity.session.resetLBCookie` property with a value of `true` for both the Policy Agent and the Access Manager server. For example:

```
com.sun.identity.session.resetLBCookie='true'
```

- For the Policy Agent, add the property to the `AMAgent.properties` file.
- For the Access Manager server, add the property to the `AMConfig.properties` file.

Note: This property is required only if you have implemented Access Manager session failover.

CR# 6440648: `com.iplanet.am.lbcookie.name` property assumes default value of `amlbcookie`

By default, a Policy Agent and Access Manager servers assume a load balancer cookie name of `amlbcookie`. If you change the name of the cookie on the back-end server, you must use the

same name in the AMAgent.properties file for the Policy Agent. Also, if you are using the Access Manager client SDK, you must also use the same cookie name used by the back-end server.

CR# 6440641: com.iplanet.am.lbcookie.value property is deprecated

Access Manager no longer supports the com.iplanet.am.lbcookie.value property on servers to customize the load balancer cookie. Instead, Access Manager now uses the server ID, which is configured as part of session configuration, for the cookie value and for the name to be replayed by the agent.

CR# 6429610: Unable to create SSO token in ID-FF SSO use case

After setting up the Liberty Identity Federation Framework (ID-FF) sample 1, Federation succeeded, but SSO failed.

Workaround. Add the uuid of dsameuser to the com.sun.identity.authentication.special.users property in the AMConfig.properties file. For application authentication, dsameuser needs a non-expiring SSO token for the Access Manager server.

CR# 6389564: Repetitious successive queries on role memberships of user in an LDAP v3 data store during Access Manager login

When a user logs into Access Manager, repetitive LDAP searches on the user's nsRoleDN attribute occur.

Workaround. After the Access Manager 7 patch 3 is installed, run the following command shown with Access Manager installed in the default directory on Solaris systems:

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/idRepoServiceAddAttrSchemaRequest_Cache.xml
```

CR# 6385185: Authentication module must be able to override the “goto” URL and specify a different URL

An authentication module can override the “goto” URL and request re-direction to a different URL of an external Web site to get the user status validated.

To override the “goto” URL after the authentication is complete, set the property shown in the following example in the SSOToken. You set this property using the onLoginSuccess method of the PostProcess class implementing the AMPostAuthProcessInterface. For example, *OverridingURL* is the URL that overrides the “goto”URL:

```
public class <..> implements AMPostAuthProcessInterface {
...
    public void onLoginSuccess(...) {
        try {
            ssoToken.setProperty("PostProcessSuccessURL", OverridingURL);
         } catch (Exception ...) {
         ...         }
...
}
```

CR# 6385184: Re-direct from within a custom authentication module when SSO Token is still in invalid state

New `RedirectCallback` for custom authentication module allows redirection to an external Web site via the Authentication UI to get a user validated. If the authentication is successful, the user is then redirected back to the original Access Manager server URL. Sample files include:

- `LoginModuleSample.java`
- `LoginModuleSample.xml`
- `testExtWebSite.jsp`

To implement this feature:

1. Create a custom authentication module using the sample `LoginModuleSample.java`.
2. Load the module into an Access Manager server.
3. Construct the `RedirectCallback` in the XML file using the sample `LoginModuleSample.xml`.
4. To test the module, use the sample `testExtWebSite.jsp` file for the external Web site.
5. Login using this URL:

   ```
   http://example.com/amserver/UI/Login?module=LoginModuleSample
   ```

The user name and password are redirected to the external Web site for validation. If the name and password are valid, the authentication is successful and the user is then redirected back to the original Access Manager server URL.

For example, consider this scenario, where the deployment is using a custom authentication module to access a provisioning/credit card site:

1. A user invokes the authentication process/login page for the custom authentication module.
2. The user enters the credentials (user name and password) and submits a request to the custom authentication module.
3. The custom authentication module redirects the user to an external provisioning/credit card site with the required user information along with the request.
4. The external provisioning/credit card site checks the user's status and returns the request with either success or failure, which is set as part of the returned request.
5. The custom authentication module validates the user based on the status returned in Step 4 and returns the corresponding status to the authentication service.

6. The user authentication completes with either success or failure.

CR# 6324056: Federation fails when using artifact profile

Workaround: To fix this problem, apply latest version of the "Core Mobile Access" patch, depending on your platform:

- Solaris OS on SPARC based systems: 119527
- Solaris OS on x86 platforms: 119528
- Linux systems: 119529

After applying the patch, restart the Web container.

Access Manager 7 2005Q4 Patch 2

Access Manager 7 2005Q4 patch 2 (revision 02) fixed a number of problems, as listed in the README file included with the patch. Patch 2 also includes the following new features and known issues:

New Features in Patch 2

Known Issues and Limitations in Patch 2

New Properties for the User Management, Identity Repository, and Service Management Caches

Patch 2 includes the following new properties for the User Management (Access Manager SDK), Identity Repository (IdRepo), and Service Management caches. These properties allow you to enable and disable the different caches independently, based on your deployment requirements, and to set the time to live (TTL) for the cache entries.

TABLE 3 New Properties for the User Management, Identity Repository, and Service Management Caches

Property	Description
New Properties to Enable and Disable Caches	
`com.iplanet.am.sdk.caching.enabled`	Global property that enables (true) or disables (false) the Identity Repository (IdRepo), User Management, and Service Management caches. If true, or if the property is not present in the `AMConfig.properties` file, all three caches are enabled.
Note The following three properties to enable or disable the specific caches apply only if the previous global property is set to false.	
`com.sun.identity.amsdk.cache.enabled`	Enables (true) or disables (false) only the User Management (Access Manager SDK) cache.
`com.sun.identity.idm.cache.enabled`	Enables (true) or disables (false) only the Identity Repository (IdRepo) cache.
`com.sun.identity.sm.cache.enabled`	Enables (true) or disables (false) only the Service Management cache.
New User Management Cache Properties for TTL	
`com.iplanet.am.` `sdk.cache.entry.expire.enabled`	Enables (true) or disables (false) the expiration time (as defined by the following two properties) for the User Management cache.
`com.iplanet.am.` `sdk.cache.entry.user.expire.time`	Specifies the time in minutes that user entries for the User Management cache remain valid after their last modification. That is, after this specified time elapses (after the last modification or read from the directory), the data for the entry that is cached will expire. Then, new requests for data for these entries must be read from the directory.
`com.iplanet.am.` `sdk.cache.entry.default.expire.time`	Specifies the time in minutes that non-user entries for the User Management cache remain valid after their last modification. That is, after this specified time elapses (after the last modification or read from the directory), the data for the entry that is cached will expire. Then, new requests for data for these entries must be read from the directory. New Identity Repository Cache Properties for TTL
`com.sun.identity.` `idm.cache.entry.expire.enabled`	Enables (true) or disables (false) the expiration time (as defined by the following property) for the IdRepo cache.

TABLE 3 New Properties for the User Management, Identity Repository, and Service Management Caches *(Continued)*

`com.sun.identity.idm.cache.entry.default.expire.time`	Specifies the time in minutes that non-user entries for the IdRepo cache remain valid after their last modification. That is, after this specified time elapses (after the last modification or read from the repository), the data for the entry that is cached will expire. Then, new requests for data for these entries must be read from the repository.

Using the New Caching Properties

The Access Manager 7 2005Q4 patches do not automatically add the new caching properties to the `AMConfig.properties` file.

To use the new caching properties:

1. With a text editor, add the properties and their values to the `AMConfig.properties` file in the following directory, depending on your platform:
   - Solaris systems: `/etc/opt/SUNWam/config`
   - Linux systems: `/etc/opt/sun/identity/config`
2. Restart the Access Manager Web container for the values to take effect.

New Property for Federation Service Provider

The new `com.sun.identity.federation.spadapter` property defines the implementation class for `com.sun.identity.federation.plugins.FederationSPAdapter`, which is used to add application specific processing during Federation processing on the Service Provider side.

See also "CR# 6385696: Existing and new IDPs and SPs are not visible" on page 67.

LDAP Filter Condition Support

LDAP Filter Condition support is added in patch 2. A policy administrator can now specify an LDAP filter in the Condition while defining a policy. The Policy is applied to the user only if the LDAP entry of the user satisfies the LDAP filter specified in the Condition. The LDAP entry of the user is looked up from the directory specified in the Policy Configuration service.

To register and use the LDAP Filter Condition, run following commands after the Access Manager 7 patch 2 is installed shown with Access Manager installed in the default directory on Solaris systems:

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-s /etc/opt/SUNWam/AddLDAPFilterCondition.xml
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/amPolicyConfig_mod_ldfc.xml
```

Patch 5 Note If you added Access Manager 7 2005Q4 Patch 5 and ran the `updateschema.sh` script, you do not need to load these files using `amadmin`. For more information see "New `updateschema.sh` script to load LDIF and XML files" on page 37.

CR# 6283582: Num of login failures are not shared across Access Manager instances

After Access Manager 7 patch 2 is installed, run following commands, shown with Access Manager installed in the default directory in Solaris systems:

```
# cd DirectoryServer-base/shared/bin
# ./ldapmodify -h DirectoryServerHost -p DirectoryServerPort
-D "cn=Directory Manager" -w DirectoryMangerPassword
-a -f /etc/opt/SUNWam/accountLockout.ldif
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/accountLockoutData.xml
```

The default value of *DirectoryServer-base* is `/var/opt/mps/serverroot` on Solaris systems and `/var/opt/sun/directory-server` on Linux systems.

Patch 5 Note If you added Access Manager 7 2005Q4 Patch 5 and ran the `updateschema.sh` script, you do not need to load these files using `amadmin`. For more information see "New `updateschema.sh` script to load LDIF and XML files" on page 37.

CR# 6293673: Need to retain the original session information when sending out session timeout notification

The new `com.sun.identity.session.property.doNotTrimList` property in the `AMConfig.properties` file can contain list of comma separated session property names. Once a session is timed out, the properties defined in this list will not be trimmed off, so that they can be accessed before the session is purged. For example:

`com.sun.identity.session.property.doNotTrimList=`*UserId*`,`*HostName*

CR# 6244578: Access Manager should warn user that the browser cookie support is disabled/not available

The new `com.sun.identity.am.cookie.check` property in the `AMConfig.properties` file indicates whether the server should check for the cookie support / cookie enabled in the browser. A value of `true` causes the server to check for the cookie support / cookie enabled in the browser and to throw an error page if the browser does not support or has not enabled cookies. This value should be set to false (which is the default) if the server is expected to support cookie-less mode for authentication functionality.

CR# 6236892: Image/Text place holder while CDCServlet is processing the AuthNResponse after login

The following new properties are added to `AMConfig.properties` file and are read by the CDCServlet:

- `com.iplanet.services.cdc.WaitImage.display` causes an image to be displayed in the browser while a user is waiting for the protected page in a CDSSO scenario, if set to true. Default is false.
- `com.iplanet.services.cdc.WaitImage.name` specifies the image name. Default is `waitImage.gif`. This image be copied from the `login_images` directory.
- `com.iplanet.services.cdc.WaitImage.width` specifies the image width. Default is 420.
- `com.iplanet.services.cdc.WaitImage.height` specifies the image height. Default is 120.

CR# 6363157: New property disables persistent searches if absolutely required

The new `com.sun.am.event.connection.disable.list` property in the `AMConfig.properties` file specifies which event connection can be disabled. Values (case insensitive) can be:

`aci` - Changes to the `aci` attribute, with the search using the LDAP filter (`aci=*`)

`sm` - Changes in the Access Manager information tree (or service management node), which includes objects with the `sunService` or `sunServiceComponent` marker object class. For example, you might create a policy to define access privileges for a protected resource, or you might modify the rules, subjects, conditions, or response providers for an existing policy.

`um` - Changes in the user directory (or user management node). For example, you might change a user's name or address.

For example, to disable persistent searches for changes to the Access Manager information tree (or service management node):

```
com.sun.am.event.connection.disable.list=sm
```

To specify multiple values, separate each value with a comma.

Caution – Persistent searches cause some performance overhead on Directory Server. If you determine that removing some of this performance overhead is absolutely critical in a production environment, you can disable one or more persistent searches using the `com.sun.am.event.connection.disable.list` property.

However, before disabling a persistent search, you should understand the limitations described above. It is strongly recommended that this property not be changed unless absolutely required. This property was introduced primarily to avoid overhead on Directory Server when multiple 2.1 J2EE agents are used, because each of these agents establishes these persistent searches. The 2.2 J2EE agents no longer establish these persistent searches, so you might not need to use this property.

For more information, see "Document more information about disabling persistent searches (6486927)" on page 102.

CR# 6385696: Existing and new IDPs and SPs are not visible

The new `com.sun.identity.federation.spadapter` property in the `AMConfig.properties` file specifies the default implementation of the federation service provider adapter where the application can get assertions and response information. For example:

```
com.sun.identity.federation.spadapter=com.sun.identity.federation.plugins.FSDefaultSPAdapter
```

Access Manager 7 2005Q4 Patch 1

Access Manager 7 2005Q4 patch 1 (revision 01) fixed 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:

Creation of Debug Files

Access Manager debug files are created by default in the debug directory, even when `com.iplanet.services.debug.level` property in the `AMConfig.properties` file is set to error. Before Access Manager 7 patch 1 was released, a debug file was created only when the first debug message was logged to the file.

Support for Roles and Filtered Roles in the LDAPv3 Plug-in

Access Manager 7 patch 1 adds support for roles and filtered roles in the LDAPv3 plug-in, if the data is stored in Sun Java System Directory Server. For more information, see "Document the roles and filtered roles support for LDAPv3 plug-in (6365196)" on page 107.

CR# 6320475: `com.iplanet.am.session.client.polling.enable` on server side must not be true

The `com.iplanet.am.session.client.polling.enable` property in the `AMConfig.properties` file on the server side is set to false by default and should never be reset to true.

CR# 6358751: Access Manager 7 patch 1 apply fails if the there are embedded spaces in the encryption key

If the password encryption key contains spaces, applying the patch fails.

Workaround. Use a new encryption key that includes no spaces. For the detailed steps to change the encryption key, see: Appendix B, "Changing the Password Encryption Key," in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

What's New in This Release

For a list of new features in the Access Manager patch releases, see "Access Manager 7 2005Q4 Patch Releases" on page 11. The initial release of Access Manager 7 2005Q4 included the following new features:

Access Manager Modes

Access Manager 7 2005Q4 includes Realm mode and Legacy mode. Both modes support:

- New Access Manager 7 2005Q4 features
- Access Manager 6 2005Q1 features, except for these limitations:
  - When realms are created, the corresponding organizations are not created in Sun Java System Directory Server.
  - The new Access Manager 7 2005Q4 Console cannot set a Class of Service (CoS) template priority. See "New Access Manager Console cannot set the CoS template priorities (6309262)" on page 90.
- Identity repositories in Sun Java System Directory Server and other data stores

Legacy mode is required for:

- Sun Java System Portal Server
- Sun Java System Communications Services servers, including Messaging Server, Calendar Server, Instant Messaging, or Delegated Administrator
- Coexistence deployments when Access Manager 6 2005Q1 and Access Manager 7 2005Q4 access the same Directory Server

New Access Manager Console

The Access Manager Console has been redesigned for this release. However, if Access Manager is deployed with Portal Server, Messaging Server, Calendar Server, Instant Messaging, or Delegated Administrator, you must install Access Manager in Legacy mode and use the Access Manager 6 2005Q1 Console:

For more information, see "Compatibility Issues" on page 77.

Identity Repository

An Access Manager identity repository contains information pertinent to identities such as users, groups, and roles. You can create and maintain an identity repository using either Access Manager or another provisioning product such as Sun Java System Identity Manager.

In the current release, an identity repository can reside in either Sun Java System Directory Server or Microsoft Active Directory. Access Manager can have read/write access or read-only access to an identity repository.

Access Manager Information Tree

The Access Manager information tree contains information pertinent to system access. Each Access Manager instance creates and maintains a separate information tree in Sun Java System Directory Server. An Access Manager information tree can have any name (suffix). The Access Manager information tree includes realms (and sub-realms, if needed), as described in the following section.

Access Manager Realms

A realm and any sub-realms are part of the Access Manager information tree and can contain configuration information that defines a set of users and/or groups, how users authenticate, which resources users can access, and the information that is available to applications after users are given access to resources. A realm or sub-realm can also contain other configuration information, including globalization configuration, password reset configuration, session configuration, console configuration, and user preferences. A realm or sub-realm can also be empty.

You can create a realm using either the Access Manager Console or the `amadmin` CLI utility. For more information refer to the Console online help or the Chapter 14, "The amadmin Command Line Tool," in *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Session Failover Changes

Access Manager provides a web container independent session failover implementation using Sun Java System Message Queue (Message Queue) as the communications broker and the Berkeley DB by Sleepycat Software, Inc. as the session store database. Access Manager 7 2005Q4 enhancements includes the `amsfoconfig` script to configure the session failover environment and the `amsfo` script to start and stop the Message Queue broker and Berkeley DB client.

For more information, see "Implementing Access Manager Session Failover" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Session Property Change Notification

The session property change notification feature enables Access Manager to send a notification to the specific listeners when a change occurs on a specific session property. This feature takes effect when the "Enable Property Change Notifications" attribute is enabled in the Access Manager administrator Console. For example, in a single sign-on (SSO) environment, one Access Manager session can be shared by multiple applications. When a change occurs on a specific session property defined in the "Notification Properties" list, Access Manager sends a notification to all registered listeners.

For more information, see "Enabling Session Property Change Notifications" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Session Quota Constraints

The session quota constraints feature allows the Access Manager administrator (`amadmin`) to set the "Active User Sessions" attribute to limit the maximum number of concurrent sessions allowed for a user. The administrator can set a session quota constraint at the global level for all users or for an entity such as an organization, realm, role, or user that applies only to one or more specific users.

By default, session quota constraints are disabled (OFF), but the administrator can enable them by setting the "Enable Quota Constraints" attribute in the Access Manager administrator Console.

The administrator can also configure the behavior if a user exhausts the session constraint quota by setting the "Resulting Behavior If Session Quota Exhausted" attribute:

- DENY_ACCESS. Access Manager rejects the login request for a new session.
- DESTROY_OLD_SESSION. Access Manager destroys the next expiring existing session for the same user and allows the new login request to succeed.

The "Exempt Top-Level Admins From Constraint Checking" attribute specifies whether session constraint quotas apply to the administrators who have the "Top-level Admin Role".

For more information, see "Setting Session Quota Constraints" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*

Distributed Authentication

Access Manager 7 2005Q4 includes the Distributed Authentication UI, which is a remote authentication UI component that provides for secure, distributed authentication across two firewalls in a deployment. Without the Distributed Authentication UI component, the Access Manager service URLs can be exposed to the end users. This exposure can be avoided by using a proxy server; however, a proxy server is not necessarily an acceptable solution for many deployments.

The Distributed Authentication UI component is installed on one or more servers within the non-secure (DMZ) layer of an Access Manager deployment. A Distributed Authentication UI server does not run Access Manager; it exists only to provide the authentication interface to end users through a web browser.

The end user sends an HTTP request to the Distributed Authentication UI, which in turn presents a login page to the user. The Distributed Authentication component then sends the user's request through the second firewall to an Access Manager server, which eliminates the need to open holes in the firewalls between the end users and the Access Manager server.

For more information, see the *Technical Note: Using Access Manager Distributed Authentication*.

Multiple Authentication Module Instances Support

All authentication modules (out of box) are extended to support the sub-schema with Console UI support. Multiple authentication module instances can be created for each module type (module class loaded). For example, for instances with names of `ldap1` and `ldap2` for an LDAP module type, each instance can point to a different LDAP directory server. Module instances with the same names as their types are supported for backward compatibility. Invocation is:

server_deploy_uri`/UI/Login?module=`*module-instance-name*

Authentication "Named Configuration" or "Chaining" Name Space

A separate name space is created under an Organization/Realm, which is a chain of authentication module instances. The same chain can be reused and assigned to an Organization/Realm, Role, or User. The Authentication Service instance equals the Authentication Chain. Invocation is:

server_deploy_uri`/UI/Login?service=`*authentication-chain-name*

Policy Module Enhancements

Personalization Attributes

In addition to Rules, Subjects, and Conditions, policies can now have personalization attributes (`IDResponseProvider`). The policy decision sent to the client from the policy evaluation now includes policy-based response personalization attributes in the applicable policies. Two types of personalization attributes are supported:

- Static attributes. You define the attribute name and value in the policy.
- Dynamic attributes. You list the attribute names in the policies, and values are fetched from the Identity Repository data stores at policy evaluation time.

Policy Enforcement Points (agents) typically forward these attribute values as HTTP Header or Cookies or Request Attributes to the protected application.

Access Manager 7 2005Q4 does not support custom implementations of the Response Provider interface by customers.

Session Property Condition

The session policy condition implementation (`SessionPropertyCondition`) decides whether a policy is applicable to the request based on values of properties set in a user's Access Manager session. At policy evaluation time, the condition returns "true" only if the user's Access Manager session has every property value defined in the condition. For properties defined with multiple values in the condition, it is sufficient if the user session has at least one value listed for the property in the condition.

Policy Subject

The policy subject implementation (Access Manager Identity Subject) allows you to use entries from the configured Identity Repository as policy subject values.

Policy Export

You can export policies in XML format using the `amadmin` command. The new `GetPolices` and `RealmGetPolicies` elements in the `amAdmin.dtd` file support this feature.

Policy Status

A policy now has a status attribute, which can be set to active or inactive. Inactive policies are ignored during policy evaluation.

Site Configuration

Access Manager 7 2005Q4 introduces the "site concept," which provides centralized configuration management for an Access Manager deployment. When Access Manager is configured as a site, client requests always go through the load balancer, which simplifies the deployment as well as resolves issues such as a firewall between the client and the back-end Access Manager servers.

For more information, see "Configuring an Access Manager Deployment as a Site" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Bulk Federation

Access Manager 7 2005Q4 provides bulk federation of user accounts to applications that are outsourced to business partners. Previously, federating accounts between a Service Provider (SP) and an Identity Provider (IDP) required each user to access both the SP and IDP sites, create accounts if not already there, and federate the two accounts through a web link. This process was time consuming. It was not always suitable for a deployment with existing accounts or for a site that acted as an identity provider itself or use one of its partners as an authenticating provider.

For more information, see the *Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide*.

Logging Enhancements

Access Manager 7 2005Q4 includes several new logging enhancements:

- New fields (or columns): The `MessageID` field contains the message identifier for the logged event. The `ContextID` field contains the context identifier, which is analogous to a session identifier and applies to all events for a particular user's login session. For a user's specific login session, `ContextID` will be the same in all log files for logged events.
- Logging API. The API includes additions for reading log records, including from a database (DB), when logging to DB is configured. Refer to `LogReaderSample.java` in the `/opt/SUNWam/samples/logging` directory, which shows the retrieval of log records from a flat file or DB table repository.

Caution – Database tables tend to be larger than flat file logs. Therefore, in a given request, do not retrieve all of the records in a database table, because the quantity of data can consume all of the Access Manager server resources.

Hardware and Software Requirements

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

TABLE 4 Hardware and Software Requirements

Component	Requirement
Operating system (OS)	Solaris OS on SPARC based systems, versions 8, 9, and 10, including support for whole root local zones on Solaris 10
	Solaris OS on x86 platforms, versions 9 and 10, including support for whole root local zones on Solaris 10
	Solaris OS on AMD64 platforms, version 10, including support for whole root local zones
	Red Hat Linux, WS/AS/ES 2.1 Update 6 or later
	Red Hat Linux, WS/AS/ES 3.0
	Red Hat Linux, WS/AS/ES 3.0 Updates 1, 2, 3, and 4
	HP-UX OS. See the Sun Java Enterprise System 2005Q4 Document Collection for HP-UX: `http://docs.sun.com/coll/1258.2`
	Windows OS. See the Sun Java Enterprise System 2005Q4 Document Collection for Microsoft Windows: `http://docs.sun.com/coll/1259.2`
Java 2 Standard Edition (J2SE)	J2SE platform 1.5.0_04, 1.5_01, 1.5, and 1.4.2
Directory Server	Access Manager information tree: Sun Java System Directory Server 5 2005Q4
	Access Manager identity repository: Sun Java System Directory Server 5 2005Q4 or Microsoft Active Directory
Web containers	Sun Java System Web Server 6.1 2005Q4 SP5
	Sun Java System Application Server Enterprise Edition 8.1 2005Q2
	BEA WebLogic Server 8.1 SP4
	IBM WebSphere Application Server 5.1 and 5.1.1 (and associated cumulative fixes)
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 Oracle technical representative.

Supported Browsers

The following table shows the browsers that are supported by the Sun Java Enterprise System 2005Q4 release.

TABLE 5 Supported Browsers

Browser	Platform
Microsoft Internet Explorer 5.5 SP2	Windows 2000
Microsoft Internet Explorer 6.0	Windows 2000
	Windows XP
Mozilla 1.7.1	Solaris OS, versions 9 and 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0
Netscape™ 7.0	Solaris OS, versions 9 and 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0

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. Oracle 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 support for Sun Java System products in virtualized environments, see http://docs.sun.com/doc/820-4651.

Compatibility Issues

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 2005Q4 installation, see "Determining the Access Manager Mode" on page 78.

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 2005Q4 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
...
```

On Windows systems, the configuration file is *AccessManager-base*`\setup\AMConfigurator.properties`.

For more information about configuring Access Manager by running the `amconfig` script, refer to the *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Determining the Access Manager Mode

To determine whether a running Access Manager 7 2005Q4 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 2005Q4 modes.

TABLE 6 Policy Agents Compatibility With Access Manager 7 2005Q4 Modes

Agent and Version	Compatible Mode
Web and J2EE agents, version 2.2	Legacy and Realm modes
Web agents, version 2.1	Legacy and Realm modes
J2EE agents, version 2.1	Legacy mode only

Installation Notes

Access Manager installation notes include the following information:

- "Access Manager Legacy Mode" on page 77
- "Installation Issues" on page 81

Known Issues and Limitations

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

Compatibility Issues

Incompatibility between Java ES 2004Q2 servers and IM on Java ES 2005Q4 (6309082)

The following deployment scenario caused this problem:

- server-1: Java ES 2004Q2: Directory Server
- server-2: Java ES 2004Q2: Application Server, Access Manager, and Portal Server
- server-3: Java ES 2004Q2: Calendar Server and Messaging Server
- server-4: Java ES 2005Q4: Application Server, Instant Messaging, and Access Manager SDK

When running the `imconfig` utility to configure Instant Messaging on server-4, the configuration was not successful. The Access Manager 7 2005Q4 SDK, which is used by Instant Messaging (IM) on server-4, is not compatible with the Java ES 2004Q2 release.

Workaround: Ideally, the Access Manager server and Access Manager SDK should be the same release. For more information, see the *Sun Java Enterprise System 2005Q4 Upgrade Guide*.

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

Access Manager 7 2005Q4 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 2005Q4 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.

Agent cannot login because "Profile not in the organization" (6295074)

In the Access Manager Console, create an agent in Realm Mode. If you log out and then login again using the agent name, Access Manager returns an error because the agent does not have the privileges to access the realm.

Workaround: Modify the permissions to allow read/write access for the agent.

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 2005Q4 but you do not upgrade Delegated Administrator. For information about upgrading Delegated Administrator, see the *Sun Java Enterprise System 2005Q4 Upgrade Guide*.

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.

Installation Issues

After applying patch 1, `/tmp/amsilent` file allows read access for all users (6370691)

After you apply patch 1, the `/tmp/amsilent`file allows read access for all users.

Workaround: After you apply the patch, reset the permissions for the file to allow read access only by the Access Manager administrator.

On SDK install with container configuration, notification URL is not correct (6327845)

If you perform an SDK installation with the container configuration (DEPLOY_LEVEL=4), the notification URL is not correct.

Workaround:

1. Set the following property in the `AMConfig.properties` file:

   ```
   com.iplanet.am.notification.url=
   protocol://fqdn:port/amserver/servlet/com.iplanet.services.comm.client.
   PLLNotificationServlet
   ```

2. Restart Access Manager for the new value to take effect.

Access Manager `classpath` refers to expired JCE 1.2.1 package (6297949)

The Access Manager `classpath` refers to Java Cryptography Extension (JCE) 1.2.1 Package (Signing Certificate), which expired on July 27, 2005.

Workaround: None. Although the package reference is in the `classpath` Access Manager does not use this package.

Installing Access Manager on an existing DIT requires rebuilding Directory Server indexes (6268096)

To improve the search performance, Directory Server has several new indexes.

Workaround: After you install Access Manager with an existing Directory Information Tree (DIT), rebuild the Directory Server indexes by running the `db2index.pl` script. For example:

```
# ./db2index.pl -D "cn=Directory Manager" -w password -n userRoot
```

The `db2index.pl` script is available in the *DS-install-directory/slapd-hostname/* directory.

Log and debug directories permissions incorrect for non-root users (6257161)

When a non-root user is specified in the silent install configuration file, permissions on the debug, logs, and starts directories are not set appropriately.

Workaround: Change the permissions on these directories to allow access for a non-root user.

Authentication service is not initialized when Access Manager and Directory Server are installed on separate machines (6229897)

Although the `classpath` and other Access Manager web container environment variables are updated during installation, the installation process does not restart the web container. If you try to login to Access Manager after installation before the web container is restarted, the following error is returned:

```
Authentication Service is not initialized.
Contact your system administrator.
```

Workaround: Restart the web container before you login to Access Manager. Directory Server must also be running before you login.

Installer doesn't add platform entry for existing directory install (6202902)

The Java ES Installer does not add a platform entry for an existing directory server installation (DIRECTORY_MODE=2).

Workaround: Add the Realm/DNS aliases and platform server list entries manually. For the steps, see the "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Upgrade Issues

Access Manager `ampre70upgrade` script does not remove localized packages (6378444)

If you are upgrading Access Manager to Access Manager 7 2005Q4, the `ampre70upgrade` script does not remove any Access Manager localized packages that you have on your system.

Workaround: Before you upgrade to Access Manager 7 2005Q4, use the `pkgrm` command to manually remove any localized Access Manager packages that are installed on your system.

`AMConfig.properties` file has an old version for the web container (6316833)

After Access Manager and Application Server are upgraded to Java ES 2005Q4 versions, the Access Manager `AMConfig.properties` file has an old version of Application Server.

Workaround: Before you run the Delegated Administrator configuration program (`config-commda`), change the following property in the `AMConfig.properties` file:

```
com.sun.identity.webcontainer=IAS8.1
```

Node agent `server.policy` file isn't updated as part of an Access Manager upgrade (6313416)

After upgrading Access Manager, the node agent `server.policy` file isn't updated.

Workaround: Replace the `server.policy` file for the node agent with the following file:

```
/var/opt/SUNWappserver/domains/domain1/config/server.policy
```

After upgrade, Session Property Condition is missing in the Condition list (6309785)

After upgrading Access Manager from version 2005Q1 to version 2005Q4, the Session Property Condition is not displayed as a choice in the policy Condition list if you try to add a Condition to a policy.

Workaround: Select the Session Property Condition type in the policy configuration service template at the corresponding realm.

After upgrade, Identity Subject type is missing from the policy subject list (6304617)

After upgrading Access Manager from version 2005Q1 to version 2005Q4, the Identity Subject, a newly added policy subject type, is not displayed as a choice in the policy subject list.

Workaround: Select the Identity Subject type as a default subject type in the policy configuration service template.

Access Manager upgrade failed because the `classpath` is not migrated (6284595)

During the upgrade of Access Manager from Java ES 2004Q2 to Java ES 2005Q4, the upgrade from Java ES 2004Q2 to Java ES 2005Q1 failed. Access Manager was being deployed on Application Server, which was also being upgraded from Java ES 2004Q2 to Java ES 2005Q4. The `classpath` in the `domain.xml` file did not have Access Manager JAR file paths.

Workaround: Follow these steps:

1. Before running the `amupgrade` script, re-index Directory Server, because of a problem with the `comm_dssetup.pl` script.
2. Add entries for Access Manager to the `server.policy` file of the node agent. A copy of `server.policy` from the default server policy (`/var/opt/SUNWappserver/domains/domain1/config/server.policy`) is sufficient.
3. Update the `classpath` in the `domain.xml` file of the node agent as follows. Copy the `classpath-suffix` and relevant `classpath` from the `server-classpath` attributes of the `java-config` element from the `server.xml` file to the respective attributes in the `java-config` element of `domain.xml`. The `java-config` element can be found under the `config` element in `domain.xml`.

After upgrade, `amadmin` command returns wrong version shown (6283758)

After Access Manager was upgraded from version 6 2005Q1 to version 7 2005Q4, the `amadmin --version` command returned the wrong version: Sun Java System Access Manager version 2005Q1.

Workaround: After you upgrade Access Manager, run the `amconfig` script to configure Access Manager. When you run `amconfig`, specify the full path to the configuration (`amsamplesilent`) file. For example, on a Solaris system:

```
# ./amconfig -s ./config-file
```

or

```
# ./amconfig -s /opt/SUNWam/bin/config-file
```

Add `ContainerDefaultTemplateRole` attribute after data migration (4677779)

The 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.

Configuration Issues

Application Server 8.1 `server.policy` file must be edited when using non-default URIs (6309759)

If you are deploying Access Manager 7 2005Q4 on Application Server 8.1 and you are using non-default URIs for the services, console, and password web applications, which have default URI values of `amserver`, `amconsole`, and `ampassword`, respectively, you must edit the application server domain's `server.policy` file before attempting to access Access Manager via a web browser.

Workaround: Edit the `server.policy` file as follows:

1. Stop the Application Server instance on which Access Manager is deployed.

2. Change to the `/config` directory. For example:

```
cd /var/opt/SUNWappserver/domains/domain1/config
```

3. Make a backup copy of the `server.policy` file. For example:

```
cp server.policy server.policy.orig
```

4. In the `server.policy` file, look for the following policies:

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amserver/-" { ...
};
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amconsole/-" { ...
};
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/ampassword/-" { ...
};
```

5. Replace `amserver` with the non-default URI used for the services web application in the following line:

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amserver/-" {
```

6. For legacy mode installations, replace `amconsole` with the non-default URI used for the console web application in the following line:

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amconsole/-" {
```

7. Replace `ampassword` with the non-default URI used for the password web application in the following line:

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/ampassword/-" {
```

8. Start the Application Server instance on which Access Manager is deployed.

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 "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Data validation for required attributes in the services (6308653)

Access Manager 7 2005Q4 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 2005Q4 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 "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning 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
```

URL signing failed in IBM WebSphere when using RSA key (6271087)

When using an RSA key in IBM WebSphere, the signing of URL string failed with the following exception:

```
ERROR: FSSignatureUtil.signAndReturnQueryString: FSSignatureException
occured while signing query string: no such provider: SunRsaSign
```

Workaround: The "SunRsaSign" provider is missing from the WebSphere bundled JDK. To fix this problem, edit the *websphere_jdk_root*`/jre/lib/security/java.security` file and add following line to enable "SunRsaSign" as one of the providers:

```
security.provider.6=com.sun.rsajca.Provider
```

Access Manager Console Issues

For SAML, duplicate Trusted Partner console edit errors (6326634)

In the Access Manager Console, create SAML Trusted Partner under the Federation > SAML tab. If you try to duplicate the Trusted Partner, errors occur.

Workaround: None. This problem is fixed in patch 1. See "Access Manager 7 2005Q4 Patch 1" on page 67 for information about applying the patch for your specific platform.

Remote logging is not working for `amConsole.access` and `amPasswordReset.access` (6311786)

When remote logging is configured, all logs are written to the remote Access Manager instance except `amConsole.access`and `amPasswordReset.access` for the password reset information. The log record is not written anywhere.

Workaround: None.

Adding more `amadmin` properties in the console is changing the `amadmin` user password (6309830)

Adding or editing some of the properties for the `amadmin` user in the administration console causes the `amadmin` user password to change.

Workaround: None. This problem is fixed in patch 1. See "Access Manager 7 2005Q4 Patch 1" on page 67 for information about applying the patch for your specific platform.

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

The new Access Manager 7 2005Q4 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.

Exception error occurs when adding a group to a user as a policy admin user (6299543)

The Access Manager Console returns an exception error when you add a group to a user as a policy admin user.

Workaround: None.

In legacy mode, you cannot delete all users from a role (6293758)

In legacy mode, if you try to delete all users from a role, a user is left.

Workaround: Try again to delete the user from the role.

Cannot add, delete, or modify Discovery Service resource offerings (6273148)

The Access Manager Administration Console does not allow you to add, delete, or modify the resource offerings for a user, role, or realm.

Workaround: None. This problem is fixed in patch 1. See "Access Manager 7 2005Q4 Patch 1" on page 67 for information about applying the patch for your specific platform.

Wrong LDAP bind password should give error for the subject search (6241241)

The Access Manager Administration Console is not returning an error when the wrong LDAP bind password is used.

Workaround: None.

Access Manager cannot create an organization under a container in legacy mode (6290720)

If you create a container and then try to create an organization under the container, Access Manager returns a “uniqueness violation error”.

Workaround: None.

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

Portal Server and Access Manager are installed on the same serve. 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.

SDK and Client Issues

Can't remove Session Service configuration for a subrealm (6318296)

After creating a subrealm of the top-level realm and adding the Session Service to it, a subsequent attempt to remove the Session Service configuration caused an error message.

Workaround: Remove the default top-level ID repository, AMSDK1, and then add this repository back into the configuration.

This problem is fixed in patch 1. See "Access Manager 7 2005Q4 Patch 1" on page 67 for information about applying the patch for your specific platform.

CDC servlet redirecting to the invalid login page when policy condition is specified (6311985)

With the Apache agent 2.2 in CDSSO mode, when accessing the agent protected resource, the CDC servlet redirects the user to the anonymous authentication page, instead of the default login page.

Workaround: None. This problem is fixed in patch 1. See "Access Manager 7 2005Q4 Patch 1" on page 67 for information about applying the patch for your specific platform.

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. See "Access Manager 7 2005Q4 Patch 1" on page 67 for information about applying the patch for your specific platform.

Command-Line Utilities Issues

Null attribute LDAP search returns an error when Access Manager points to Directory Proxy (6357975)

If you are using Sun Java System Directory Proxy Server, a null attribute LDAP search returns an error. For example:

```
# ldapsearch -b base-dn uid=user ""
```

If Access Manager points directly to the LDAP director server, the same search is successful.

Workaround: If you are using Directory Proxy Server, either enable null attribute searches or supply an attribute name for the search.

New schema files are missing from `amserveradmin` script (6255110)

After installation, when you need to run `amserveradmin` script to load the services into Directory Server, the script is missing the `defaultDelegationPolicies.xml` and `idRepoDefaults.xml` schema files.

Workaround: Manually load the `defaultDelegationPolicies.xml` and `idRepoDefaults.xml` files using the `amadmin` CLI tool with the `-t`option.

Cannot save XML documents with escape character in Internet Explorer 6.0 (4995100)

If you add a special character (such as the string "`amp;`" next to an "`&`") in an XML file, the file will save properly, however; if you later retrieve the XML profile using Internet Explorer 6.0, the file doesn't display properly. If you then try to save the profile again, an error is returned.

Workaround: None.

Authentication Issues

`UrlAccessAgent` SSO Token is expiring (6327691)

The `UrlAccessAgent` SSO Token is expiring because the application module does not return the special user `DN`, which causes the special user `DN` match and hence a non-expiring token to fail.

Workaround: None. This problem is fixed in patch 1. See "Access Manager 7 2005Q4 Patch 1" on page 67 for information about applying the patch for your specific platform.

Unable to login to subrealm with LDAPV3 plugin/dynamic profile after correcting password (6309097)

In realm mode, if you create an ldapv3 datastore in a realm with a "wrong" password and you later change the password as `amadmin`, when you try to login again as the user with the changed password, the logon fails, saying that no profile exists.

Workaround: None.

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

Access Manager instances across time zones timeout other user sessions (6323639)

Access Manager instances installed across different time zones and in the same circle of trust cause user sessions to timeout.

Session failover (`amsfoconfig`) script has incorrect permissions on Linux 2.1 system (6298433)

The session failover configuration script (`/opt/sun/identity/bin/amsfoconfig`) has incorrect permissions and is not executable on Linux 2.1 system.

Workaround: Change the permissions to make the `amsfoconfig` script executable (for example, 755).

This problem is fixed in patch 1. See "Access Manager 7 2005Q4 Patch 1" on page 67 for information about applying the patch for your specific platform.

Session failover (`amsfoconfig`) script fails on Linux 2.1 system (6298462)

The session failover configuration script (`amsfoconfig`) fails on Linux 2.1 server because the tab character (`\t`) is not being interpreted correctly.

Workaround: Configure session failover manually. For the steps, see "Configuring Session Failover Manually" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

This problem is fixed in patch 1. See "Access Manager 7 2005Q4 Patch 1" on page 67 for information about applying the patch for your specific platform.

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 (No CR number)

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)

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)" on page 97
- "Using BEA WebLogic Server as a web container" on page 97

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

Access Manager 7 2005Q4 startup returns the debug errors in `amDelegation` and `amProfile` debug files:

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

Workaround: None. You can ignore these messages.

Using BEA WebLogic Server as a web container

If you deploy Access Manager using BEA WebLogic Server as the web container, Access Manager might not be accessible.

Workaround: Restart WebLogic Server a second time for Access Manager to be accessible.

Linux OS Issues

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: 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;
```

Federation and SAML Issues

Running the web services sample returns "Resource offering not found" (6359900)

When Access Manager is configured to access the web services samples under the *AccessManager-base*`/SUNWam/samples/phase2/wsc` directory on Solaris systems or the *AccessManager-base*`/identity/samples/phase2/wsc` directory on Linux systems, querying the Discovery Service or modifying the Resource Offering returns the error message: "Resource offering not found".

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

Workaround:

1. Go to the following samples directory: *AccessManager-base*`/SUNWam/samples/phase2/wsc`) directory on Solaris systems or the *AccessManager-base*`/identity/samples/phase2/wsc` directory on Linux systems
2. In the `index.jsp` file, search for the following string:

   ```
   com.sun.org.apache.xml.security.utils.XMLUtils.outputDOM
   ```
3. Immediately before the line that contains the string you found in the previous step, insert the following new line:

   ```
   com.sun.org.apache.xml.security.Init.init();
   ```
4. Re-run the sample. (You do not need to restart Access Manager.)

Federation fails when using Artifact profile (6324056)

If you setup an identity provider (IDP) and a service provider (SP), change the communication protocol to use the browser Artifact profile, and then try to federate users between the IDP and SP, the federation fails.

Workaround: None.

Special characters (&) in SAML statements should be encoded (6321128)

With Access Manager as the source site and destination site and SSO configured, an error occurs in the destination site, because the special character (&) in the SAML statements is not encoded and hence the parsing of assertion fails.

Workaround: None. This problem is fixed in patch 1. See "Access Manager 7 2005Q4 Patch 1" on page 67 for information about applying the patch for your specific platform.

Exception occurs when trying to add Disco Service to a role (6313437)

In the Access Manager Console, if you try to add a resource offering to the Disco Service, an unknown exception occurs.

Workaround: None.

Auth Context attributes are not configurable until you have configured and saved other attributes (6301338)

Auth Context attributes are not configurable until you have configured and saved other attributes.

Workaround: Configure and save a provider profile before you configure the Auth Context attributes.

EP Sample does not work if root suffix contains "&" character (6300163)

If Directory Server has a root suffix that contain the "&" character and you try to add an Employee Profile Service Resource Offering, an exception is thrown.

Workaround: None.

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

- "Multibyte characters are displayed as question marks in log files (5014120)" on page 101

User locale preferences are not applied to the whole administration console (6326734)

Parts of the Access Manager administration console are not following the user locale preferences but instead using the browser locale settings. This problem affects the Version, Logout and online help buttons as well as the contents of the Version and online help.

Workaround: Change the browser settings to the same locale as user preferences.

Online help is not fully available for European languages if Access Manager is deployed on IBM WebSphere (6325024)

In all European locales (Spanish, German, and French), the online help is not fully accessible when Access Manager is deployed on an IBM WebSphere Application Server instance. The online help displays "Application Error" for these frames:

- Upper frame, where the Help and Close buttons should be.
- Left frame, where the Contents, Index, and Search buttons should be.

Workaround: Set your browser language setting to English and refresh the page to access the left frame. The upper frame, however, will still display "Application Error."

Version information is blank when Access Manager is deployed on IBM WebSphere (6319796)

In any locale, when Access Manager is deployed on an IBM WebSphere Application Server instance, the product version is not visible when you click the Version button. A blank page is displayed instead.

Workaround: None.

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 2005Q4 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.

Multibyte characters are displayed as question marks in log files (5014120)

Multibyte 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

Document that Access Manager cannot revert from Realm Mode to Legacy Mode (6508473)

If you install Access Manager 7 2005Q4 in Realm Mode, you cannot revert to Legacy Mode.

If you install Access Manager 7 2005Q4 in Legacy Mode, however, you can change to Realm Mode by using the `amadmin` command with the `-M` option. For example:

```
amadmin -u cn=amAdmin,ou=People,dc=example,dc=com -w amadmin-password
-M dc=example,dc=com
```

Document more information about disabling persistent searches (6486927)

Access Manager uses persistent searches to receive information about Sun Java System Directory Server entries that change. By default, Access Manager creates the following persistent search connections during server startup:

`aci` - Changes to the `aci` attribute, with the search using the LDAP filter (`aci=*`)

`sm` - Changes in the Access Manager information tree (or service management node), which includes objects with the `sunService` or `sunServiceComponent` marker object class. For example, you might create a policy to define access privileges for a protected resource, or you might modify the rules, subjects, conditions, or response providers for an existing policy.

`um` - Changes in the user directory (or user management node). For example, you might change a user's name or address.

Caution – Disabling persistent searches for any of these components is not recommended, because a component with a disabled persistent search does not receive notifications from Directory Server. Consequently, changes made in Directory Server for that particular component will not be notified to the component cache, and the component cache will go stale.

For example, if you disable persistent searches for changes in the user directory (`um`), the Access Manager server will not receive notifications from Directory Server. Therefore, an agent would not get notifications from Access Manager to update its local user cache with the new values for the user attribute. Then, if an application queries the agent for the user attributes, it might receive the old value for that attribute.

Use this property only in special circumstances when absolutely required. For example, if you know that Service Configuration changes (related to changing values to any of services such as Session Service and Authentication Services) will not happen in production environment, the persistent search to the Service Management (`sm`) component can be disabled. However, if any changes occur for any of the services, a server restart would be required. The same condition also applies to other persistent searches, specified by the `aci` and `um` values.

For more information, see "CR# 6363157: New property disables persistent searches if absolutely required" on page 66.

Document Access Manager supported and unsupported privileges (2143066)

Privileges define the access permissions to administrators who are members of roles or groups that exist within a realm. Access Manager allows you to configure permissions for the following administrator types:

- Realm administrators can perform all realm-related tasks, including defining identity repositories (data stores), configuring authentication, and defining policies.
- Policy administrators can configure policies in existing realms.

The following privileges are supported:

- Read and write access to all realm and policy properties. Defines read and write access privileges for realm administrators.
- Read and write access for only policy properties. Defines read and write access privileges for policy administrators.
- Combination of supported privileges: Read and write access only for policy properties and read only access to data stores. Other combinations of privileges are not supported.

Document cookie-based sticky request routing (6476922)

When Access Manager servers are deployed behind a load balancer, cookie-based sticky request routing prevents a client request from being misrouted to an incorrect Access Manager server (that is, to a server that is not hosting the session). This feature was implemented in Access Manager 7 2005Q4 patch 3.

In the previous behavior, without cookie-based sticky request routing, requests from non-browser based clients (such as policy agents and clients using the remote Access Manager client SDK) were often misrouted to an Access Manager server that was not hosting the session. Then, in order to send the request to the correct server, the Access Manager server had to validate the session using back-channel communication, which usually caused some performance degradation. Cookie-based sticky request routing prevents the need for this back-channel communication and thus improves Access Manager performance.

To implement cookie-based sticky request routing, the Access Manager deployment must be configured as a site. For information, see "Configuring an Access Manager Deployment as a Site" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

To configure cookie-based sticky request routing:

1. To specify a cookie name, set the `com.iplanet.am.lbcookie.name` property in the `AMConfig.properties` file. Access Manager then generates the load balancer cookie value using the two-byte server ID (such as 01, 02, and 03). If you do not specify a cookie name, Access Manager generates the load balancer cookie value using the default name `amlbcookie` plus the two-byte server ID.

   If you set the cookie name on the Access Manager server, you must use the same name in the `AMAgent.properties` file for a Policy Agent. Also, if you are using the Access Manager client SDK, you must also use the same cookie name used by the Access Manager server.

   Note: Do not set the `com.iplanet.am.lbcookie.value` property, because Access Manager sets the cookie value using the two-byte server ID.
2. Configure your load balancer with the cookie name from Step 1. You can use a hardware or software load balancer with your Access Manager deployment.
3. If session failover is implemented, enable the `com.sun.identity.session.resetLBCookie` property for both Policy Agents and the Access Manager server.
   - For a Policy Agent, add and enable the property in the `AMAgent.properties` file.
   - For the Access Manager server, add and enable the property in the `AMConfig.properties` file.

   For example:

   ```
   com.sun.identity.session.resetLBCookie='true'
   ```

If a failover situation occurs, the session is routed to a secondary Access Manager server, and the load balancer cookie value is set using the server ID for the secondary Access Manager server. Any subsequent requests for the session are then routed to the secondary Access Manager server.

Document Windows Desktop SSO configuration for Windows 2003 (6487361)

To configure Windows Desktop SSO on Windows 2003, as described in the "Configuring Windows Desktop SSO" in *Sun Java System Access Manager 7 2005Q4 Administration Guide*, use the following `ktpass` command:

```
ktpass /out filename /mapuser username
/princ HTTP/hostname.domainname /crypto encryptiontype /rndpass
/ptype principaltype /target domainname
```

For example:

```
ktpass /out demo.HTTP.keytab
/mapuser http /princ HTTP/demo.identity.sun.com@IDENTITY.SUN.COM
/crypto RC4-HMAC-NT /rndpass /ptype KRB5_NT_PRINCIPAL /target IDENTITY.SUN.COM
```

For the syntax definitions, see the following site:

`http://technet.microsoft.com/en-us/library/cc779157(WS.10).aspx`

Document steps to set up Distributed Authentication UI server passwords (6510859)

The following procedure describes how to set up the encrypted passwords for a Distributed Authentication UI server that communicates with an Access Manager server.

To set up the passwords for a Distributed Authentication UI server:

1. On the Access Manager server:
   a. Encrypt the `amadmin` password using the `ampassword -e` utility. For example, on Solaris systems:

      ```
      # cd /opt/SUNWam/bin
      # ./ampassword -e amadmin-password
      AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      ```

      Save this encrypted value.

   b. Copy and save the `am.encryption.pwd` property value from the Access Manager server's `AMConfig.properties` file. For example:

      ```
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```

2. On the Distributed Authentication UI server, make these changes to the `AMConfig.properties` file:

a. Comment out the `com.iplanet.am.service.password` property.

b. Set the `com.iplanet.am.service.secret` property to the encrypted `amadmin` password from Step 1a.

c. Add the `am.encryption.pwd` and encrypted value that you copied from Step 1b. For example:

```
com.sun.identity.agents.app.username=username
#com.iplanet.am.service.password=password
com.iplanet.am.service.secret=AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
```

3. Restart the Distributed Authentication UI server.

Online Help for "To create a new site name" needs more information (2144543)

The Access Manager Console online Help is missing the Save step for "To create new site name" under Configuration>System Properties>Platform. If you don't click Save after adding a new site name and you then try to add an instance name, the process fails. Therefore, always click Save after adding the site name, and then add the instance name.

Document that administrator password configuration parameter is `ADMIN_PASSWD` on Windows systems (6470793)

On Solaris and Linux systems, the Access Manager administrator (`amadmin`) password configuration parameter in the `amsamplesilent` file is `ADMINPASSWD`. On Windows systems, however, the parameter in the `AMConfigurator.properties` file is `ADMIN_PASSWD`.

If you are running `amconfig.bat` on Windows systems, set the `amadmin` password in the `AMConfigurator.properties` file using the `ADMIN_PASSWORD` parameter and not `ADMINPASSWD`.

Release Notes have wrong workaround for known issue (6422907)

Step 3 of the workaround for "Running the web services sample returns "Resource offering not found" (6359900)" on page 98 has been corrected.

Document `com.iplanet.am.session.protectedPropertiesList` in `AMConfig.properties` (6351192)

The `com.iplanet.am.session.protectedPropertiesList` parameter allows you to protect certain core or internal session properties from remote updates via the `SetProperty` method of the Session Service. By setting this "hidden" key security parameter, you can customize session attributes in order to participate in authorization as well as other Access Manager features. To use this parameter:

1. With a text editor, add the parameter to the `AMConfig.properties` file.
2. Set the parameter to the session properties that you want to protect. For example:

```
com.iplanet.am.session.protectedPropertiesList =
PropertyName1,PropertyName2,PropertyName3
```

3. Restart the Access Manager Web container for the values to take effect.

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 CR 6349959). In the Access Manager 7 2005Q4 Administrator Console, in LDAPv3 configuration for the "LDAPv3 Plugin 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
```

`com.iplanet.am.session.client.polling.enable` on server side must not be true (6320475)

The `com.iplanet.am.session.client.polling.enable` property in the `AMConfig.properties` file must never be set to true on the server side.

Workaround: This property is set to false by default and should never be reset to true.

Default Success URL is incorrect in the console online help (6296751)

The Default Success URL is incorrect in the `service.scserviceprofile.iplanetamauthservice.html` online help file. The Default Success URL field accepts a list of multiple values that specify the URL where users are redirected after successful authentication. The format of this attribute is `clientType|URL`, although you can specify only the value of the URL, which assumes a default type of HTML.

The "`/amconsole`" default value is incorrect.

Workaround: The correct default value is "`/amserver/console`".

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 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

Sun Java System Access Manager 7 2005Q4 Collection

The following table lists the new and revised Access Manager 7 2005Q4 documents that have been published since the initial release. To access these documents, see the Access Manager 7 2005Q4 collection:

`http://docs.sun.com/coll/1292.1`

TABLE 7 Access Manager 7 2005Q4 Documentation Update History

Title	Publication Date
Sun Java System Access Manager 7 2005Q4 Release Notes	See Table 1.
Sun Java System Access Manager 7 2005Q4 Administration Guide	February 2006
Sun Java System Access Manager 7 2005Q4 Developers Guide	February 2006
Sun Java System Access Manager Policy Agent 2.2 User's Guide	February 2006
Sun Java System Access Manager 7 2005Q4 C API Reference	February 2006
Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide	February 2006
Technical Note: Using Access Manager Distributed Authentication	February 2006
Technical Note: Installing Access Manager to Run as a Non-Root User	February 2006
Sun Java System SAML v2 Plug-in for Federation Services User's Guide	February 2006
Sun Java System SAML v2 Plug-in for Federation Services Release Notes	February 2006
Sun Java System SAMLv2 Plug-in for Federation Services Java API Reference	February 2006
Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide	January 2006
Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide	December 2005
Sun Java System Access Manager 7 2005Q4 Technical Overview	December 2005

Sun Java System Federation Manager 7.0 2005Q4 Collection

To access the documents in the Federation Manager 7.0 2005Q4 collection, see:

`http://docs.sun.com/coll/1321.1`

Sun Java System Access Manager Policy Agent 2.2 Collection

The Access Manager Policy Agent 2.2 collection is revised on an ongoing basis to document new agents. To access the documents in this collection, see:

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

Redistributable Files

Sun Java System Access Manager 7 2005Q4 does not contain any files that you can redistribute to non-licensed users of the product.

How to Report Problems and Provide Feedback

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

- 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

Oracle Welcomes Your Comments

Oracle is interested in improving its documentation and welcomes your comments and suggestions. Go to `http://docs.sun.com/` and click the Feedback link.

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 819-2134-28.

Additional 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 Advanced Customer Services for Systems:

  `http://www.oracle.com/us/support/systems/advanced-customer-services/index.html`
- Sun Software Product Map: `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 Services: `http://developers.sun.com/services/`

Oracle's Accessibility Program

For information about Oracle's commitment to accessibility, see the following site:

`http://www.oracle.com/us/corporate/accessibility/index.html`

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.
