Sun Java System Access Manager 7.1 Release Notes for Microsoft Windows

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

Part No: 819–5686–10
February 2007

070330@17039

Contents

◆ ◆ ◆ CHAPTER 1

Sun Java System Access Manager 7.1 Release Notes for Microsoft Windows

The Sun Java™ System Access Manager 7.1 Release Notes contain important information about 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.

The Access Manager 7.1 Release Notes contain the following sections:

About Sun Java System Access Manager 7.1

Sun Java System Access Manager is part of the Sun Identity Management infrastructure that enables 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

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, and 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, and 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 into outgoing messages
- Evaluates incoming messages for security tokens
- Enables point-and-click selection of authentication providers for new applications

Single Access Manager WAR file deployment

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

Enhancements to Core Services

Web Containers supported

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

Monitoring Framework Integration

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

- 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, both running and waiting states
  - Connectivity failures for backend servers
- Sessions
  - Size of the session table, which indicates the maximum number of sessions
  - Number of active sessions using an incremental counter
  - Session failover, including the number of "stored" sessions, or the session count using an incremental counter, and the number of operations performed on the failover DB, including read, write, delete, and number of operations
- 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, both running and waiting
- 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 service names in `policyListenerRegistry`
  - Number of `tokenIDs` in `role` cache
  - Number of service names 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
- Federation
  - Number of artifacts in table for a given provider
  - Number of assertions in table for a given provider
  - Number of session entries in a given table for a given provider ID
- SAML
  - Size of artifact map
  - Size of assertion map

Authentication module

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

Policy module

- Support for policy definition based on service-based authentication.
- A new policy condition added: AuthenticateToRealmCondition.
- Support for one-level wild card compare to facilitate the ability to protect the contents of a directory without protecting its sub-directory.
- Support for LDAP filter condition. The policy admin can specify an LDAP filter in the Condition while defining a policy.
- Policies can be created in subrealms without explicit referral policies from the parent realm if an organization alias referral is enabled in the global policy configuration.
- `AuthLevelCondition` can specify the realm name in addition to the authentication level.
- `AuthSchemeCondition` can specify the realm name in addition to the authentication module name.

Service Management module

- Support for storing the 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 provider consists of a client and server provider.
- HTTP layer SSO provider: `HttpServlet` layer authentication provider that encapsulates server-side Access Manager-based SSO.

Installation module

- Repackaging Access Manager as a J2EE Application resulting in a single WAR file to become web deployable

Delegation module

- Support for grouping of delegation privileges

Logging

- Support for delegation in logging module - Delegation controls which identities are authorized to write to or read from the log files.
- Support JCE Based SecureLogHelper - This addition enables the use of 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 1–1 Hardware and Software Requirements

Component	Requirement
Operating system (OS)	■ Windows 2000 Advance Server SP4 ■ Windows XP SP2 ■ Windows 2003 Enterprise Server SP1 (32 bit) ■ Windows 2003 Enterprise Server SP1 (64 bit)
Java 2 Standard Edition (J2SE™ platform)	J2SE platform 6.0, 5.0 Update 7, and 1.4.2 Update 11
Directory Server	Access Manager information tree: Sun Java System Directory Server 5.2 Access Manager identity repository: Sun Java System Directory Server 6.0 or Microsoft Active Directory
Web Containers	Sun Java System Web Server7.0 Sun Java System Application Server Enterprise Edition 8.2
RAM	Basic testing: 512 Mbytes Actual deployment: 1 Gbyte for threads, Access Manager SDK, HTTP server, and other internals
Disk space	512 Mbytes for Access Manager and associated applications

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

Supported Browsers

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

TABLE 1–2 Supported Browsers

Browser	Platform
Firefox 1.0.7	Windows XP
	Windows 2000
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows 2000
Mozilla 1.7.12	Windows XP
	Windows 2000
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000

General Compatibility Information

Access Manager Legacy Mode

If you are installing Access Manager with Sun Java System Portal Server, you must select the Access Manager Legacy (6.x) mode.To determine the more for an Access Manager 7.1 installation, see "Determining the Access Manager Mode" on page 12.

Configure Automatically During Installation Option

If you are running the Java ES Installer in graphical mode with the Configure automatically during installation option, the Access Manager is configured in "Legacy (version 6.x style)" mode.

Configure Manually After Installation Option

If you ran the Java ES Installer with the Configure Manually After Installation option, you must run the `install-dir\identity\setup\amconfig.bat` file to configure Access Manager after installation. To select Legacy (6.x) mode, set the following parameter in your configuration file

```
AM_REALM = disabled

...
install-dir\identity\setup\AMConfigurator.properties
...
```

Determining the Access Manager Mode

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

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

A return value of `true` indicates Realm mode. A return value of `false` indicates Legacy mode.

Access Manager Policy Agents

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

TABLE 1–3 Policy Agents Compatibility With Access Manager 7.1 Modes

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

Other Known Issues and Limitations

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

Installation Issues

- "Authentication Service Is Not Initialized When Access Manager and Directory Server Are Installed on Separate Machines (6229897)" on page 13

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.

Upgrade Issues

- "Portal Server and Web Console Do Not Work After Upgrading Java ES 4 Access Manager to Java ES 5 Access Manager (6515054)" on page 13

Portal Server and Web Console Do Not Work After Upgrading Java ES 4 Access Manager to Java ES 5 Access Manager (6515054)

After upgrading Java ES 5 Access Manager to Java ES 5 Access Manager, the deployed applications, Portal Server, and web console do not work.

Workaround: Copy the `config.properties` file from the Java ES 5 installation location to Java ES 4 installation location:

`copy` *install-Dir*`\share\MobileAccess\config\config.properties`
JavaES4–install-dir`\PortalServer\`*https-host-name*`\portal\web-apps\WEB-INF\classes\`

Configuration Issues

Active Perl 5.8 or Later Is Required to Configure Some Access Manager Modules

Active Perl 5.8 or later needs to be installed to configure the following components with Access Manager:

- MFWK
- Session Failover
- Bulk Federation
- Performance Tuning

You can download Active Perl from`http://www.activestate.com/Products/ActivePerl/`.

Installer Unable to Configure Distributed Authentication and Client SDK Components

In Configure Automatically During Installation, the distributed authentication and client SDK components are not configured. No error message is displayed.

Workaround: Use the Configure Manually After Installation option during installation and manually configure the distributed authentication and client SDK components after installation.

`am2bak.bat` and `bak2am.bat` Files Not Generated Correctly (6491091)

Access manager 7.1 does not support the backup (`am2bak.bat`) and restore (`bak2am.bat`) utilities.

Workaround: None.

User Account Is Not Deactivated After Many Successive Unsuccessful Logins (6469200)

User account is not deactivated after multiple unsuccessful logins to the Access Manager.

Workaround: Use the realm administration console (`\amserver\console`) to enable or disable the lockout utility. To set the Login Failure Lockout Mode attribute, follow these steps:

1. Open the Access Manager GUI.
2. Select a ream to enable lockout.
3. Select the Authentication tab.
4. Click the Advanced Properties button.
5. Select the Login Failure Lockout Mode attribute.
6. Save the properties by clicking the Save button.

Access Manager Console Issues

New Access Manager Console Cannot Set the CoS Template Priorities (6309262)

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

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

Old Console Appears When Adding Portal Server Related Services (6293299)

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

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

Console Does Not Return the Results Set From Directory Server After Reaching the Resource Limit (6239724)

In the following situation , the Console does not display accurate information: 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

Unable to Create The Same Deleted User Through the Portal (6479611)

You cannot create the same deleted user profile through the portal. The following error message is displayed:

```
An error occurred while storing the user profile.
```

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.

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.

Session and SSO Issues

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 such as 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 the editing of policies in this scenario:

1. Create two dynamic attributes in the Policy Configuration Service.
2. Create a policy and select the newly created dynamic attributes 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.

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

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

Server Startup Issues

Debug Error Occurs on Access Manager Startup (6309274, 6308646)

Access Manager 7.1 startup returns the following debug errors in the `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.

Federation and SAML Issues

- "Federation Fails When Using Artifact Profile (6324056)" on page 17
- "Logout Error Occurs in Federation (6291744)" on page 18

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, the following error message is displayed: Error: No sub organization found.

Workaround: None.

Globalization (g11n) Issues

Application Error Displayed in Left Panel of Online Help in Realm Console (6508103)

When Access Manager is deployed to the Application Server, the left panel in the online help in the realm console displays an application error.

Workaround: Follow these steps:

1. Copy the `jhall.jar` file.

   `copy` *install-dir*`\share\lib\jhall.jar %JAVA_HOME%\jre\lib\ext`

2. Restart the Application Server.

Removing UTF-8 Does Not Work in Client Detection (5028779)

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

Workaround: Try the following workarounds:

1. Restart the Access Manager web container after you make a change in the Client Detection section.
2. Perform the following steps in the Access Manager Console:
   a. Click `Client Detection` under the `Configuration` tab.
   b. Click the `Edit` link for `genericHTML`.
   c. Under the HTML tab, click the `genericHTML` link.
   d. Type 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.)

e. Click Save.

f. Logout and then log in again.

Multi-byte Characters Are Displayed as Question Marks in Log Files (5014120)

Multi-byte messages in log files in the `install_dir\identity\logs` directory are displayed as question marks (`?`). Log files are in native encoding and are 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: When starting any web container instances, always use 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. In , in for

1. Go to the Access Manager 7.1 Administrator Console.
2. Select LDAPv3 configuration.
3. In the "LDAPv3 Plugin Supported Types and Operations" field, type the following values depending on the roles and filtered roles you plan to use in your LDAPv3 configuration:

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

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, perform the following steps:

1. (Optional) If you are using a JDK version earlier than JDK version 1.5:,
   a. download the Bouncy Castle JCE provider from the Bouncy Castle site (`http://www.bouncycastle.org/`).

      For example, for JDK version 1.4, download the `bcprov-jdk14-131.jar` file.

   b. Copy the file to the *jdk_root*`\jre\lib\ext` directory.
2. Download the JCE Unlimited Strength Jurisdiction Policy Files. for your version of the JDK.
   - For Sun Systems, download the 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.
3. Copy the downloaded `US_export_policy.jar` and `local_policy.jar` files to the *jdk_root*`\jre\lib\security` directory.
4. 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
   ```

5. Set the following property in the `AMConfig.properties` file to true:

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

6. Restart the Access Manager web container.

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

Documentation Updates

These documents are available in the Access Manager 7.1 collection at `http://docs.sun.com/coll/1292.1`

The Sun Java System Access Manager Policy Agent 2.2 collection has also been revised to document new agents and is available at`http://docs.sun.com/coll/1322.1`

Redistributable Files

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

How to Report Problems and Provide Feedback

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

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

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

To obtain the most useful help 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 affect 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 819-5686.

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.
