Sun™ ONE Identity Server 6.1 Release Notes

Version 6.1

Part Number 816-6779-10

December 2003

These release notes contain important information available at the time of release of Version 6.1 of Sun™ Open Net Environment (Sun ONE) Identity Server. New features and enhancements, known limitations and problems, technical notes, and other information are addressed here. Read this document before you begin using Identity Server 6.1.

The most up-to-date version of these release notes can be found at the Sun ONE documentation web site: `http://docs.sun.com/prod/sunone`. 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 manuals.

These release notes contain the following sections:

- Revision History
- Identity Server 6.1 Documentation Set
- What's New in Identity Server, Version 6.1
- Hardware and Software Requirements
- Known Issues
- How to Report Problems and Provide Feedback
- Additional Sun Resources

Revision History

Table 1   Revision History

Date	Description of Changes
May 6, 2004	Added new descriptions to Known Problems section.

Table 1   Revision History *(Continued)*

Date	Description of Changes
February 20, 2004	Added new descriptions to Known Problems section.
January 8, 2004	Update to Known Problem #4732470 description.
December 8, 2003	Initial release of these release notes

Identity Server 6.1 Documentation Set

The Identity Server documentation set contains the following titles:

- *Product Brief* provides an overview of the Identity Server application and its features and functions.

- *Migration Guide* provides details on how to migrate existing data and Sun ONE product deployments to the latest version of Identity Server. For instructions on installing Identity Server, see the *Sun Java Enterprise System 2003Q4 Installation Guide*.

- *Administration Guide* describes how to use the Identity Server console as well as manage user and service data via the command line.

- *Customization and API Guide* documents how to customize an Identity Server installation. It also includes instructions on how to augment the application with new services using the public APIs.

- *Deployment Guide* provides information on planning an Identity Server deployment within an existing information technology infrastructure.

- The *Release Notes* will be available online after the product is released. They gather an assortment of last-minute information, including a description of what is new in this current release, known problems and limitations, installation notes, and how to report issues with the software or the documentation.

Identity Server Policy Agent Documentation Set

Policy agents for Identity Server are available on a different schedule than the server product itself. Therefore, the documentation set for the policy agents is available outside the core set of Identity Server documentation. The following titles are included in the set:

- *Web Policy Agents Guide* documents how to install and configure an Identity Server policy agent on various web and proxy servers. It also includes troubleshooting and information specific to each agent.

- *J2EE Policy Agents Guide* documents how to install and configure an Identity Server policy agent that can protect a variety of hosted J2EE applications. It also includes troubleshooting and information specific to each agent.

- The *Release Notes* will be available online after the set of agents is released. There is generally one *Release Notes* file for each agent type release. The *Release Notes* gather an assortment of last-minute information, including a description of what is new in this current release, known problems and limitations, installation notes, and how to report issues with the software or the documentation.

What's New in Identity Server, Version 6.1

The following sections lists the new features and the bugs that have been fixed in Identity Server 6.1.

- Java Enterprise System integration

- Federation Management includes Liberty 1.1 Specification requirements

- Support for SecurID® Authentication module

- Support for HTTP Basic Authentication module

- Support for deployment on Sun ONE Application Server 7.0

- SDK support on J2EE containers including, BEA WebLogic® and IBM WebSphere® Application servers

- C APIs for client Authentication and Single Sign-on

- Filtered roles support for User Management

- Password Reset/Forgotten Password service

- Globalization Settings service

- New Policy condition to support resource-based Session time-out

Bugs Fixed in Identity Server 6.1

Below is a short description of the most important bugs fixed in since the Identity Server 6.0 release.

Table 2 Fixed Bugs in Identity Server 6.1

Bug Number	Description
4787204	The password was stored in cleartext in Directory Server if basic authentication was used for the SAML trust relationship.
4702556	User search used different scope for simple and advanced searches.
4784279	Error received when creating a normal policy in a suborganization.
4787748	Unable to define referral policies for services with no defined resources.
4786584	Logout does not work with multiple Identity Server instances.
4816388	Port 80 issue in Federation Management code.
4825448	Prelogin service missing URL encoding of LRURL.
4837673	Authentication unable to create users with attributes from an external Directory Server.
4757643	Debug directories for additional Identity Server instances must have read and write permissions manually set.
4788320	Login fails if second service instance is created over SSL.
4781602	Installation fails with Directory Server with Password Policy enabled.
4697120	Reloading the Session Timeout page will authenticate user with valid username and password.
4759858	User login fails if DN To Start User Search is not set to the object.
4756294	Different directories must be specified for multiple SafeWord servers.
4738577	Problems creating policies with amadmin command line utility.
4786292	am2bak does not back up service configuration data when Directory Server is in SSL mode.
4786299	Identity Server unable to create log/debug files after a restore.

Hardware and Software Requirements

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

Table 3 Hardware and Software Requirements

Component	Solaris Requirement
Operating system	Solaris 8 or Solaris 9 (SPARC® platforms)
	Sun Solaris 9 for x86
CPU	Sun Ultra™ 1 (or compatible) workstation
RAM	512 Mbytes
Disk space	200 Mbytes for Identity Server and associated applications

New Information

This section contains the latest information that is not contained in the core product documentation.

Identity Server Security Service, Sun ONE Certificate Server 4.7 Not Supported in 6.1

Identity Server 6.0 provided an integration with Sun ONE Certificate Server 4.7 named the Identity Server Security Service (ISS). That integration allowed users authenticated by Identity Server 6.0 to be presented a digital certificate issuance button on their User Profile page.

In March of 2003, Sun announced the End of Life (EOL) of Certificate Server. Therefore, the ISS functionality is not present in Identity Server 6.1 and will not be carried forward in future releases of this product.

Errata and Identity Server Documentation Updates

The following section lists information that pertains to Identity Server features that was not included in the original release of the Identity Server 6.1 documentation set.

Identity Server Does Not Switch Over Properly in a High Availability Environment

Some of the default values set during installation may cause Identity Server to fail in a High Availability scenario.In such a scenario, once the node switches over, the Identity Server console will not allow you to log in. In a High Availability scenario, the encryption key should be filled out identically for both installation instances of the Identity Server.

Identity Server Removes Anonymous Bind During Installation

During installation, Identity Server removes the anonymous bind ACI for a fresh directory (not provisioned) installation. If you have any applications or samples that rely on anonymous bind, they will fail. Identity Server does not remove this ACI for existing (provisioned) directory installations.

Multiple Instances of Identity Server Do Not Contain Map Additions

If you have customized authentication screens and are also using `amserver` to create new Identity Server instances, MAP does not update Identity Server's `services.war` (Web Archive file), so the newly created instance does not contain MAP additions.

Workaround

Update the services.war file. By default, it is in the following location:

> *IdentityServer_base*/SUNWam/services.war

To update the services.war file, enter the following command:

```
jar -uvf services.war IdentityServer_base/SUNWam/services.war
```

The `uvf` option will replace the old file with the new modified one. For example:

```
cd /opt/SUNWam

jar -uvf services.war index.html

rm index.html
```

The following files can be modified:

- JSPs (`IdentityServer_base/SUNWam/web-apps/services/config/auth/default/*.jsp`)

- javascripts (`IdentityServer_base/SUNWam/web-apps/services/js/*.js`)

- images (`IdentityServer_base/SUNWam/web-apps/services/login_images/*.gif`)

- Cascading style sheets (`IdentityServer_base/SUNWam/web-apps/services/css/*.css`)

- xml files (`IdentityServer_base/SUNWam/web-apps/services/config/auth/default/*.xml`)

Web Container Redeployment

To redeploy the `.war` file to the Application Server web container, enter the following commands:

```
asadmin deploy -u $IAS7_ADMIN -w $IAS7_ADMINPASSWD -H $SERVER_HOST -p $IAS7_ADMINPORT
--type web $SECURE_FLAG --contextroot

$SERVER_DEPLOY_URI --name amserver --instance $IAS7INSTANCE
${BASEDIR}/${PRODUCT_DIR}/services.war
```

To redeploy the `.war` file to the BEA WebLogic web container, enter the following commands:

```
java weblogic.deploy -url $SERVER_URL -component ${SERVER_DEPLOY_URI}:${WL61 _SERVER}
deploy $WL61_ADMINPASSWD

${SERVER_DEPLOY_URI}

${BASEDIR}/${PRODUCT_DIR} /services.war
```

To redeploy the `.war` file to the IBM Websphere web container, see the deployment documentation at the following location:

http://www-3.ibm.com/software/webservers/studio/doc/v40/studioguide/en/html/sdsscenario1.html

Known Issues

This section contains a list of the more important known issues at the time of the Identity Server 6.1 release. This section covers the following topics:

- General
- Authentication
- Command Line Tools
- Identity Sever Console
- Logging Service
- Policy
- Session Service
- SDK
- Internationalization (i18n)

General

Roles and Groups Membership Not Updated in the User Cache

During Identity Server installation, the Java Enterprise System does not (by default) enable the Directory Server referential integrity plugin. As a result, Directory Server notifications are not generated when role membership and group membership changes occur. This is not a bug.

Workaround

See the `Sun ONE Identity Server Migration Guide` for instructions on configuring the referential integrity plugin.

Authentication

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.

Workaround

In `server.xml`, set `http.nonProxyHosts` to the host's fully qualified domain name and then restart the server. For example:

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

Authentication Fails On Anonymous Bind (#4919897)

During installation you are asked for the LDAP User ID and LDAP Password. If you leave both of these fields blank, then by default Identity Server performs an anonymous bind to Directory Server during authentication. This works as designed. If the Directory Server is configured to allow anonymous bind access, then authentication will succeed; otherwise, authentication will fail.

Workaround

Re-install Identity Server and be sure to provide values for LDAP User ID and LDAP Password during installation.

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.

HTTP Basic Does Not Work In Internet Explorer With Authlevel Login (#4945190)

The HTTP Basic authentication module does not work with Internet Explorer when you perform an Authlevel login.

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

Identity Server Instances Not Properly Deleted From Platforms List Using amserver (#4889686)

When you use the `amserver` command to create a new instance of Identity Server, and then delete the instance, the instance is not deleted from the Platforms List in the Service Configuration tab.

Workaround

To manually remove the instance name from the Platforms List:

1. In the Service Configuration tab, in the left frame, click Platforms.
2. In the right frame, in the Servers List, select the instance name, and then click Remove.

Startup Scripts Not Properly Deleted (#4794971)

When you use the `multiserverinstall` utility to create a new instance of Identity Server, and then delete the new instance, the startup scripts created at installation are left behind in the default directory `/etc/rc3.d/` You can remove these startup scripts manually.

Example:

```
cd /etc/rc3.d
rm S86amserver.<instanceName>
rm K86amserver.<instanceName>
```

Identity Sever Console

""** 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**`.

Re-registered Services Do Not Display Properly (#4915234)

When you register a service, then assign the service to a user, the service should be displayed in the user's profile. When you unregister the service, the service will no longer be displayed in the user's profile. This works as designed. However, if you re-register the service, before assigning the service to the user, the user's profile may display the service. This is a known problem. The service should not be displayed until you assign the service to a the user.

Filtered Role Memberships Not Displayed In User View (#4947334)

When you view a user's roles, the Identity Server Console does not display the user's filtered role membership.

Policies And Roles Sorted Incorrectly (#4914819)

If you create a number of policies and roles, they are not sorted in the correct order in the Identity Server Console.

Unregistered Service Incorrectly Listed As Registered (#4918930)

If you have only one service registered to the organization and then unregister the service, it will still be listed under Registered services in the Identity Server Console.

Close Button Does Not Function In Role Pages (#4919099)

In the Identity Sever Console, clicking the Close button will not work in the Role pages for users logged in with the view set to `roleDN`.

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.

Apostrophes In Suborganization Names Cause Errors (#4922287)

When creating a suborganization, the name should not contain any apostrophes ('). Apostrophes in suborganization names cause javascript errors.

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

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`. 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

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 Sever 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)

Problem With zh_CN.GB18030 Locale (#4925958)

When Identity Server is started the in `zh_CN.GB18030` locale, problems may occur, including corrupted files and failure to start Identity Server functions.

Workaround

In the Identity Server Console, go to the Globalization Settings service and set `UTF-8` as the default character set for the `zh` locale.

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
```

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:

```
/opt/SUNWam/web-apps/services/config/auth/default
```

to

```
/opt/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 occurs when Identity Server is deployed with Application Server only.

Incorrect Default Globalization Settings For Korean Character Set (#4921424)

The Charsets Supported by each Locale attribute in the Globalization Settings service currently contains the following default value:

```
locale=ko|charset=UTF-8;Johab
```

It should contain the following locale:

```
UTF-8;EUC-KR
```

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
```

Javascript Error With zh_CN.GB18030 Locale (#4948665)

Identity Server will display a Javascript error if the web container is started is with the locale defined as `zh_CN.GB180130`.

Workaround

Restart the server in with other locales, such as `C` or `zh`.

Cannot Restart Server With amserver If serverconfig.xml Is Not In UTF-8 Format (#4910650)

`ampssword` will update serverconfig.xml and, by default, `serverconfig.xml` is in UTF-8 after installation. If `serverconfig.xml` includes multi-byte data and you run ampassword in a non-UTF-8 locale, `serverconfig.xml` will be in natice encoding. amserver will not be able to retart the server.

Workaround

Run `ampassword` in UTF-8 locale, then restart `amserver`.

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:Munute 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 (#4773213)

Exception.jsp is not localized and contains hard-coded title, error messages and copyright information.

How to Report Problems and Provide Feedback

If you have problems with Sun ONE Identity Server, 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 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. Email your comments to Sun at this address:

docfeedback@sun.com

Please include the part number and the full title of the document that you would like to address in the subject line of your email. The part number can be found on the title page of the book, and is usually a seven or ten digit number, for example: 123-4567-10.

Additional Sun Resources

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

- Sun ONE Documentation
  http://docs.sun.com/prod/sunone

- Sun ONE Professional Services
  http://www.sun.com/service/sunps/sunone

- Sun ONE Software Products and Service
  http://www.sun.com/software

- Sun ONE Software Support Services
  http://www.sun.com/service/sunone/software

- Sun ONE Support and Knowledge Base
  http://www.sun.com/service/support/software

- Sun Support and Training Services
  http://www.sun.com/supporttraining

- Sun ONE Consulting and Professional Services
  http://www.sun.com/service/sunps/sunone

- Sun ONE Developer Information
  http://sunonedev.sun.com

- Sun Developer Support Services
  http://www.sun.com/developers/support

- Sun ONE Software Training
  http://www.sun.com/software/training

- Sun Software Data Sheets
  http://wwws.sun.com/software

Additional Sun Resources