Sun Java System Access Manager 7.1 Release Notes

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

Part No: 819–4683–10
March 2007

070301@16599

Contents

Sun Java System
Access Manager 7.1 Release Notes

March 2007

Part Number 819-4683-10

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

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

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

These Release Notes Contain the following sections:

Revision History

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

TABLE 1 Revision History

Date	Description of Changes
July 2006	Beta release.
March 2007	Java Enterprise System 5 release

About Sun Java System Access Manager 7.1

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

Access Manager provides these main functions:

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

What's New in This Release

This release includes the following new features:

- "Java ES Monitoring Framework Integration" on page 6
- "Web Service Security " on page 7
- "Single Access Manager WAR file deployment" on page 7
- "Enhancements to Core Services" on page 7
- "Deprecation Notification and Announcement" on page 10

Java ES Monitoring Framework Integration

Access Manager 7.1 integrates with the Java Enterprise System monitoring framework through Java Management Extensions (JMX). JMX technology provides the tools for building distributed, Web-based, modular, and dynamic solutions for managing and monitoring

devices, applications, and service-driven networks. Typical uses of the JMX technology include: consulting and changing application configuration, accumulating statistics about application behavior, notification of state changes and erroneous behaviors. Data is delivered to centralized monitoring console.

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

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

Web Service Security

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

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

Single Access Manager WAR file deployment

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

Enhancements to Core Services

Web Containers supported

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

Monitoring Framework Integration

Access Manager can use the JES Monitoring Framework to monitor the following:

1. Authentication
   - Number of authentications attempted
   - Number of remote authentications attempted (optional)

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

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

Authentication module

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

Policy module

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

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

Service Management module

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

Access Manager SDK

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

Web Services support

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

Installation module

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

Delegation module

- Support for grouping of delegation privileges

Upgrade

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

Logging

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

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

Deprecation Notification and Announcement

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

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

Hardware and Software Requirements

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

TABLE 2 Hardware and Software Requirements

Component	Requirement
Operating system (OS)	■ Solaris™10 on SPARC, x86, and x64 based systems, including support for whole root local and sparse root zones. ■ Solaris 9 on SPARC and x86 based systems. ■ Red Hat™ Enterprise Linux 3 and 4, all updates Advanced Server (32 and 64–bit versions) and Enterprise Server (32 and 64–bit versions) ■ Windows Windows 2000 Advanced Server, Data Center Server version SP4 on x86 Windows 2003 Standard (32 and 64–bit versions), Enterprise (32 and 64–bit versions), Data Center Server (32–bit version) on x86 and x64 based systems Windows XP Professional SP2 on x86 based systems HP-UX 11i v1 (11.11 from uname), 64–bit on PA-RISC 2.0 For the most updated list of supported operating systems, see "Platform Requirements and Issues" in *Sun Java Enterprise System 5 Release Notes for UNIX* in the *Sun Java Enterprise System 5 Release Notes for UNIX*, or "Hardware and Software Platform Information" in *Sun Java Enterprise System 5 Release Notes for Microsoft Windows* in the *Sun Java Enterprise System 5 Release Notes for Windows*.
Java 2 Standard Edition (J2SE)	J2SE platform 6.0, 5.0 Update 9 (HP-UX: 1.5.0.03), and 1.4.2 Update 11
Directory Server	Access Manager information tree: Sun Java System Directory Server 6.0 or Sun Java System Directory Server 5.2 2005Q4 Access Manager identity repository: Sun Java System Directory Server 6.0 or Microsoft Active Directory

TABLE 2 Hardware and Software Requirements *(Continued)*

Component	Requirement
Web containers	Sun Java System Web Server 7.0 On supported platform/OS combinations you may elect to run the Web Server instance in a 64 bit JVM. Support platforms: Solaris 9/SPARC, Solaris 10/SPARC, Solaris 10/AMD64, Red Hat AS or ES 3.0/AMD64, Red Hat AS or ES 4.0/AMD64
	Sun Java System Application Server Enterprise Edition 8.2
	BEA WebLogic 8.1 SP4
	IBM WebSphere Application Server 5.1.1.6
RAM	Basic testing: 512 Mbytes
	Actual deployment: 1 Gbyte for threads, Access Manager SDK, HTTP server, and other internals
Disk space	512 Mbytes for Access Manager and associated applications

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

Supported Browsers

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

TABLE 3 Supported Browsers

Browser	Platform
Firefox 1.0.7	Windows XP
	Windows 2000
	Solaris OS, versions 9 and 10
	Red Hat Linux 3 and 4
	Mac OS X
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows™ 2000

TABLE 3 Supported Browsers *(Continued)*

Browser	Platform
Mozilla™ 1.7.12	Solaris OS, versions 9 and 10
	Windows XP
	Windows 2000
	Red Hat Linux 3 and 4
	Mac OS X
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000
Netscape Communicator 7.1	Solaris OS, versions 9 and 10

General Compatibility Information

AMSDK intersystem incompatibility with Access Manager server

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

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

Upgrade not supported for Access Manager HPUX version

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

Access Manager Legacy Mode

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

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

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

- "Java ES Silent Installation Using a State File" on page 14
- ""Configure Now" Installation Option in Graphical Mode" on page 14
- ""Configure Now" Installation Option in Text-Based Mode" on page 14
- ""Configure Later" Installation Option" on page 15

To determine the more for an Access Manager 7.1 installation, see "Determining the Access Manager Mode" on page 15.

Java ES Silent Installation Using a State File

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

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

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

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

"Configure Now" Installation Option in Graphical Mode

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

"Configure Now" Installation Option in Text-Based Mode

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

"Configure Later" Installation Option

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

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

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

Determining the Access Manager Mode

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

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

Results are:

- true: Realm mode
- false: Legacy mode

Access Manager Policy Agents

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

TABLE 4 Policy Agents Compatibility With Access Manager 7.1 Modes

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

Known Issues and Limitations

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

Installation Issues

Information about installation issues is contained in the JES5 Release Notes. See the section "Access Manager Installation Issues" in *Sun Java Enterprise System 5 Release Notes for UNIX*.

Upgrade Issues

Information about upgrade issues is contained in section "Upgrade Issues" in *Sun Java Enterprise System 5 Release Notes for UNIX* in the *Sun Java Enterprise System 5 Release Notes for UNIX*.

Compatibility Issues

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

The problem occurs after you install Access Manager, Messaging Server, and Calendar Server and configure them to work together, and then install the JES5 120955-01 patch. The user encounters a login error. The error is due to an incompatibility between Policy Agent 2.1 properties and AMSDK. There is no workaround at this time. This problem will be fixed in the final Access Manager 7.1 release.

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

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

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

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

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

   Change the stack size value to at least 261144, and then click Save.
5. Click the "Deployment Pending" link in the upper right corner of the screen.

   In the Configuration Deployment page, click the Deploy button.
6. In the Results window, click OK to restart the Web Server instance.

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

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

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

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

Workaround: None.

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

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

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

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

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

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

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

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

4. Restart the Access Manager web container.

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

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

Workaround: See the workaround for the previous problem.

Configuration Issues

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

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

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

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

When a password is changed, Access Manager submits the email notification using an unqualified sender name `Identity-Server` which results in errors entries in the `amPasswordReset` logs. 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 configuration in `/opt/SUNWam/locale/amPasswordResetModuleMsgs.properties.`

- Change the from address. Change `fromAddress.label=<Identity-Server>` to `fromAddress.label=<IdentityServer@myhost.company.com>`
- Change the `lockOutEmailFrom` property to insure that lockout notifications use the correct `from` address.

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

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

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

Data validation for required attributes in the services (6308653)

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

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

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

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

Workaround: Follow these steps:

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

   Find the following line containing the `wl8_classpath`:

   ```
   wl8_classpath= ...
   ```

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

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

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

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

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

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

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

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

```
AM_REALM = disabled
```

Access Manager Console Issues

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

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

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

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

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

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

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

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

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

Add `ContainerDefaultTemplateRole` attribute after data migration (4677779)

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

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

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

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

Command Line Issue

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

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

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

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

5. Click Save.

SDK and Client Issues

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

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

Workaround: None.

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

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

Workaround: Restart the client after a service schema change.

This problem is fixed in patch 1.

Authentication Issues

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

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

Workaround: Create a new user with appropriate privileges.

To create a new user with the proper ACIs:

1. In the Access Manager console, create a new user. For example, create a user named `AuthUIuser`.

2. In Directory Server console , add the following ACI.

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

   Notice that the `userdn` is set to `"ldap:///<AuthUIuser's DN>"`.

3. See the instructions in the "To Install and Configure a Distributed Authentication UI Server" in *Sun Java System Access Manager 7.1 Postinstallation Guide* for editing the `amsilent` file, and for running the `amadmin` command.
4. In the `amsilent`file, set the following properties:

APPLICATION_USER	Enter `AuthUIuser`.
APPLICATION_PASSWD	Enter a password for `AuthUIuser`.

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

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

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

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

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

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

Workaround: None.

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

After you install Access Manager, login as `amadmin` and add the `o`, `sunPreferredDomain`, `associatedDomain`, `sunOrganizationAlias`, `uid`, and `mail` attributes to the Unique Attribute

List. If you create two new organizations with the same name, the operation fails, but Access Manager displays the "organization already exists" message rather than the expected "attribute uniqueness violated" message.

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

Session and SSO Issues

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

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

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

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

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

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

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

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

Using `HttpSession` with third-party web containers

The default method of maintaining sessions for authentications is "internal session" instead of `HttpSession`. The default invalid session maximum time value of three minutes is sufficient. The `amtune` script sets the value to one minute for Web Server or Application Server. However,

if you are using a third-party web container (IBM WebSphere or BEA WebLogic Server) and the optional `HttpSession`, you might need to limit the web container's maximum `HttpSession` time limit to avoid performance problems.

Policy Issues

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

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

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

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

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

Server Startup Issues

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

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

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

Workaround: None. You can ignore these messages.

AMSDK Issues

Error displayed when performing AMIdentity.modifyService (6506448)

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

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

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

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

The problem occurs under the following conditions:

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

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

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

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

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

Example: `HostName.PRC.Example.COM`

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

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

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

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

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

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

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

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

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

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

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

SSL Issue

- "The amconfig script fails when SSL certificate is expired. (6488777)" on page 29

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

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

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

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

Samples Issue

- "Clientsdk samples directory contains unwanted makefile (6490071)" on page 29

Clientsdk samples directory contains unwanted makefile (6490071)

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

```
.../clientsdk-samples/
```

```
.../clientsdk-webapps/
```

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

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

Linux OS Issues

- "JVM problems occur when running Access Manager on Application Server (6223676)" on page 30

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

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

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

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

Windows and HP-UX Issues

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

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

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

HP-UX needs gettext binary with AM while installing JES full stack (6497926)

There is no current workaround for this problem.

Federation and SAML Issues

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.

Logout error occurs in Federation (6291744)

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

Workaround: None.

Globalization (g11n) Issues

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

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

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

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

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

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

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

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

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

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

Workaround: There are two workarounds:

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

  or

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

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

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

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

Documentation Issues

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

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

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

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

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

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

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

Document how to enable XML encryption (6275563)

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

1. If you are using a JDK version earlier than JDK 1.5, download the Bouncy Castle JCE provider from the Bouncy Castle site (`http://www.bouncycastle.org/`). For example, for JDK 1.4, download the `bcprov-jdk14-131.jar` file.
2. If you downloaded a JAR file in the previous step, copy the file to the *jdk_root*`/jre/lib/ext` directory.
3. For the domestic version of the JDK, download the JCE Unlimited Strength Jurisdiction Policy Files from the Sun site (`http://java.sun.com`) 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

To access these documents, see the Access Manager 7.1 collection:

`http://docs.sun.com/coll/1292.1`

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

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

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

Redistributable Files

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

How to Report Problems and Provide Feedback

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

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

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

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

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

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. Go to `http://docs.sun.com/` and click Send Comments.

Provide the full document title and part number in the appropriate fields. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the part number of the *Access Manager Release Notes* is 819-4683-10.

Additional Sun Resources

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

- Sun Java Enterprise System Documentation: `http://docs.sun.com/prod/entsys.05q4`
- Sun Services: `http://www.sun.com/service/consulting/`
- Software Products and Service: `http://wwws.sun.com/software/`
- Support Resources `http://sunsolve.sun.com/`
- Developer Information: `http://developers.sun.com/`
- Sun Developer Support Services: `http://www.sun.com/developers/support/`

Accessibility Features for People With Disabilities

To obtain accessibility features that have been released since the publishing of this media, consult Section 508 product assessments available from Sun upon request to determine which versions are best suited for deploying accessible solutions. Updated versions of applications can be found at `http://sun.com/software/javaenterprisesystem/get.html`.

For information on Sun's commitment to accessibility, visit `http://sun.com/access`.

Related Third-Party Web Sites

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

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