Sun Java™ System Identity Server Release Notes

Version 2004Q2

Part Number 817-5712-10

These Release Notes contain important information available at the time of release of Sun Java System Identity Server 2004Q2. New features and enhancements, known issues and limitations, and other information are addressed here. Read this document before you begin using Identity Server 2004Q2.

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/db/prod/entsys.04q2

Check the web site prior to 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 Identity Server 2004Q2
- What's New in This Release
- Bugs Fixed in This Release
- Installation Notes
- 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
June 23, 2004	Second release of these release notes for Linux support. Also added descriptions to the Known Problems list.
May 18, 2004	Initial release of these release notes.

About Identity Server 2004Q2

Sun Java™ System Identity Server is an identity management solution designed to meet the needs of rapidly expanding enterprises. Identity Server enables you to get identities for your employees, your partners and suppliers into one online directory. Then it provides a means for establishing policies and permissions regarding who has access to which information in your enterprise. Identity Server is the key to all your data, your services, and who has access to what—it's the key to all your internal and external business relationships.

What's New in This Release

New features in Identity Server 2004Q2 include the following (for more a more detailed explanation of these features, see the *Sun Java System Identity Server Technical Overview*):

- Enhancements to Federation Management
  - Identity Federation Framework 1.2
  - Liberty Identity Web Services Framework 1.0
  - Identity Service Instance Specification 1.0
- Support for SAML 1.1
- Customized JAAS Authorization Framework
- Enhancements to Authentication
  - Windows Desktop SSO Authentication Service
  - JAAS Shared State
  - Java Database Connectivity Authentication Module Sample
  - Java Card Digital Identity Authentication Module Sample
- Enhancements to the Identity Server console
  - Nested Groups Support
  - Centralized Agents Management
  - Display Options and Available Actions
- Session Failover for Application Server
- Configuration and Tuning Scripts

Hardware and Software Requirements

The following hardware and software are required for this release of Identity Server.

Table 2 Hardware and Software Requirements

Component	Solaris Requirement
Operating system	Solaris™ Operating System (OS), SPARC® Platform Edition, versions 8 and 9 Solaris™ 9 OS, x86 Platform Edition Red Hat™ Linux, Advanced Server 2.1 Update 2
RAM	512 Mbytes
Disk space	250 Mbytes for Identity Server and associated applications

Bugs Fixed in This Release

The table below describes the bugs fixed in Identity Server 2004Q2:

Table 3 Fixed Bugs in Identity Server 2004Q2

Bug Number	Description
4919897	Authentication fails on anonymous bind.
4794971	Startup scripts not properly deleted.
4922287	Apostrophes in suborganization names cause errors.
4925958, 4948665	Problem with zh_CN.GB18030 locale.
4921424	Incorrect default globalization settings for Korean character set.
4918930	Unregistered Service Incorrectly Listed As Registered.

Installation Notes

This release of Identity Server separates installation of Identity Server packages from the configuration steps you must take. In this release, you must use the Java Enterprise System installer to install the first instance of Identity Server.

Configuration Scripts

After installing the first Identity Server instance, you can create additional instances on Sun Java System Application Server as well as Sun Java System Web Server using the configuration scripts.

The IS installation/configuration scripts do this:

- Deploy additional Identity Server instances for a web container on a single host.
- Reconfigure Identity Server instances. For example: Change an Identity Server instance's owner and group (for example, from root to another user or group).
- Make the Identity Server SDK available to web applications.
- Uninstall additional instances (you are supposed to use the JES uninstaller to uninstall the first instance).

For detailed instructions, see the *Identity Server Administration Guid*e. Note that the amserver command is no longer supported.

Known Issues and Limitations

This section contains a list of the more important known issues at the time of the Identity Server 2004Q2 release. This section covers the following topics:

- Installation
- Authentication
- Command Line Tools
- Configuration
- Identity Server Console
- Federation
- Logging Service
- Policy
- Session Service
- Single Sign-On
- SDK

- Internationalization (i18n)
- Cookies
- Cookie Hijacking

Installation

Commas in Root Suffix May Cause Installation to Fail (#4750396)

During installation, when asked to specify an Identity Server root suffix, do not use commas in the root distinguished name (RDN).

Authentication

Persistent Cookie Mode Property is Inconsistent (#5038544)

In Persistent Cookie mode, the UserId property set in the token is inconsistent. Because of this, the policy agent, which depends on the UserID property, may fail.

Workaround

Use UserToken for a non DN value and Principal for the DN value.

Administrator Unable to Add Roles From Parent Organizations (#5042217)

If you configure an authentication service for suborganizations with a user dynamic profile creation role and then login to the service with dynamic profile creation enabled, when you view the user properties, no role gets assigned because the authentication service only allows the roles that belong to the sub organization.

Cannot Login to Identity Server After Adding Proxy Properties (#4966788)

If you add proxy properties to server.xml and then restart Identity Server, you will not be able to login to the Identity Server Console. This only occurs when the Proxy Server cannot recognize Identity Server.

Workaround

In server.xml, set http.nonProxyHosts to the hostname with a fully qualified host name and then restart the server. For example:

```
<JVMOPTIONS>-Dhttp.nonProxyHosts=Identity_Server_FQDN</JVMOPTIONS>
```

For performance purposes, the properties defined in this workaround should be set even if the Proxy Server recognizes Identity Server.

Reloading the Session Timeout Page Will Authenticate User with Valid Username and Password (#4697120)

At the login page, if a user waits for the page to timeout and then enters a valid username and password, the user will see the session timeout page. The user will be authenticated to Identity Server if the user reloads the page without re-entering username and password.

Different Directories Must Be Specified For Multiple SafeWord Servers (#4756295)

A configuration with multiple organizations using their own respective SafeWord servers have to specify their own .../serverVerification directories in their SafeWord Authentication service templates. If you leave the default value, and all servers use the same directory, then the first organization to authenticate with its SafeWord server will be the only one that works.

Command Line Tools

JVM May Abort When Running amadmin in SSL Mode (#5009031)

While running the server in secured mode, continuous usage of amadmin might abort the JVM.

If you experience this behavior, please contact Sun Java System Software Support Services.

am2bak and bak2am Scripts Not Working for Linux (#5053866)

The am2bak and bak2am restore scripts do work for Identity Server running on Linux.

Workaround

1. Correct the path of the following commands:

   ```
   ECHO=/usr/bin/echo
   ```

   should be ECHO=/bin/echo

   ```
   uid=`/usr/xpg4/bin/id -un`
   ```

   should be uid=`/usr/bin/id -un`

   ```
   /usr/bin/tar
   ```

   should be /bin/tar

   ```
   usr/bin/rm
   ```

   should be /bin/rm

   ```
   /usr/bin/grep
   ```

   should be /bin/grep

   ```
   /usr/bin/ps
   ```

   should be /bin/ps

   ```
   /usr/bin/ls
   ```

   should be/bin/lsv

2. Modify the check_for_invalid_chars() function. For example:

   ```
   check_for_invalid_chars() {
           echo "$1" | grep '[^/_.a-zA-Z0-9a-]' > /dev/null
           if [ $? = 0 ]; then
   ```

```
                return 1
            else
                return 0
            fi
        }
```

On Linux Systems, amserver stop Does Not Stop the amunixd Process (#5050332)

On Linux systems, the `/etc/init.d/amserver stop` command does not stop the `amunixd` authentication helper process.

Workaround
First, use the `ps` command with the `f` option to determine the `amunixd` process ID:

```
ps -efl | grep /opt/sun/identity/share/bin/amunixd
```

Then, use the `kill` command with this process ID to stop the `amunixd` process.

Failed Message Appears When Running am2bak (#5043752)

When performing the back-up process using am2bak, you may receive an error message stating that the backup process failed, when in reality it did not.

amadmin Returns Incorrect Error Message (#5008960)

The import option of amadmin incorrectly throws the same error message for all related errors.

amverifyarchive on Console-Only installs Has Unswapped Tags (#4993375)

If you perform an Identity Server console-only installation, the amverifyarchive utility will not have the following tags swapped out in this script:

- JSSHOME
- JDK_HOME
- BASEDIR
- PRODUCT_DIR

Configuration

amconfig Script Fails to Configure Localized Identity Server for Configure Later Option (#5062437)

If you install a localized version of Identity Server 2004Q2 using the Java Enterprise System installer and you select the "Configure Later" option, the `amconfig` script subsequently fails to configure Identity Server.

Workaround
Before you run the `amconfig` script, edit the web container script, depending on the web container you are using to run Identity Server:

1. Locate the web container script:
   - Web Server: `amws61config`
   - Application Server: `amas70config`

   Both scripts are located in the *IdentityServer_base*`/SUNWam/bin` directory on Solaris systems or the *IdentityServer_base*`/identity/bin` directory on Linux systems.

2. In the web container script, add the `/WEB-INF` directory to the $DEPLOY_SRC variable in the following `if` statement:

```
if [ ! -d $DEPLOY_SRC/WEB-INF ]; then
  mkdir -p $DEPLOY_SRC
  cd $DEPLOY_SRC
  jar xf $PKGDIR/$warfile
```

3. Run the `amconfig` script to configure Identity Server. For information about the `amconfig` script, see the *Identity Server 2004Q2 Administration Guide*:

   `http://docs.sun.com/doc/817-5709`

Do Not Use amconfig With Silent File Option (#5003430, 5003386, 5000964)

Do not use the interactive mode of amconfig. Example: amconfig -s. Results are unpredictable.

Workaround
Invoke amconfig in silent mode. Example: amconfig -s *path-to-silent-file*

Indices Are Always Created For userRoot Irrespective of the Backend Name (#5002886)

The index.ldif hardcodes the userRoot for creating index for the attributes. It is possible to install Identity Server on a rootsuffix residing on any arbitrary backend database name. The backend name can be obtained by ldapsearch with base cn=config using nsslapd-suffix=SUFFIX_NAME as the filter.

Federation

Exception Thrown for PP Modify if Attribute Value is Empty (#5047103)

Identity Server throws an exception when you perform a PP Modify with an empty attribute value. For example, if you create the setup to test the sis-ep sample and then send the EP Modify page and click on the button without entering any value for the attribute, the exception is incorrectly thrown.

Policy Effect Requires Server Restart (#5045036)

Federation policy implementation does not take effect until you restart the server. This is valid for both Application Server and Web Server. You must restart the server only after a fresh install and when the policy is first implemented.

Identity Server Console

Creating Roles With Defined Access Permissions as Org Admin Generates Error (#5037978)

If you are logged in as an Organization Administrator and create a role and assign Access Permissions (such as creating an Org Admin or Help Desk Admin role) to it, you will receive an error.

Organization Administrators' permissions are set to prevent them from modifying any values in the organization. When the role is created with permissions, an ACI in the organization entry is attempting to be modified.

Workaround

1. After installation, go to the directory where the XML files are located. By default, they are:

   /etc/opt/SUNWam/config/xml (Solaris)

   /etc/opt/sun/identity/config/xml (Linux)

2. Backup the amAdminConsole.xml file. For example:

   ```
   cp amAdminConsole.xml amAdminConsole.bak
   ```

3. Edit amAdminConsole.xml.

a. Search for all the lines which start with “S1IS Organization Admin Role access allow read” and delete that ACI. For example, delete all occurrences of this ACI used for the organization administrator role:

```
aci: (target="ldap:///ORGANIZATION")(targetfilter=(!(|(nsroledn=cn=Top-level Admin
Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com))))(targetattr !=
"nsroledn")(version 3.0; acl "S1IS Organization Admin Role access allow read"; allow (read,search) roledn =
"ldap:///ROLENAME";)
```

b. Search for all the lines which start with “S1IS Organization Admin Role access allow all” and edit that ACI to remove the '*,' at the beginning of this ACI:

```
aci: (target="ldap:///*,
```

Edit all occurrences of this ACI for the organization administrator role. For example:

Modify this ACI:

```
aci: (target="ldap:///*,ORGANIZATION")(targetfilter=(!(|( nsroledn=cn=Top-level Admin
Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help D esk Admin Role,dc=iplanet,dc=com))))(targetattr !=
"nsroledn")(version 3.0; acl "S1IS Organization Admin Role access allow all"; allow (all) roledn =
"ldap:///ROLENAME”;)
```

to:

```
aci: (target="ldap:///ORGANIZATION")(targetfilter=(!(|( nsroledn=cn=Top-level Admin
Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com))))(targetattr
!="nsroledn")(version 3.0; acl "S1IS Organization Admin Role access allow all"; allow (all) roledn =
"ldap:///ROLENAME";)
```

c. Save this file.

4. Delete the iPlanetAMAdminConsoleService using the amadmin command line tool:

```
/opt/SUNWam/bin/amadmin -u "uid=amAdmin,ou=People,dc=iplanet,dc=com" -w "iplanet1" -r
"iPlanetAMAdminConsoleService"
```

5. If the file is successfully deleted, the following message will be displayed:

```
Deleting Service Schema iPlanetAMAdminConsoleService

Success 0: Successfully completed.
```

6. Import the same service again with the newly modified amAdminConsole.xml using the amadmin command line tool:

```
/opt/SUNWam/bin/amadmin -u "uid=amAdmin,ou=People,dc=iplanet,dc=com" -w "iplanet1" -s
/etc/opt/SUNWam/config/xml/amAdminConsole.xml
```

7. If the file is successfully loaded, the following message will be displayed:

   Loading Service Schema XML /etc/opt/SUNWam/config/xml/amAdminConsole.xml

   Success 0: Successfully completed.

8. Restart the Identity Server.

Console Samples Do Not Compile (#5026635)

Some of the Identity Server Console samples do not compile, because files have changed locations in this release.

Workaround

Change the existing jato.jar path to the following in the rules.mk file:

$*USER_DIR*/share/lib/identity/console-war/WEB-INF/lib/jato.jar

Users Cannot Be Created With the SAML Service(#5038600)

Only the top-level administrator can create users while assigning the SAML service at the same time

Workaround

Organization administrators need to create the user without the SAML service. Once the user is created, they can add the service through the User Profile page.

Values Not Retained When Clicking Back Button (#4992972)

Whenever there is a multiple page process, such as creating a group, role, or adding a condition to a policy, and then the Back button is selected, the values in the previous page will not be restored.

Policy Admin Cannot Not Modify Own Profile (#5042100)

A policy administrator cannot modify his or her own profile through the Identity Server console.

Workaround

Set the Display Options for the Navigation View to Users and the Available Actions for users to Full Access.

Error in Console While Searching for Users When User Management is Disabled (#5049218)

If User Management is disabled and you perform a search for users, you may receive a Server Error.

Workaround

Replace the PMAdminRoldSelect.jsp with the new JSP. This can be found in the following location:

IdentityServer_base/applications/console/policy

Entity Descriptors Search Filter Does Not Work Properly (#4959895)

In the Federation Module, in the Entity Descriptors view, if you use the Search field to find an entity descriptor, the search results are not always accurate.

“**” Search Mask Does Not Work (#4961370)

If you use “**” without additional characters as the search filter mask in the Identity Server console, the search will fail. The search field accepts “**” with additional characters, for example **a or a**.

Refresh Problem For Hosted Provider in Federation Management Module (#4915894)

In the Federation Management module, if you modify and save any attributes in the Identity Provider view of a hosted provider, the changes will be saved, but will not be automatically refreshed in the display.

Workaround

Exit the Federation Management module by selecting a different module (for example, Service Configuration) and then return to the Federation Management module. This will refresh the display.

Console Does Not Refresh User Attribute Changes (#4931455)

The Identity Server console Navigation frame does not refresh to indicate changes in User attribute values in made in the Data frame. Refresh the page manually to view the changed values.

Port Problems With Internet Explorer (#4864133)

Due to an incompatibility with Internet Explorer, you should not use 80 as the Identity Server port number when running http, or 443 when running https.

Logging Service

Logging Problem When Java Security Is Enabled (#4926520)

jdk_logging.jar may not work when Java Security is enabled.

Workaround

When Java Security is enabled and if you have a JDK version previous to 1.4, include the following permission in the java security file:

```
permission java.lang.RuntimePermission  shutdownHooks
```

Policy

Modifications in Referral Policy Rule Not Reflected in Suborg (#5016725)

After deleting a referral policy for the root organization, rules for normal policies in the sub organization are not deleted (and cannot be deleted).

Matching Entries are not Returned When nslookthrough Limit Reached (#5013538)

Matching entries are not returned to the Identity Server console even after reaching the admin limits defined in nslookthrough.

Workaround

Tune the nslookthroughlimit parameter to compensate for the number of entries.

Policy Not Enforced for Aliased Tokens (#4985823)

If you use user alias a to log in to Identity Server against an authorization module other than LDAP or Membership, and then attempt to access a protected resource, access is denied.

Problem With Policy Sample (#4923898)

The Readme.html located in the Policy Sample excludes information that causes the sample not to run. In order to run the sample, the LD_LIBRARY_PATH needs to include the path to the NSPR, NSS, and JSS shared libraries.

Set the environment variable LD_LIBRARY_PATH to /usr/lib/mps/secv1 (for Solaris) or /opt/sun/pirvate/lib (Linux). If this is not set correctly, you will encounter an error.

Session Service

Idle Sessions Are Not Cleaned Up (#4959071)

Idle sessions are currently not being cleaned up correctly. Please contact Support for a patch to rectify this problem. See How to Report Problems and Provide Feedback for more information.

SDK

Document Use of certutil For Identity Server SDK Installations That Use SSL Servers (#5027614)

Users are experiencing security-related errors and exceptions when trying to communicate from SDK-only machines with SSL-enabled Identity Server 2004Q2 servers. In this scenario, the Identity Server SDK is deployed either on no web container or on a third-party web container such as BEA WebLogic Server or IBM WebSphere Application Server.

Workaround
Create a certificate database on the SDK-only machine and install the root CA certificate for the Identity Server server into this database:

1. Log into the SDK-only machine as superuser (`root`).
2. Verify that the required Netscape Security Services (NSS) package is installed:
   - On Solaris systems: SUNWtlsu
   - On Linux systems: sun-nss RPM
3. If the package is not installed, install it. For example:

   On Solaris systems:

   ```
   cd JavaEnterpriseSystem_base/Solaris_arch/Product/shared_components/Packages
   pkgadd -d . SUNWtlsu
   ```

   On Linux systems:

   ```
   cd JavaEnterpriseSystem_base/Linux_x86/Product/shared_components/Packages
   rpm -Uvh sun-nss-3.3.10-1.i386.rpm
   ```

4. Create the password file for the token password for that certificate database. For example:

   On Solaris systems:

   ```
   echo "cert-database-password" > /etc/opt/SUNWam/config/.wtpass
   chmod 700 /etc/opt/SUNWam/config/.wtpass
   ```

   On Linux systems:

   ```
   echo "cert-database-password" > /etc/opt/sun/identity/config/.wtpass
   chmod 700 /etc/opt/sun/identity/config/.wtpass
   ```

   where *cert-database-password* is the token password.

5. Check the LD_LIBRARY_PATH variable:

   On Solaris systems, check LD_LIBRARY_PATH to see if the `/usr/lib`, `/usr/lib/mps/secv1`, and `/usr/lib/mps` directories are present. If not add any missing directories.

   On Linux systems, check LD_LIBRARY_PATH to see if the `/opt/sun/private/lib` directory is present. If not add the directory.

6. Use the Certificate Database Tool (`certutil`) to create the certificate and key databases. For information about `certutil`, refer to the following Web site:

   `http://mozilla.org/projects/security/pki/nss/tools/certutil.html`

   For example:

   certutil-home/certutil -N -d *cert-database-dir* -f *config-home*/.wtpass

   where:

   certutil-home is the location of `certutil`:

   - On Solaris systems: `/usr/sfw/bin`
   - On Linux systems: `/opt/sun/private/bin`

   cert-database-dir is the database directory for the certificate and key databases.

   config-home is the location of the Identity Server configuration files:

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

7. In the newly created certificate database, add the root CA certificate for the SSL certificate that is installed on the Identity Server server. For example:

   certutil-home/certutil -A -n "*certificate-nickname*" -t "TCu,TCu,TCuw" -d *cert-database-dir* -a
   -i *path-to-file-containing-cert* -f *config-home*/.wtpass

8. Use an editor to view the `AMConfig.properties` file and verify that the following values

   - Certificate database directory: `com.iplanet.am.admin.cli.certdb.dir`
   - Prefix: `com.iplanet.am.admin.cli.certdb.prefix`)
   - Password file: `com.iplanet.am.admin.cli.certdb.passfile` I

     If not, edit the settings as needed. For example, the prefix setting should be empty (that is, equal to “”).

9. If changes were made to the `AMConfig.properties` and the Identity Server SDK is deployed into a web container, restart the web container.

SSL Handshake Fails With DNSAlias with JCE Provider (#5038876)

SSL handshaking fails when certificates with valid DNSAlias names in the subjectaltname are used with a JCE provider.

BasicEntitySearch Filter Hardcoded to uid (#5041529)

If you install Identity Server with the user naming attribute set to cn and then log in to the Identity Server Console and create an agent entity, the agent entity will not be displayed in the Navigation pane. This is because the entity search template is hardcoded to uid.

Workaround

Change the filter from uid to cn from the Directory Server Administration console and restart the server.

Identity Methods in Init() of Filters Cause Weblogic to Crash (#5016283)

A Weblogic server will not start when the init() methods of filters have Identity Server-related code. The Identity Server API is called in the init method of the ServletFilter servlet.

Identity Server uses JSS as the security provider, but Weblogic uses JCE by default. When the init method is invoked, Weblogic attempts to validate its license using the JCE, but JSS is getting initialized.

Workaround

Change the default security encryption from JSSEncryption to JCEEncryption in the AMConfig.properties file.

Any Password That Starts with “{SSHA}” Symbols is Unusable (#4966191)

Identity Server does not support the use of hashed {SSHA} symbols in passwords.

smtp Server Port Property Incorrect in AMConfig.properties (#5048378)

The smtp server port property in the AMConfig.properties is not correct. Sent mail incorrectly looks for com.iplanet.am.smtpport.

Naming Attributes Should Be Lower Case (#4931163)

Due to a limitation in the SDK, naming attributes must be lower case. For example, if you install an Identity Server instance over Directory Server and load the Identity Server schema with the user naming attribute defined as CN, user creation will fail.

Workaround

Change the naming attribute in the Directory Server console. For example, change the basicuser user naming attribute of the creation template from CN to cn.

Group Create Option Adds Only One memberURL Attribute (#4931958)

If you create a group with the multiple LDAP-filter option (-f), the group is incorrectly created with only one memberURL attribute.

Service Registration Problem (#4853809)

If you create service templates and register them in a parent organization, then try to register them for a suborganization, some of the services registered at the parent organization will not be registered, although amConsole.access shows that the service is registered.

Workaround

Refresh the Identity Server console and re-register the services.

Services Disappear With Service Type Role User Login (#4931907)

If a user in a Service-type role logs into Identity Server with the Admin start view set to the orgDN, and then tries to unregister a service, all the listed services disappear from the display.

Workaround

Restart the server and the services will reappear.

Single Sign-On

Unable To Perform SSO With Different Deploy URIs (#4770271)

If the deployment URIs are different between two different instances of Identity Server, Single Sign-on will not function properly.

Internationalization (i18n)

Registering All Services May Not Register All Available Services (#4853809)

If you register all services through the Identity Server Console, some of the services may not be listed in Available Services.

Workaround

Do not click the Add button more than once.

Services With Policy Schema Shows as “Addable” to a User (#4996479)

When adding services to a user, the wsrp consumer service shows as available. However, if it is chosen, it will not be added and fails. Furthermore, if multiple services are checked along with the consumer service, then all of the adds fail.

Workaround

Do not add WSRP service from the Identity Management module.

Authlevel Login Fails for Japanese Browsers (#5013994)

The first time you log into Identity Server by Authentication Level, it does not work for the following Japanese browsers when the browser language is set to ja:

- IE6.0ja
- IE7.0ja
- Mozilla1.2.1

Workaround

When the “Authentication Module has Denied” error appears, do not click the “Go Back To Login Page” link. Instead, enter the following URL:

http://*server*:*port*/amserver/UI/Login?*authlevel*=*number*

Japanese Online Help Incorrectly displayed (#5024138)

If you are running the Japanese version of Identity Server and change the language to en_US, the Japanese help context will still display.

Workaround

Create a sym link from docs_en to docs_en_US.

User ID Generation Mode Generates User ID From First/ Last Name (#5028750)

Identity Server does not support multibyte user ID. By default, User ID Generation Mode generates user id from first name and last name.

Client Detection function not working properly (#5028779)

In the Client Detection service, removing UTF-8 is not working properly.

Workaround

If you remove the UTF-8 character set, restart the web container after you have made the change.

G11NSetting Does Not Handle a Space in Q Factor (#5008860)

When the client data has a space in or around q factor, the G11NSettings code fails to parse it correctly and returns the following error:

```
ERROR: G11NSettings::Fetchcharset() Unable toparse  charset entry invalid Q  q
```

Login Page Fails With Multi-byte Role Parameter On URL for ja Character Set (#4905708)

If you create a multi-byte role and then try a URL login with a user registered to the multi-byte role, the login page will produce a failure error.

Workaround
In order for the authentication framework to decode a multi-byte role value specified in the URL, you need to specify gx_charset along with the parameter. For example:

```
http://hostname:port/amserver/UI/Login?role=manager?role=%E3%81%82%&gx_charset=utf-8
```

Logfiles are Garbled in Ja Locale (#4882286)

The following log files contains Japanese characters and garbled when opened:

All the files in *IdentityServer_base* / SUNWam/debug directory except deploy.log and undeploy.log.

Locale Parameter In URL Displays Mixed Login Page (#4915137)

If you are using a non-English based browser with an instance of Identity Server installed with WebServer and login to http://<host>:<port>/amserver/UI/Login?locale=en, the login page will display with a mix of English and non-English characters.

Workaround

Change the following symbolic link:

I*dentityServer_base*/SUNWam/web-apps/services/config/auth/default

to

IdentityServer_base/SUNWam/web-apps/services/config/auth/default_en

Unlocalized Error Message For HTTP Basic (#4921418)

If you log in using the HTTP Basic authentication module, and click on the Cancel button, an Unlocalized error message will be displayed. This is a known problem with Application Server; it occurs only when Identity Server is deployed with Application Server.

Mixed Locale In Login Window When Application Server Is ja (#4932089)

The Identity Server login window will not default back to English when the browser language setting is en and Application Server’s locale is set to ja.

Workaround

Run the Application Server with locale set to en.

Lockout Notification Sends Unreadable Email (#4938511)

If you run Identity Server with web container that has the preferred locale set to anything other than C and a user is locked out of the server, lockout notification email will be sent, but it will be unreadable.

Workaround

Set email|local|charset (instead of only the email parameter) in the Email Address to Send Lockout Notification attribute. For example:

```
user1@example.com|zh|GB2312
```

Conflict Resolution Level In Fixed Locale (#4922030)

If a user logs into the Identity Server console in a particular locale (for example, zh), registers the Authentication Configuration service, creates a template for the service, then logs out and logs in again with a different locale, the Conflict Resolution Level items will be incorrectly listed in the original locale's format.

am2bak And bak2am Version Messages Only In English (#4930610)

The am2bak and bak2am restore utilities' version messages are only available in English for this release.

Multi-byte Names Do Not Work in Self Registration (#4732470)

If you create a user in the Self Registration (Membership Authentication service) module with a duplicated user ID and a multi-byte First Name and Last Name, an error will occur. Multi-byte user IDs are not supported.

Workaround

If a user logs in using Self Registration in a multi-byte environment, the administrator must make sure that the User Generator Mode attribute in the Core Authentication is not selected.

or

The user can select the Create My Own option in the Self-Registration login page.

Japanese Version Of Identity Server Does Not Work With Netscape 6.22, 6.23 (#4902421)

In the Japanese version of Identity Server 6.1, you can not log into the console with Netscape 6.22 or 6.23.

Time Condition Format Does Not Change (#4888416)

In Time Conditions for policy definitions, the time display does not change from the following format, regardless of locale:

```
Hour:Minute AM/PM
```

Message for msgid-msgstr Pairs in backup_restore.po Not Localized(#4916683)

If you receive a message that explains that the msgid-mgstr pairs are missing in the backup_restore.po script and the Directory Server certificate is not backed up, the Directory Server is still backed up. This message has not been localized.

Client Detection Screen Not Localized (#4922013)

Portions of the Current Style Properties screen of the Client Detection interface were not localized in this release.

Updated genericHTML Client Property Does Not Get Applied (#4922348)

If you remove UTF-8 from the character set list in the Client Detection service's genericHTML client property, save the changes and then enable Client Detection, and then logout and login again, the login page is still in UTF-8 character set.

Workaround

Restart the server manually with amserver.

Log File Headers Not Localized (#4923536)

The first two lines of all log files are not localized, in particular the Version and Fields sections and their lists of fields.

Data Field Values Are Not Localized In amSSO.access (#4923549)

In the amSSO.access log file, all the values under the Data field are not localized.

Exception.jsp Has Hard-Coded Messages (#4772313)

Exception.jsp is not localized and contains hard-coded title, error messages and copyright information. This exceptional error jsp page is invoked only in extreme cases. Examples are when Directory Server is down, or when no Identity Server services can be brought up and no localization is available for this jsp page.

Cookies

Cookieless Mode is Not Working (#4967866)

If a browser accesses Identity Service and then the cookie support is turned off, and if the browser supports cookies, then the browser will continue to send the older Identity Server cookie. This causes access to Identity Server resources to be denied.

Workaround
Choose one of the following workarounds:

- Clear the browser cookie cache to remove all Identity Server cookies.
- Disable cookies in the browser.

Cookie Hijacking

Security may be compromised when applications using the session cookies cannot be trusted.

When single sign-on (SSO) or cross domain single sign-on (CDSSO) is enabled in your Identity Server deployment, `http(s)` session cookies are set on the user's browser. These cookies are validated across multiple applications. When the Identity Server is deploy across multiple DNS domains, the Liberty protocol transfers the `http(s)` session cookies from the authenticated DNS domain to web application's target domain.

Although the user is automatically signed on to web resources, there is a known security weakness when applications using the session cookies cannot be trusted. The weakness may be present when an Identity Provider provides authentication, authorization and profile information about a user to applications (or Service Providers) that are developed by 3rd parties or by unauthorized groups within the enterprise. Possible security issues are:

- All applications share the same `http` session cookie. This makes it possible for a rouge application to hijack the session cookie and impersonate the user to another application.
- If the application does not use the `https` protocol, the session cookie is prone to network eavesdropping.
- If just one application can be hacked, the security of the entire infrastructure is in jeopardy of being compromised.
- A rouge application can use the session cookie to obtain and possibly modify the profile attributes of a user. If the user has administrative privileges, the application would be able to do a lot more damage.

Workaround
Follow these steps:

1. Use the Identity Server administration console to make an entry for each agent.

   a. In the organization that contains the agent to be created, choose Agents from the View menu, and then click New.

   b. Provide the following information:

      Name. Enter the name or identity of the agent. Example: i.e. `agent123`

      Password. Enter the agent password. Example: `agent123`

      Confirm Password. Confirm the password.

      Description. Enter a brief description of the agent. For example, you can enter the agent instance name or the name of the application it is protecting.

      Agent Key Value. Set the agent properties with a key / value pair. This property is used by Identity Server to receive agent requests for credential assertions about users.

      Enter a property value for `agentRootURL` with value equal to the agent URL with port number. Note that the `agentRootURL` value is case sensitive.

      Example: `agentRootURL=http`: / /*server_name:99*/

      Device Status. Enter the device status of the agent. If set to Active, the agent will be able to authenticate to and communicate with Identity Server. If set to Inactive, the agent will not be able to authenticate to Identity Server.

   c. Click OK.

2. Run the following command on the password that was entered in step 1b.

   ```
   /opt/SUNWam/agents/bin/crypt_util agent123
   ```

   This will give the following output:

   ```
   WnmKUCg/y3l404ivWY6HPQ==
   ```

3. Change AMAgent.properties to reflect the new value, and then and restart the agent. Example:

```
# The username and password to use for the Application authentication module.


com.sun.am.policy.am.username = agent123
com.sun.am.policy.am.password = WnmKUCg/y3l404ivWY6HPQ==


# Cross-Domain Single Sign On URL

# Is CDSSO enabled.

com.sun.am.policy.agents.cdsso-enabled=true


# This is the URL the user will be redirected to after successful login

# in a CDSSO Scenario.

com.sun.am.policy.agents.cdcservletURL =
http://server.example.com:port/amserver/cdcservlet
```

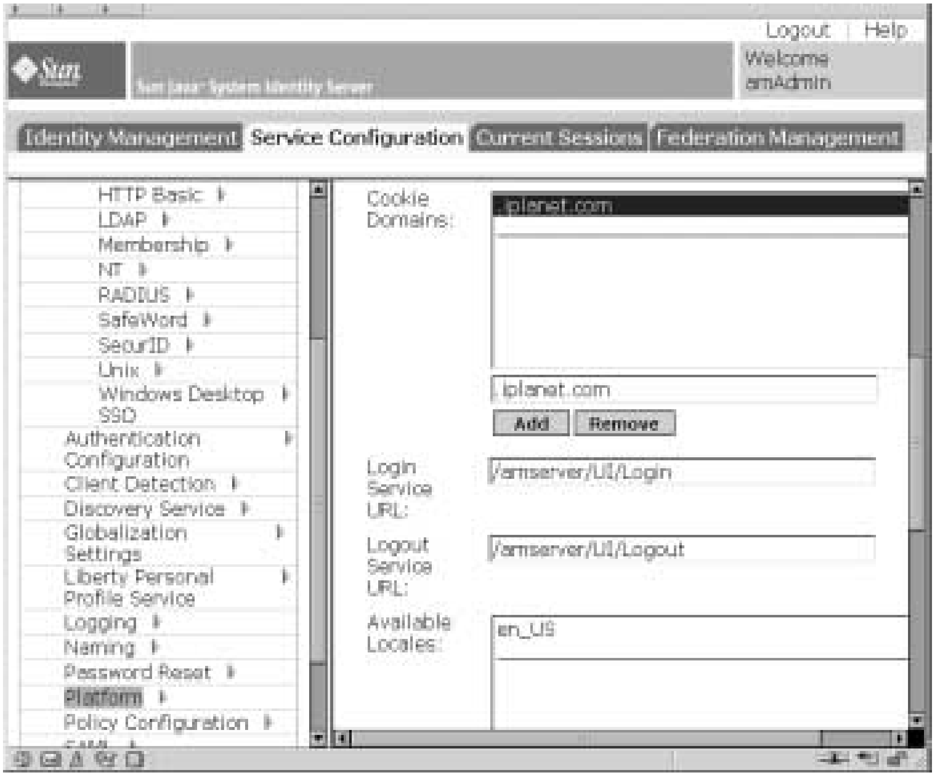
4. Change AMConfig.properties to reflect the new values, and then and restart Identity Server. Example:

```
com.sun.identity.enableUniqueSSOTokenCookie=true

com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer


com.sun.identity.authentication.uniqueCookieDomain=example.com
```

5. In the Identity Server administration console, choose Service Configuration>Platform.



Cookie Domains: .iplanet.com

.iplanet.com

Login Service URL: /amserver/UI/Login

Logout Service URL: /amserver/UI/Logout

Available Locales: en_US

6. In the Cookie Domains list, change the cookie domain name:

   a. Select the default `iplanet.com` domain, and then click Remove.

   b. Enter the host name of the Identity Server installation, and then click Add.

   Example: server.`example.com`

   You should see two cookies set on the browser:

Cookie	Host Name
`iPlanetDirectoryPro`	`server.example.com`
`sunIdentityServerAuthNServer`	`example.com`

Redistributable Files

Sun Java System Identity Server 2004Q2 does not contain any files which you can redistribute.

How to Report Problems and Provide Feedback

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

- Sun Software Support services online at http://www.sun.com/supportraining

  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. Use the web-based form to provide feedback to Sun:

http://docs.sun.com/coll/entsys_04

Please 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 these Release Notes document is 817-5712-10.

Additional Sun Resources

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

- Sun Java System Documentation
  http://docs.sun.com/db/prod/entsys.04q2
- Sun Java System Professional Services
  http://www.sun.com/service/products/software/javaenterprisesystem/
- Sun Java System Software Products and Service
  http://wwws.sun.com/software/
- Sun Java System Software Support Services
  http://www.sun.com/supportraining
- 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