Sun Java System Access Manager 7.1 2006Q4 Release Notes

Beta

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

Part No: 819–4683–05
July 2006

060724@15490

Contents

Sun Java System Access Manager 7.1 2006Q4 Release Notes

July 2006

Part Number 819-4638-05

The Sun Java^{TM} System Access Manager 7.1 2006Q4 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.

Contents

The Access Manager 7.1 2006Q4 Release Notes contain the following sections:

- “Additional Sun Resources” on page 41

  “Related Third-Party Web Sites” on page 42

Revision History

The following table shows the Access Manager 7.1 2006Q4 Release Notes revision history.

TABLE 1 Revision History

Date	Description of Changes
July 2006	Beta release.

About Sun Java System Access Manager 7.1 2006Q4

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 organizations 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

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
- Number of active sessions, statistics from session failover DB
- Session failover database statistics
- Policy caching statistics
- Policy evaluation transaction times
- Number of assertions for a given provider in a SAML/Federation deployment

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
- Provides two JSR 196 providers: Liberty ID-WSF SOAP provider and HTTP Basic SSO provider
- Integrates with Sun Application Server 9.0

  Manages configuration through NetBeans Enterprise Pack
- 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 (optional)
   - Transaction time for each module if possible (running and waiting states)
   - Connectivity failures for backend servers
2. Sessions
   - Size of the session table (hence maximum number of sessions)
   - Number of active sessions (incremental counter)
   - Session failover: number of "stored" sessions, or session count (incremental counter) and number of operations performed on the failover DB (read, write, delete, # of operations)
3. User Management / Identity Repository/ Session Management Service
   - Maximum cache size
   - Cache-related statistics such as number of hits, ratio, peak, current size, and so forth
   - Transaction time for operations (running and waiting)
4. Policy
   - Number of policies in cache
   - Number of `policyManagers` in cache
   - Number of service names in `policyListeners` cache
   - Number of services in `resultsCache`
   - Number of `tokenIDs` in `sessionListernerRgistry`
   - Number of `serviceNames` in `policyListenerRegistry`
   - Number of `tokenIDs` in role cache
   - Number of `serviceNames` in `resourceNames` cache
   - Number of entries for `SubjectEvaluationCache`
   - Number of `PolicyEvaluators` in cache
   - Number of policy change listeners in cache
   - Transaction time for policy evaluation processing
5. Federation
   - Number of artifacts in table for provider <X>
   - Number of assertions in table for provider <X>
   - Number of session entries in <X> table for provider <ID>
6. SAML
   - Size of artifact map
   - Size of assertion map

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 to support custom policy 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 to support Certificate authentication module - adding `CertAuth` to Distributed Authentication UI to make it a full featured credential extractor presentation

Policy module

- Support for policy definition based on service-based authentication
- A new policy condition added: `AuthenticateToRealmCondition`
- Support for one level wild card compare to facilitate protecting the contents of the directory without protecting sub-directory
- Support for LDAP filter condition - Policy admin can specify an LDAP filter in the Condition while defining policy

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

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 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)
Java 2 Standard Edition (J2SE)	J2SE platform 6.0, 5.0 Update 7 (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 2006Q4 or Sun Java System Directory Server 5.2 2005Q4 Access Manager identity repository: Sun Java System Directory Server 6.0 2006Q4 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 2006Q4 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

- "Access Manager Legacy Mode" on page 12
- "Access Manager Policy Agents" on page 14

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 12
- ""Configure Now" Installation Option in Graphical Mode" on page 13
- ""Configure Now" Installation Option in Text-Based Mode" on page 13
- ""Configure Later" Installation Option" on page 13

To determine the more for an Access Manager 7.1 2006Q4 installation, see "Determining the Access Manager Mode" on page 13.

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 2006Q4 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 2006Q4 Administration Guide*.

Determining the Access Manager Mode

To determine whether a running Access Manager 7.1 2006Q4 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 2006Q4 modes.

TABLE 4 Policy Agents Compatibility With Access Manager 7.1 2006Q4 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

Known Issues and Limitations in Access Manager 7.1 Beta

The following are known issues and limitations that have been identified after Access Manager 7.0 was released. Many of these may be fixed after the 7.1 Beta release.

For information about issues and limitations identified in previous Access Manager releases, see "Older Known Issues and Limitations" on page 22

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 2006Q4 Release Notes.*

Upgrade Issues

Information about upgrade issues is contained in the JES5 Release Notes. See the section "Access Manager Upgrade Issues" in *Sun Java Enterprise System 2006Q4 Release Notes.*.

Uninstallation Issues

Information about uninstallation issues is contained in the JES5 Releaes Notes. See the section "Access Manager Uninstallation Issues" in *Sun Java Enterprise System 2006Q4 Release Notes.*.

Compatibility Issues

The amconsole Login Page is different after an upgrade of Access Manager (6295051)

The amconsole Login Page that is displayed after a fresh install is different from the amconsole Login Page after an upgrade of Access Manager from Java Enterprise System 3 to Java Enterprise System 4. The Logout page that is displayed is also different between a fresh install and an Access Manager upgrade.

Workaround: Restart the Mozilla browser to get the correct login or logout page.

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

The problem occurs after you install Access Manager, Messaging Server, and Calander 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 AMDK. There is no workaround at this time. This problem will be fixed in the final Access Manager 7.1 release.

Applications deployed on an SDK-only instance container are not accessible (6374625)

This problem occurs when you install Access Manager using the SDK-only installation option. During server startup, some lines in the file `servconfig.xml` are not tag-swapped properly. Error messages are displayed, and applications deployed on the container are not accessible.

Access to JES Monitoring Framework fails (6378913)

Access Manager uses `MfManagedElementServerFactory.makeManagedElementServer()`, to gain access to the JES Monitoring Framework's managed element server. This call, which is performed in a servlet loaded on a web container, fails if the following directory isn't present:

On Solaris, `/var/opt/SUNWmfwk/logs/`

On Linux, `/var/opt/sun/mfwk/logs/`

No workaround exists at this time.

Access Manager does not update the Application Server `domain.xml` (6439597)

Access Manager does not update the Application Server `domain.xml` properly with JVM options and server classpath . This is known to occur in the following scenario:

1. You install Application Server and Directory Server.

2. You create a node agent.
3. You create a non-default Application Server instance.
4. You install Access Manager in “Configure Later” mode.
5. You edit and run the `./amconfig -s amsamplesilent` file.
6. When you try to log in to Access Manager with a browser, an error message is displayed.

Workaround: Before installing Access Manager, edit the `amsaplesilent` file so that the container block includes the following information:

```
AS81_HOME=/opt/SUNWappserver/appserver
AS81_PROTOCOL=$SERVER_PROTOCOL
AS81_HOST=$SERVER_HOST
#AS81_HOST=$DISTAUTH_HOST
AS81_PORT=$SERVER_PORT
AS81_ADMINPORT=$ADMIN_PORT
AS81_ADMIN=admin
AS81_ADMINPASSWD="$ADMINPASSWD"
AS81_INSTANCE=server1
AS81_DOMAIN=domain1
AS81_INSTANCE_DIR=/var/opt/SUNWappserver/nodeagents/<nodename>/<server-instance>
AS81_DOCS_DIR=/var/opt/SUNWappserver/nodeagents/<nodename>/<server-instance>/docroot
AS81_ADMIN_IS_SECURE=true
```

After the edits are completed, run the `amconfig` command.

```
./amconfig -s amsamplesilent
```

Access Manager script contains syntax errors (6442374)

The problem occurs when upgrading from JES 3 to JES 5 on Linux. The file `/opt/sun/identity/bin/amws61config` contains the following syntax errors (the space should be deleted):

```
WS61_HOST = $WS_HOST WS61_INSTANCE = $WS_INSTANCE WS61_HOME= $WS_HOME
```

Errors are shown only when “if” conditions are met.

No workaround exists at this time. This problem will be fixed in the final Access Manager 7.1 release.

Exceptions thrown while accessing amconsole on Weblogic (6442196)

The problem occurs under the following conditions:

1. Install BEAWeblogic 8.1sp4.
2. Install Directory Server.
3. Install Access Manager in Configure Later mode.
4. Modify `amsamplesilent` with appropriate values.

5. Run `./amconfig -s amsamplesilent`.

Configuration goes through without any errors. But when you restart the container and the Access Manager in a browser, exceptions are thrown both in the terminal as well as the browser.

The problem will be fixed in the final Access Manager 7.1 release.

Workaround: After running `amconfig` to deploy Access Manager, modify the Weblogic startup scripts.

1. Run `startWebLogic.sh` and `startManagedWeblogic.sh` .
2. On the line which specifies the `IS_OPTIONS`, add the following:

   `-Djava.endorsed.dirs=/usr/share/lib/endorsed`

   After making the change, the `IS_OPTIONS` should look similar to this (assuming that `/bea` is the location where Weblogic was installed) :

```
IS_OPTIONS="-Djava.security.auth.login.config=/bea/user_projects/domains/mydomain/.java.login.config -DLOG_COMPAT
```

3. Restart Weblogic.

Binaries are not installed properly during Access Manager upgrade (6407606)

The problem occurs when upgrading from JES4 on Solaris 10 SPARC non-global zones. The installer displays the following message: “Shared Components are Partially Installed, Access Manager is Installed.” But no Access Manager binaries are installed in the directory `/opt/SUNWam/bin`.

Workaround: Run the JES installer a second time with the same options. Installation should work on the second try.

Deploying Access Manager instances to an Application Server Cluster does not work as designed (6181011)

Workaround: Follow the instructions provided in the following document:

Chapter 1, “Technical Note: Deploying Access Manager Instances to an Application Server Cluster,” in *Technical Note: Deploying Access Manager to an Application Server Cluster*.

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 (for example: -Xss) to at least 512m. Add the entry -Xss512m on the same line with -Xms and -Xmx, and then click Save.
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.

Access Manager is not displayed in the JES Monitoring Console (6445620)

The problem is due to value in the amconfig script that must be changed.

Workaround: Complete the following steps:

1. Unregister the `com.sun.cmm.am 1.0` module.

```
# cacaoadm list-modules
List of modules registered:
com.sun.cacao.agent_logging 1.0
com.sun.cacao.command_stream_adaptor 1.0
com.sun.cacao.efd 2.0
com.sun.cacao.invoker 1.0
com.sun.cacao.mib2simple 1.0
com.sun.cacao.rbac 1.0
com.sun.cacao.rmi 1.0
com.sun.cacao.snmpv3_adaptor 1.0
com.sun.cmm.am 1.0
com.sun.cmm.ws 1.0
com.sun.mfwk 1.0
```

```
# cacaoadm unregister-module com.sun.cmm.am.xml
```

2. Restart the common agent container management daemon.

```
# cacaoadm restart
```

When you list the modules now, com.sun.cmm.am 1.0 is no longer there.

3. In the file /etc/opt/SUNWam/config/com.sun.cmm.am.xml, change the following:

```
<parameter>
   <param-name>ProductName</param-name>
   <param-value>Access Manager</param-value>
   </parameter>
```

to

```
<parameter>
   <param-name>ProductName</param-name>
   <param-value>Java ES Access Manager</param-value>
   </parameter>
```

4. Register the com.sun.cmm.am 1.0 module.

```
# cacaoadm register-module /etc/opt/SUNWam/confing/com.sun.cmm.am.xml
```

5. Restart Access Manager.
6. Restart common agent container management daemon on the console side.

```
# cacaoadm restart
```

Authentication Service Issues

Distributed Authentication UI cannot be deployed as designed

See the section "Deploying the Distributed Authentication UI WAR File " on page 34 in these Release Notes for detailed deployment instructions.

AuthContext API does not work as designed (6432739)

The AuthContext API is designed to deny access to a user from one organization if the DN of a different organization is specified. But if the directory information tree (DIT) is structured as in the following illustration, when you use AuthContext, results are inconsistent.

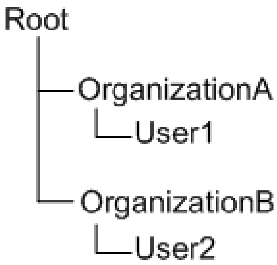

FIGURE 1 Example directory information tree (DIT) for AuthContext API

In this scenario, if you specify OrganizationA , you might be able to authenticate User2 (which is within OrganizationB) . The reverse may also occur. If you specify OrganizationB, you might be able to authenticate User1 (which is within OrganizationA).

Workarounds: Try one or more of the following workarounds.

- Restart the Access Manager web container after using the console to change any Authentication module (such as LDAP) related data.
- After creating a new organization , explicitly set the LDAP search base DN to the suborganization root.
- If multiple users exist with same userID , the parent organization's LDAP search base DN must also contain the people container.

Policy Service Issues

Composite advices are not handled properly (6431977)

Advices handled by Access Manager are configured in `PolicyConfigServer` as the following: `AuthenticateToServiceConditionAdvce` and `AuthenticateToRealmConditionAdvice` However, the conditions generate advices with the keys `AuthenticateToService` (corresponds to `AuthenticateToServiceConditionAdvice`) and `AuthenticateToRealm` (corresponds to `AuthenticateToRealmConditionAdvice`). Due to the mismatched key names, Access Manager and policy agents do not handle the composite advices from these conditions correctly.

Workaround:

follow these steps:

1. Log in to the Access Manager console as `amadmin`.
2. Under Global Properties, click Configuration.
3. Remove the following values from "Advices Handleable by Access Manager:"
   - `AuthenticateToRealmConditionAdvice`
   - `AuthenticateToServiceConditionAdvice`

4. Add the following values to "Advices Handleable by Access Manager:”
   - `AuthenticateToRealm`
   - `AuthenticateToService`
5. Click Save

AMSDK issues

AMSDK Returns Message “LDAP search limit exceeded” (6438366)

This problem occurs because the migration scripts do not properly upgrade the `searchsize` limit value in Directory Server 6.x. .

Workaround:, change the `nsslapd-sizelimit` value from 1000 to 3000.

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

This problem occurs in two known scenarios:

1. You install Access Manager in Legacy mode on Sun Java Application Server, and then use the amadmin utility to change the mode to Realm mode. When you use the default URL `http://<hostname>:8080/amserver`, the error message is displayed.
2. You install Access Manager, with userID changed to root, in Real mode on Sun Java Web Server. When you use the default URL `http://<hostname>:8080/amserver`, the error message is displayed.

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>/amserver/UI/Login?org=dc=prc,dc=example,dc=com
```

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.

Older Known Issues and Limitations

This section describes the following known issues and workarounds, if available, at the time of the Access Manager 7.0 release.

- "Compatibility Issues" on page 22
- "Installation Issues" on page 23
- "Configuration Issues" on page 24
- "Access Manager Console Issues" on page 26
- "SDK and Client Issues" on page 27
- "Authentication Issues" on page 28
- "Session and SSO Issues" on page 28
- "Policy Issues" on page 29
- "Server Startup Issues" on page 30
- "Linux OS Issues" on page 30
- "Federation and SAML Issues" on page 31
- "Globalization (g11n) Issues" on page 31
- "Documentation Issues" on page 32

Compatibility Issues

- "Incompatibilities exist in core authentication module for legacy mode (6305840)" on page 22
- "Delegated Administrator `commadmin` utility does not create a user (6294603)" on page 22
- "Delegated Administrator `commadmin` utility does not create an organization (6292104)" on page 23

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

Access Manager 7.1 2006Q4 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 2006Q4 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 2006Q4 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.

Installation Issues

- "Installing Access Manager on an existing DIT requires rebuilding Directory Server indexes (6268096)" on page 23
- "Authentication service is not initialized when Access Manager and Directory Server are installed on separate machines (6229897)" on page 24
- "Installer doesn't add platform entry for existing directory install (6202902)" on page 24

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.

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 section Adding Additional Instances to the Platform Server List and Realm/DNS Aliases in *Sun Java System Access Manager 7.1 2006Q4 Deployment Planning Guide.* .

Configuration Issues

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 .

Data validation for required attributes in the services (6308653)

Access Manager 7.1 2006Q4 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 2006Q4 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 7.1 2006Q4 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

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

The new Access Manager 7.1 2006Q4 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 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.

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.

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

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)” on page 30
- “Using BEA WebLogic Server as a web container” on page 30

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

Access Manager 7.1 2006Q4 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.

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

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

Multibytes entities within old console will not show up (6425262)

When Access Manager Legacy mode is deployed on Web Server, in the old console, entities like policies, users, groups created with multibytes name can not be found once they are created.

Workaround: Do not create entities with multibyte characters when using the old console user interface.

Policiy 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.

This problem will be fixed in the Access Manager 7.1 final release.

OLH Index does not use alphabetical ordering (6326323)

In the Access Manager administration console online Help, in both Realm and Legacy modes, the alphabetically-sorted index maintains English sorting even under different locales. As a result, index appears not to be sorted under any locale but English. There is no workaround at this time. This problem will be fixed in the final release of Access Manager 7.1.

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 2006Q4 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 2006Q4 Administrator 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).

Deploying the Distributed Authentication UI WAR File

For this Beta release, the Distributed Authentication UI WAR file deployment does not work as designed. As an alternative deployment method, follow these steps:

1. Deploy the Distributed Authentication UI WAR File
2. Complete Additional Instructions for the specific Web Container
   - "To Deploy the Distributed Authentication UI on Web Server" on page 38
   - "To Deploy the Distributed Authentication UI on Application Server 8.2" on page 39
3. Access the Distributed Authentication UI

▼ To Deploy the Distributed Authentication UI WAR File

Before You Begin To implement the Distributed Authentication UI, you must have at least two host computer systems. In the following steps, Host A is host to the full Access Manager server, and Host B is hosts to the Distributed Authentication UI server.

1 **On Host A, install Access Manager on any supported web container.**

Supported web containers include Sun Java Web Server 7.0, Sun Java Application 8.2, BEA WebLogic Server 8.1sp4, IBM WebSphere 5.1.1.6.

Standard Access Manager installation includes the following JES subcomponents: Identity Management and Policy Services Core, Access Manager Administration Console, Common Domain Services for Federation, and Access Manager SDK.

2 **On Host B, install a supported web container.**

Supported web containers include Sun Java Web Server 7.0, Sun Java Application 8.2, BEA WebLogic Server 8.1sp4, IBM WebSphere 5.1.1.6.

You can use the JES installer to install Web Server 7.0 or Application Server, or you can use an existing installation of BEA WebLogic Server 8.1sp4 or IBM WebSphere 5.1.1.6.

3 **Start the web container instance on Host B, the host where the Distributed Authentication UI will be deployed.**

Be sure to start any administration server instances needed for deployment.

4 **On Host B, invoke the JES installer and select Access Manager.**

During installation:

- Choose only the Distributed Authentication UI subcomponent. When you choose this option, the ClientSDK will automatically installed, too.
- When asked about Directory Server, choose the option to use an existing directory server on a remote machine.
- When asked whether you want to configure now or configure later, choose "Configure Later."

5 Go to the Access Manager `/war` directory.

(Solaris) `cd ${AM_INSTALL_DIR}/SUNWam/war`

(Linux) `cd ${AM_INSTALL_DIR}/identity/war`

6 In the file `Makefile.distAuthUI`, in the `sed` command, edit the values for the following parameters:

Parameter	New Value
`JAVA_HOME`	`/usr/jdk/entsys-j`
`SERVER_PROTOCOL`	The protocol used by the web container instance for the Access Manager server on Host A.
`SERVER_HOST`	The fully qualified domain name of Host A.
`SERVER_PORT`	The port used by the web container instance for the Access Manager server on Host A.
`SERVER_DEPLOY_URI`	Change this value only iff the services URI on host A is something other than `amserver`.
`DISTAUTH_PROTOCOL`	The protocol that will be used by the web container instance on which the Distributed Authentication UI WAR file will be deployed.
`DISTAUTH_HOST`	The fully qualified domain name of Host B.
`DISTAUTH_PORT`	The port used by the web container instance on which the Distributed Authentication UI WAR file will be deployed.
`DISTAUTH_DEPLOY_URI`	The deployment URI that will be used by the Distributed Authentication WAR file.
`APPLICATION_USER`	`amadmin` The Application user `com.sun.identity.agents.app.username` can be any user who minimally has READ permissions for all global service configuration data (for example, global services such as Platform service, Client detection service, Localization service, and so forth.)

Parameter	New Value
APPLICATION_PASSWD	amadmin password
NOTIFICATION_URL	Uncomment this parameter and the line to: NOTIFICATION_URL=$(DISTAUTH_PROTOCOL):\/\/$(DISTAUTH_HOSTNAM
NAMING_URL	Uncomment this parameter, and change the line to: NAMING_URL=$(SERVER_PROTOCOL):\/\/$(SERVER_HOSTNAME):$(SERV
DEBUG_LEVEL	If you require more debugging messages, change this value to messages.
DEBUG_DIR	/var/opt/SUNWamdistauth/debug
DISTAUTH_VERSION	7.1

7 In the file Makefile.distAuthUI, in the sed command, make the following changes:

a. Change the line:

```
-e 's/SERVER_HOSTNAME/$(SERVER_HOSTNAME)/' \
```

to

```
-e 's/SERVER_HOST/$(SERVER_HOSTNAME)/' \
```

b. Change the line:

```
-e 's/DISTAUTH_HOSTNAME/$(DISTAUTH_HOSTNAME)/' \
```

to

```
-e 's/DISTAUTH_HOST/$(DISTAUTH_HOSTNAME)/' \
```

c. Change the lines:

```
-e 's/APPLICATION_USERNAME/$(APPLICATION_USERNAME)/' \

—e 's/APPLICATION_PASSWORD/$(APPLICATION_PASSWORD)/' \
```

to

```
-e 's/APPLICATION_USER/$(APPLICATION_USERNAME)/' \

-e 's/APPLICATION_PASSWD/$(APPLICATION_PASSWORD)/' \
```

d. Change the line:

```
-e 's#NOTIFICATION_URL#$(NOTIFICATION_URL)#' \
```

to

```
-e 's/NOTIFICATION_URL/$(NOTIFICATION_URL)/' \
```

e. **After this line :**

```
-e 's/NOTIFICATION_URL/$(NOTIFICATION_URL)/' \
```

add the following line :

```
-e 's/PROFILE_URLSERVER_DEPLOY_URI/$(NAMING_URL)/' \
```

When the changes above have been completed the sed command looks like the following example:

```
sed -e 's/SERVER_PROTOCOL/$(SERVER_PROTOCOL)/' \
          -e 's/SERVER_HOST/$(SERVER_HOSTNAME)/' \
          -e 's/SERVER_PORT/$(SERVER_PORT)/' \
          -e 's/DISTAUTH_PROTOCOL/$(DISTAUTH_PROTOCOL)/' \
          -e 's/DISTAUTH_HOST/$(DISTAUTH_HOSTNAME)/' \
          -e 's/DISTAUTH_PORT/$(DISTAUTH_PORT)/' \
          -e 's/NAMING_URL/$(NAMING_URL)/' \
          -e 's/DISTAUTH_VERSION/$(DISTAUTH_VERSION)/' \
          -e 's/COOKIE_ENCODE/$(COOKIE_ENCODE)/' \
          -e 's/DEBUG_LEVEL/$(DEBUG_LEVEL)/' \
          -e 's#DEBUG_DIR#$(DEBUG_DIR)#' \
          -e 's#DISTAUTH_DEPLOY_URI#$(DISTAUTH_DEPLOY_URI)#' \
          -e 's/APPLICATION_USER/$(APPLICATION_USERNAME)/' \
          -e 's/APPLICATION_PASSWD/$(APPLICATION_PASSWORD)/' \
          -e 's/NOTIFICATION_URL/$(NOTIFICATION_URL)/' \
          -e 's/PROFILE_URLSERVER_DEPLOY_URI/$(NAMING_URL)/' \
          WEB-INF/classes/AMConfig.properties >  temp/AMConfig.properties; \
```

f. **In the properties section, change the following line :**

```
cp ../lib/amclientsdk.jar WEB-INF/lib; \
```

to:

```
cp ../../lib/amclientsdk.jar WEB-INF/lib; \
```

g. **In the properties section, remove the following line:**

```
rm WEB-INF/classes/AMConfig.properties; \
```

8 **Use the** `make`**command or** `gmake` **command to execute** `Makefile.distAuthUI`**.**

(Solaris)`/usr/sfw/bin/gmake -f Makefile.distAuthUI`

(Linux) `/usr/ccs/bin/make -f Makefile.distAuthUI`

For Linux, both `make` and `gmake` are located in `/usr/bin`.

This WAR creates a deployable WAR file:

(Solaris) `${AM_INSTALL_DIR}/SUNWam/war/${DISTAUTH_DEPLOY_URI}.war`

(Linux) `${AM_INSTALL_DIR}/identity/war/${DISTAUTH_DEPLOY_URI}.war`

▼ To Deploy the Distributed Authentication UI on Web Server

1 **Deploy the Distributed Authentication WAR file.**

Use the following default values.

WS_ADMIN_PORT	`8989` This is the secure web server administration port.
WS_CONFIG.	`${DISTAUTH_HOST}`, This is the web server configuration.
WS_VIRTUAL_SERVER	`${DISTAUTH_HOST}`

a. **Go to the bin directory.**

```
cd ${WS_INSTALL_DIR}/bin
```

b. **Run the** `wadam add` **command.**

```
(Solaris) ./wadm add-webapp --user=admin --host=${DISTAUTH_HOST}
--port=${WS_ADMIN_PORT} --config=${WS_CONFIG} --vs=${WS_VIRTUAL_SERVER}
--uri=/${DISTAUTH_DEPLOY_URI}
${AM_INSTALL_DIR}/SUNWam/war/${DISTAUTH_DEPLOY_URI}.war
```

```
(Linux) ./wadm add-webapp --user=admin --host=${DISTAUTH_HOST}
--port=${WS_ADMIN_PORT} --config=${WS_CONFIG} --vs=${WS_VIRTUAL_SERVER}
--uri=/${DISTAUTH_DEPLOY_URI}
${AM_INSTALL_DIR}/identity/war/${DISTAUTH_DEPLOY_URI}.war
```

c. **Enter the Web Server 7.0 administration password when prompted.**

d. **Run the** `wadm deploy` **command.**

```
./wadm deploy-config --user admin --host=${DISTAUTH_HOST}
--port=${WS_ADMIN_PORT} --restart=true ${WS_CONFIG}
```

e. **Enter the Web Server 7.0 administration password when prompted.**

2 **Restart the Web Server instance.**

3 **Log in to the Access Manger console.**

4 **Deploy all pending deployments.**

To Deploy the Distributed Authentication UI on Application Server 8.2

1 **Deploy the distributed authentication war file.**

Use the following default values:

AS_INSTALL_DIR	(Solaris) `/opt/SUNWappserver` (Linux) `/opt/sun/appserver`
AS_ADMIN_PORT	`4849`

a. **Go to the `/bin` directory.**

(Solaris) `cd ${AS_INSTALL_DIR}/appserver/bin`

(Linux) `cd ${AS_INSTALL_DIR}/bin`

b. **Run the `asadmin deploy` command.**

(Solaris) `./asadmin deploy --user admin --host ${DISTAUTH_HOST} --port ${AS_ADMIN_PORT} --contextroot amdistauth --name amdistauth --target server ${AM_INSTALL_DIR}/SUNWam/war/${DISTAUTH_DEPLOY_URI}.war`

(Linux) `./asadmin deploy --user admin --host ${DISTAUTH_HOST} --port ${AS_ADMIN_PORT} --contextroot amdistauth --name amdistauth --target server ${AM_INSTALL_DIR}/identity/war/${DISTAUTH_DEPLOY_URI}.war`

c. **Enter the Application Server 8.2 administration password when prompted.**

2 **Go to the Application Server domain's configuration directory.**

(Solaris) `cd /var/opt/SUNWappserver/domains/domain1/config`

(Linux) `cd /var/opt/sun/appserver/domains/domain1/config`

3 **Make a copy of `server.policy`.**

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

4 **Edit `server.policy`.**

At the end of the file, add the following:

```
// Distributed Authentication User Interface web application RELATED ADDITIONS

grant codeBase "file:${com.sun.aas.instanceRoot}/applications/j2ee-modules/amdistauth/-" {
    permission java.net.SocketPermission "*", "connect,accept,resolve";
    permission java.util.PropertyPermission "*", "read, write";
};
```

```
// END OF ADDITIONS FOR Distributed Authentication User Interface web application
```

5 **Restart the Application Server domain.**

Upon a successful authentication, the user will be redirected to the URL specified by the `goto`parameter.

To Access the Distributed Authentication UI

On all platforms, use the following URL:

```
${DISTAUTH_PROTOCOL}://${DISTAUTH_HOST}:${DISTAUTH_PORT}
    /${DISTAUTH_DEPLOY_URI}/UI/Login?goto=http://www.sun.com
```

Example: http://hostb.sun.com:80/amdistauth/UI/Login?goto=http://www.sun.com

This will display a login page.

Documentation Updates

To access these documents, see the Access Manager 7.1 2006Q4 collection:

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

A new document entitled *Technical Note: Deploying Access Manager Instances to an Application Server Cluster*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 7.0 2006Q4 collection. See

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 2006Q4 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 819-4638-05.

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.