

# Sun Java™ System Access Manager Release Notes for HP-UX

Version 7 2005Q4

Part Number 819-8002-10

---

These Release Notes contain important information available at the time of release of Sun Java System Access Manager 7 2005Q4 (formerly Sun Java™ System Identity Server) for HP-UX. Known issues and limitations, and other information are addressed here. Read this document before you install and use this release.

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

<http://docs.sun.com/prod/entsys.05q4>.

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

These release notes contain the following sections:

- [Release Notes Revision History](#)
- [About Access Manager 7 2005Q4](#)
- [Bugs Fixed in This Release](#)
- [Important Information](#)
- [Known Issues and Limitations](#)
- [Redistributable Files](#)
- [How to Report Problems and Provide Feedback](#)
- [Additional Sun Resources](#)

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

---

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

---

---

## Release Notes Revision History

**Table 1** Revision History

Date	Description of Changes
February 2006	Revenue release.
November 2005	Beta release.

---

---

## About Access Manager 7 2005Q4

Sun Java System Access Manager (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. Logging is based on the J2SE logging APIs (`java.util.logging`).

This section includes:

- [What's New in This Release](#)
- [Hardware and Software Requirements](#)

## What's New in This Release

This release includes the following new features:

- [Access Manager Modes](#)
- [New Access Manager Console](#)
- [Identity Repository](#)
- [Access Manager Information Tree](#)
- [Session Failover Changes](#)
- [Session Property Change Notification](#)
- [Session Quota Constraints](#)
- [Distributed Authentication](#)
- [Multiple Authentication Module Instances Support](#)
- [Authentication "Named Configuration" or "Chaining" Name Space](#)
- [Policy Module Enhancements](#)
- [Site Configuration](#)
- [Bulk Federation](#)
- [Logging Enhancements](#)

### Access Manager Modes

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

- New Access Manager 7 2005Q4 features
- Access Manager 6 2005Q1 features, except for these limitations:
  - When realms are created, the corresponding organizations are not created in Sun Java System Directory Server.

- The new Access Manager 7 2005Q4 Console cannot set a Class of Service (CoS) template priority. See [“New Access Manager Console cannot set the CoS template priorities \(6309262\)”](#) on page 21.
- Identity repositories in Sun Java System Directory Server and other data stores

Legacy mode is required for:

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

## New Access Manager Console

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

- For more information, see [“Compatibility Issues”](#) on page 13.

## Identity Repository

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

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

## Access Manager Information Tree

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

## Access Manager Realms

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

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

## Session Failover Changes

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

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

## Session Property Change Notification

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

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

## Session Quota Constraints

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

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

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

- DENY\_ACCESS. Access Manager rejects the login request for a new session.
- DESTROY\_OLD\_SESSION. Access Manager destroys the next expiring session.

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

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

## Distributed Authentication

The distributed authentication service allows user identity and credential collection interaction for the demilitarized zone (DMZ). During authentication to Access Manager, the user must provide user identification and credentials. During this process, the Access Manager service URLs are exposed to the user. You can avoid this exposure by using a proxy server; however, a proxy server is not an acceptable solution for some deployments.

Most of the secure deployments do not allow Agents (from the DMZ layer) redirecting the request to the Access Manager server (in secure zone, behind the firewall) directly and hence this is the primary requirement for the Distributed Authentication service.

This feature is delivered and deployed as J2EE Web application on any servlet compliant Web container. The Authentication Service can have a remote authentication presentation and extraction framework (that is, distributed authentication UI) that can be deployed as J2EE Web application in the DMZ layer (on a machine not running Access Manager) and which in turn, can communicate with back-end servers for the actual authentication. The Distributed Authentication service communicates to the Authentication server (remotely) for actual authentication via remote API.

## Multiple Authentication Module Instances Support

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

## Authentication “Named Configuration” or “Chaining” Name Space

A separate name space is created under an Org/Realm, which is a chain of authentication module instances. The same chain can be reused and assigned to an Org/Realm, Role, or User. The Authentication Service instance equals the Authentication Chain. Invocation is `server_deploy_uri/UI/Login? service=authentication-chain-name`.

## Policy Module Enhancements

### *Personalization Attributes*

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

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

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

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

### *Session Property Condition*

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

### *Policy Subject*

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

### *Policy Export*

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

### *Policy Status*

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

## Site Configuration

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

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

## Bulk Federation

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

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

## Logging Enhancements

Access Manager 7 2005Q4 includes several new logging enhancements:

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

---

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

---

## Hardware and Software Requirements

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

**Table 2** Hardware and Software Requirements

Component	Requirement
Operating system	HP-UX11i V1
RAM	512 Mbytes
Disk space	250 Mbytes for Access Manager and associated applications

## Supported Browsers

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

**Table 3** Supported Browsers

Browser	Platform
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000
Microsoft Internet Explorer 6.0	Windows 2000 Windows XP
Mozilla 1.7.1	Solaris OS, versions 9 and 10 Java Desktop System Windows 2000 Red Hat Linux 8.0
Netscape™ 4.79	Windows NT Solaris 8 and 9 OS
Netscape™ 7.0	Solaris OS, versions 9 and 10 Java Desktop System Windows 2000 Red Hat Linux 8.0

## Bugs Fixed in This Release

None

## Compatibility Issues

- [Access Manager Legacy Mode](#)
- [Access Manager Policy Agents](#)

### 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](#)
- [“Configure Now” Installation Option in Graphical Mode](#)
- [“Configure Now” Installation Option in Text-Based Mode](#)
- [“Configure Later” Installation Option](#)

### *Java ES Silent Installation Using a State File*

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

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

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

For more information about running the Java ES installer in silent mode using a state file, see the Chapter 5, “Installing in Silent Mode,” in *Sun Java Enterprise System 2005Q4 Installation Guide for UNIX*.

### *“Configure Now” Installation Option in Graphical Mode*

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

### *“Configure Now” Installation Option in Text-Based Mode*

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

### *“Configure Later” Installation Option*

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

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

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

### *Determining the Access Manager Mode*

To determine whether a running Access Manager 7 2005Q4 installation has been configured in Realm or Legacy mode, invoke:

[http\(s\)://host:port/amserver/SMSServlet?method=isRealmEnabled](http(s)://host:port/amserver/SMSServlet?method=isRealmEnabled).

Results are:

- true: Realm mode
- false: Legacy mode

## Access Manager Policy Agents

The following table shows the compatibility of Policy Agents with the Access Manager 7 2005Q4 modes.

**Table 4** Policy Agents Compatibility With Access Manager 7 2005Q4 Modes

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

**Table 4** Policy Agents Compatibility With Access Manager 7 2005Q4 Modes

Agent and Version	Compatible Mode
J2EE agents, version 2.1	Legacy mode only.

---

## Important Information

This section lists the requirements that must be met before installing the Sun Java System Access Manager Enterprise Edition 2005Q4 product. This section contains the following important information:

- [Upgrade Instructions for Access Manager](#)
- [Accessibility Features for People With Disabilities](#)

Web Server or Application Server can be used as web container for deploying Access Manager.

For information about running the configuration scripts, see the *Access Manager 6 2005Q4 Administration Guide*.

## Upgrade Instructions for Access Manager

If you are upgrading to Access Manager 7 2005Q4 from an earlier release, follow the upgrade instructions in the *Sun Java Enterprise System 2005Q4 Upgrade Guide for HP-UX* located at <http://docs.sun.com/app/docs/doc/819-4460>.

## 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>.

---

# Known Issues and Limitations

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

- [“Compatibility Issues” on page 13](#)
- [“Installation Issues” on page 15](#)
- [“Configuration Issues” on page 17](#)
- [“Access Manager Console Issues” on page 20](#)
- [“SDK and Client Issues” on page 23](#)
- [“Command-Line Utilities Issues” on page 24](#)
- [“Authentication Issues” on page 25](#)
- [“Session and SSO Issues” on page 26](#)
- [“Policy Issues” on page 27](#)
- [“Server Startup Issues” on page 28](#)
- [“Federation and SAML Issues” on page 28](#)
- [“Globalization \(g11n\) Issues” on page 30](#)
- [“Documentation Issues” on page 31](#)

## Compatibility Issues

[“Incompatibility between Java ES 2004Q2 servers and IM on Java ES 2005Q4 \(6309082\)” on page 13](#)

[“Incompatibilities exist in core authentication module for legacy mode \(6305840\)” on page 14](#)

[“Agent cannot login because “Profile not in the organization” \(6295074\)” on page 14](#)

[“Delegated Administrator commadmin utility does not create a user \(6294603\)” on page 14](#)

[“Delegated Administrator commadmin utility does not create an organization \(6292104\)” on page 15](#)

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

The following deployment scenario caused this problem:

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

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

*Workaround:*

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

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

Access Manager 7 2005Q4 legacy mode has the following incompatibilities in the core authentication module from Access Manager 6 2005Q1:

- Organization Authentication Modules are removed in legacy mode.
- The presentation of the “Administrator Authentication Configuration” and “Organization Authentication Configuration” has changed. In the Access Manager 7 2005Q4 Console, the drop-down list has `ldapService` selected by default. In the Access Manager 6 2005Q1 Console, the Edit button was provided, and the LDAP module was not selected by default.

*Workaround:*

None.

#### **Agent cannot login because “Profile not in the organization” (6295074)**

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

*Workaround:*

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

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

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

*Workaround:*

This problem occurs if you upgrade Access Manager to version 7 2005Q4 but you do not upgrade Delegated Administrator. For information about upgrading Delegated Administrator, see the *Sun Java Enterprise System 2005Q4 Upgrade Guide for Microsoft Windows*.

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

1. In the `UserCalendarService.xml` file, mark the `mail`, `icssubscribed`, and `icsfirstday` attributes as optional instead of required. This file is located by default in the `/opt/sun/comms/commcli/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/sun/comms/commcli/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

- [“On SDK install with container configuration, notification URL is not correct \(6327845\)” on page 16](#)
- [“Access Manager does not deploy on WebSphere with non-default URIs \(6306605\)” on page 16](#)
- [“Access Manager classpath refers to expired JCE 1.2.1 package \(6297949\)” on page 16](#)
- [“Installing Access Manager on an existing DIT requires rebuilding Directory Server indexes \(6268096\)” on page 17](#)
- [“Log and debug directories permissions incorrect for non-root users \(6257161\)” on page 17](#)
- [“Installer doesn’t add platform entry for existing directory install \(6202902\)” on page 17](#)

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

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

*Workaround:*

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

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

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

### **Access Manager does not deploy on WebSphere with non-default URIs (6306605)**

If you deploy Access Manager with IBM WebSphere and use non-default values (other than amconsole, amserver, ampassword, and amcommon) for the URI parameters (CONSOLE\_DEPLOY\_URI, SERVER\_DEPLOY\_URI, PASSWORD\_DEPLOY\_URI, COMMON\_DEPLOY\_URI), these problems occur:

- If you try to access Access Manager using the non-default URI, the browser returns Error 404.
- If you try to access Access Manager using the default URI (/amserver) the images on the login page are missing and you cannot login as amadmin.

*Workaround:*

In the /opt/sun/identity/bin/amwas51config script, add the following lines before the “.\$AMUTILS” line.

```
uri1="${CONSOLE_DEPLOY_URI:-/amconsole}"  
uri2="${SERVER_DEPLOY_URI:-/amserver}"  
uri3="${PASSWORD_DEPLOY_URI:-/ampassword}"  
uri4="${COMMON_DEPLOY_URI:-/amcommon}"  
if [ $DEPLOY_LEVEL -eq 2 -o $DEPLOY_LEVEL -eq 12 ];  
then CONSOLE_DEPLOY_URI=$uri2 uri1=$uri2  
fi
```

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

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

*Workaround:*

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

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

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

*Workaround:*

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

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

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

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

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

*Workaround:*

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

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

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

*Workaround:*

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

## Configuration Issues

- "Application Server 8.1 `server.policy` file must be edited when using non-default URIs (6309759)" on page 18
- "Platform server list and FQDN alias attribute are not updated (6309259, 6308649)" on page 19
- "Data validation for required attributes in the services (6308653)" on page 19
- "Document workaround for deployment on a secure WebLogic 8.1 instance (6295863)" on page 19

- “The `amconfig` script does not update the realm/DNS aliases and platform server list entries (6284161)” on page 20
- “Default Access Manager mode is realm in the configuration state file template (6280844)” on page 20

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

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

*Workaround:*

Edit the `server.policy` file as follows:

1. Stop the Application Server instance on which Access Manager is deployed.
2. Change to the `/config` directory. For example:

```
cd /var/opt/sun/appserver/domains/domain1/config
```

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

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

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

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

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

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

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

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

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

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

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

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

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

*Workaround:*

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

### **Data validation for required attributes in the services (6308653)**

Access Manager 7 2005Q4 enforces required attributes in service XML files to have default values.

*Workaround:*

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

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

If you deploy Access Manager 7 2005Q4 into a secure (SSL enabled) BEA WebLogic 8.1 SP4 instance, an exception occurs during the deployment of each Access Manager web application.

*Workaround:*

Follow these steps:

1. Apply the WebLogic 8.1 SP4 patch JAR CR210310\_81sp4.jar, which is available from BEA.

2. In the `/opt/sun/identity/am/bin/amw181config` script, (Solaris systems) or `/opt/sun/identity/bin/amw181config` script (Linux systems), update the `doDeploy` function and the `undeploy_it` function to prepend the path of the patch JAR to the `w18_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 `w18_classpath`:

```
w18_classpath= ...
```

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

```
w18_classpath=path-to-CR210310_81sp4.jar:$w18_classpath
```

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

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

*Workaround:*

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

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

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

*Workaround:*

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

```
AM_REALM = disabled
```

## Access Manager Console Issues

- [“For SAML, duplicate Trusted Partner console edit errors \(6326634\)”](#) on page 21
- [“Remote logging is not working for `amConsole.access` and `amPasswordReset.access` \(6311786\)”](#) on page 21
- [“Adding more `amadmin` properties in the console is changing the `amadmin` user password \(6309830\)”](#) on page 21
- [“New Access Manager Console cannot set the CoS template priorities \(6309262\)”](#) on page 21

- “Exception error occurs when adding a group to a user as a policy admin user (6299543)” on page 22
- “In legacy mode, you cannot delete all users from a role (6293758)” on page 22
- “Cannot add, delete, or modify Discovery Service resource offerings (6273148)” on page 22
- “Wrong LDAP bind password should give error for the subject search (6241241)” on page 22
- “Access Manager cannot create an organization under a container in legacy mode (6290720)” on page 22
- “Old console appears when adding Portal Server related services (6293299)” on page 23
- “Console does not return the results set from Directory Server after reaching the resource limit (6239724)” on page 23

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

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

*Workaround:*

None.

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

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

*Workaround:*

None.

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

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

*Workaround:*

None.

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

The new Access Manager 7 2005Q4 Console cannot set or modify a Class of Service (CoS) template priority.

*Workaround:*

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

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

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

*Workaround:*

None.

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

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

*Workaround:*

Try again to delete the user from the role.

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

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

*Workaround:*

None.

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

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

*Workaround:*

None.

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

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

*Workaround:*

None.

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

Portal Server and Access Manager are installed on the same 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 (`/amconsole`) suddenly appears.

*Workaround:*

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

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

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

*Workaround:*

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

## SDK and Client Issues

- [“Can’t remove Session Service configuration for a subrealm \(6318296\)” on page 23](#)
- [“CDC servlet redirecting to the invalid login page when policy condition is specified \(6311985\)” on page 24](#)
- [“Clients do not get notifications after the server restarts \(6309161\)” on page 24](#)
- [“Identity repository ldapv3 plugin and openldap requires patch \(6305268\)” on page 24](#)
- [“SDK clients need to restart after service schema change \(6292616\)” on page 24](#)

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

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

*Workaround:*

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

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

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

*Workaround:*

None.

### **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.

### **Identity repository ldapv3 plugin and openldap requires patch (6305268)**

The openldap does not support a persistence search, and without a persistence search connection, the plugin cannot start.

*Workaround:*

To use the ldapv3 plugin, request an Access Manager patch from your Sun Microsystems technical representative.

### **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.

## **Command-Line Utilities Issues**

- [“New schema files are missing from amserveradmin script \(6255110\)”](#) on page 24
- [“Cannot save XML documents with escape character in Internet Explorer 6.0 \(4995100\)”](#) on page 25

### **New schema files are missing from amserveradmin script (6255110)**

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

*Workaround:*

Manually load the defaultDelegationPolicies.xml and idRepoDefaults.xml files using the amadmin CLI tool with the -toption.

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

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

*Workaround:*

None.

## Authentication Issues

- [“UrlAccessAgent SSO Token is expiring \(6327691\)” on page 25](#)
- [“Unable to login to subrealm with LDAPV3 plugin/dynamic profile after correcting password \(6309097\)” on page 25](#)
- [“Incompatibility for Access Manager default configuration of Statistics Service for legacy \(compatible\) mode \(6286628\)” on page 26](#)
- [“Attribute uniqueness broken in the top-level organization for naming attributes \(6204537\)” on page 26](#)

**UrlAccessAgent SSO Token is expiring (6327691)**

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

*Workaround:*

None.

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

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

*Workaround:*

None.

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

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

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

*Workaround:*

None.

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

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

*Workaround:*

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

## Session and SSO Issues

- [“Access Manager instances across time zones timeout other user sessions \(6323639\)” on page 26](#)
- [“System creates invalid service host name when load balancer has SSL termination \(6245660\)” on page 26](#)

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

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

### **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"/>
```

## 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 28](#)
- [“Using BEAWebLogic Server as a web container” on page 28](#)

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

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

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

*Workaround:* None. You can ignore these messages.

### **Using BEAWebLogic Server as a web container**

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

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

## Federation and SAML Issues

- [“Federation fails when using Artifact profile \(6324056\)” on page 28](#)
- [“Special characters \(&\) in SAML statements should be encoded \(6321128\)” on page 29](#)
- [“Exception occurs when trying to add Disco Service to a role \(6313437\)” on page 29](#)
- [“Auth Context attributes are not configurable until you have configured and saved other attributes \(6301338\)” on page 29](#)
- [“EP Sample does not work if root suffix contains “&” character \(6300163\)” on page 29](#)
- [“Logout error occurs in Federation \(6291744\)” on page 29](#)

### **Federation fails when using Artifact profile (6324056)**

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

*Workaround:*

None.

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

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

*Workaround:*

None.

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

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

*Workaround:*

None.

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

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

*Workaround:*

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

**EP Sample does not work if root suffix contains “&” character (6300163)**

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

*Workaround:*

None.

**Logout error occurs in Federation (6291744)**

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

*Workaround:*

None.

## Globalization (g11n) Issues

- “User locale preferences are not applied to the whole administration console (6326734)” on page 30
- “Online help is not fully available for European languages if Access Manager is deployed on IBM WebSphere (6325024)” on page 30
- “Version information is blank when Access Manager is deployed on IBM WebSphere (6319796)” on page 30
- “Removing UTF-8 is not working in Client Detection (5028779)” on page 31
- “Multi-byte characters are displayed as question marks in log files (5014120)” on page 31

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

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

*Workaround:*

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

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

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

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

*Workaround:*

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

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

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

*Workaround:*

None.

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

The Client Detection function is not working properly. Changes made in the Access Manager 7 2005Q4 Console are not automatically propagated to the browser.

*Workaround:* There are two workarounds:

- Restart the Access Manager web container after you make a change in the Client Detection section.
- or
- Follow these steps in the Access Manager Console:
  - Click Client Detection under the Configuration tab.
  - Click the Edit link for genericHTML.
  - Under the HTML tab, click the genericHTML link.
  - 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.)
  - 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/sun/identity/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

- [“com.iplanet.am.session.client.polling.enable on server side must not be true \(6320475\)” on page 31](#)
- [“Default Success URL is incorrect in the console online help \(6296751\)” on page 32](#)

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

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

*Workaround:*

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

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

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

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

*Workaround:*

The correct default value is `"/amserver/console"`.

---

## Redistributable Files

The Sun Java System Access Manager 6 2005Q4 does not contain any files that you can redistribute.

---

## How to Report Problems and Provide Feedback

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

- Sun Software Support services online at <http://www.sun.com/service/sunone/software>

This site has links to the Knowledge Base, Online Support Center, and Product Tracker, 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.

To share your comments, go to <http://docs.sun.com> and click Send Comments. In the online form, provide the document title and part number. The part number is a seven-digit or nine-digit number that can be found on the title page of the guide or at the top of the document.

---

## Additional Sun Resources

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

- Sun Java System Documentation  
<http://docs.sun.com/prod/entsys.05q4>
- Sun Java System Professional Services  
<http://www.sun.com/service/products/software/javaenterprisesystem/>
- Sun Java System Software Products and Service  
<http://www.sun.com/software/>
- Sun Java System Software Support Services  
<http://www.sun.com/support/>
- Sun Java System Support and Knowledge Base  
<http://sunsolve.sun.com>
- Sun Java System Consulting and Professional Services  
<http://www.sun.com/service/products/software/javaenterprisesystem>
- Sun Java System Developer Information  
<http://developers.sun.com/>
- Sun Developer Support Services  
<http://www.sun.com/developers/support>

Copyright © 2006 Sun Microsystems, Inc. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

SUN PROPRIETARY/CONFIDENTIAL.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

Use is subject to license terms.

This distribution may include materials developed by third parties.

Portions may be derived from Berkeley BSD systems, licensed from U. of CA.

Sun, Sun Microsystems, the Sun logo, Java and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries.

---

Copyright © 2006 Sun Microsystems, Inc. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuels relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

Propriété de SUN/CONFIDENTIEL.

L'utilisation est soumise aux termes du contrat de licence.

Cette distribution peut comprendre des composants développés par des tierces parties.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie.

Sun, Sun Microsystems, le logo Sun, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays.