Sun OpenSSO Enterprise 8.0 Administration Reference

Part No: 820–3886
November 2008

100222@23474

Contents

Preface

Note – Please be advised that this book has been published for the OpenSSO Enterprise 8.0 Early Access release. The information contained in this book may not reflect the most current release of the software.

The Sun OpenSSO Enterprise 8.0 Administration Guide describes how to use the Sun Java™ System OpenSSO Enterprise console as well as manage user and service data via the command line interface.

Who Should Use This Book

This book is intended for use by IT administrators and software developers who implement a web access platform using Sun Java System servers and software.

Before You Read This Book

Readers should be familiar with the following components and concepts:

- OpenSSO Enterprise technical concepts as described in the *Sun OpenSSO Enterprise 8.0 Technical Overview*.
- Deployment platform: Solaris™ or Linux operating system
- Web container that will run OpenSSO Enterprise: Sun Java System Application Server, Sun Java System Web Server, BEA WebLogic, or IBM WebSphere Application Server

- Technical concepts: Lightweight Directory Access Protocol (LDAP), Java technology, JavaServer Pages™ (JSP) technology, HyperText Transfer Protocol (HTTP), HyperText Markup Language (HTML), and eXtensible Markup Language (XML)

Related Documentation

Related documentation is available as follows:

- "OpenSSO Enterprise Documentation Set" on page 14
- "Related Product Documentation" on page 15

OpenSSO Enterprise Documentation Set

The following table describes the OpenSSO Enterprise documentation set.

TABLE P–1 OpenSSO Enterprise Documentation Set

Title	Description
Sun OpenSSO Enterprise 8.0 Release Notes	Describes new features, installation notes, and known issues and limitations. The Release Notes are updated periodically after the initial release to describe any new features, patches, or problems.
Sun OpenSSO Enterprise 8.0 installation and Configuration Guide	Provides information about installing and configuring OpenSSO Enterprise including OpenSSO Enterprise server, Administration Console only, client SDK, scripts and utilities, Distributed Authentication UI server, and session failover.
Sun OpenSSO Enterprise 8.0 Technical Overview	Provides an overview of how components work together to consolidate access control functions, and to protect enterprise assets and web-based applications. It also explains basic concepts and terminology.
Sun OpenSSO Enterprise 8.0 Deployment Planning Guide	Provides planning and deployment solutions for OpenSSO Enterprise.
Sun OpenSSO Enterprise 8.0 Administration Guide	Describes how to use the OpenSSO Enterprise Administration Console as well as how to manage user and service data using the command-line interface (CLI).
Sun OpenSSO Enterprise 8.0 Administration Reference	Provides reference information for the OpenSSO Enterprise command-line interface (CLI), configuration attributes, log files, and error codes.
Sun OpenSSO Enterprise 8.0 Developer's Guide	Provides information about customizing OpenSSO Enterprise and integrating its functionality into an organization's current technical infrastructure. It also provides details about the programmatic aspects of the product and its API.

TABLE P–1 OpenSSO Enterprise Documentation Set *(Continued)*

Title	Description
Sun OpenSSO Enterprise 8.0 C API Reference for Application and Web Policy Agent Developers	Provides summaries of data types, structures, and functions that make up the public OpenSSO Enterprise C APIs.
Sun OpenSSO Enterprise 8.0 Java API Reference	Provides information about the implementation of Java packages in OpenSSO Enterprise.
Sun OpenSSO Enterprise 8.0 Performance Tuning Guide	Provides information about how to tune OpenSSO Enterprise and its related components for optimal performance.
Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide	Provides an overview of version 3.0 policy agents.

Related Product Documentation

The following table provides links to documentation collections for related products.

TABLE P–2 Related Product Documentation

Product	Link
Sun Java System Directory Server 6.3	`http://docs.sun.com/coll/1224.4`
Sun Java System Web Server 7.0 Update 3	`http://docs.sun.com/coll/1653.3`
Sun Java System Application Server 9.1	`http://docs.sun.com/coll/1343.4`
Sun Java System Message Queue 4.1	`http://docs.sun.com/coll/1307.3`
Sun Java System Web Proxy Server 4.0.6	`http://docs.sun.com/coll/1311.6`
Sun Java System Identity Manager 7.1	`http://docs.sun.com/coll/1514.3`

Searching Sun Product Documentation

Besides searching Sun product documentation from the docs.sun.com℠ web site, you can use a search engine by typing the following syntax in the search field:

search-term `site:docs.sun.com`

For example, to search for "broker," type the following:

```
broker site:docs.sun.com
```

To include other Sun web sites in your search (for example, java.sun.com, www.sun.com, and developers.sun.com), use `sun.com` in place of `docs.sun.com` in the search field.

Related Third-Party Web Site References

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 or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (`http://www.sun.com/documentation/`)
- Support (`http://www.sun.com/support/`)
- Training (`http://www.sun.com/training/`)

Default Paths and Directory Names

The OpenSSO Enterprise documentation uses the following terms to represent default paths and directory names:

TABLE P–3 Default Paths and Directory Names

Term	Description
zip-root	Represents the directory where the `opensso.zip` file is unzipped.

OpenSSO-Deploy-base	Represents the deployment directory where the web container deploys the `opensso.war` file.
	This value varies depending on the web container. To determine the value of *OpenSSO-Deploy-base*, view the file name in the `.openssocfg` directory, which resides in the home directory of the user who deployed the `opensso.war` file. For example, consider this scenario with Application Server 9.1 as the web container:
	■ Application Server 9.1 is installed in the default directory: `/opt/SUNWappserver`.
	■ The `opensso.war` file is deployed by super user (`root`) on Application Server 9.1.
	The `.openssocfg` directory is in the `root` home directory (`/`), and the file name in `.openssocfg` is:
	`AMConfig_opt_SUNWappserver_domains_domain1_applications_j2ee-modules_opensso_`
	Then, the value for *OpenSSO-Deploy-base* is:
	`/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/opensso`

ConfigurationDirectory	Represents the name of the configuration directory specified during the initial configuration of OpenSSO Enterprise server instance using the Configurator. The default is `opensso` in the home directory of the user running the Configurator. Thus, if the Configurator is run by `root`, *ConfigurationDirectory* is `/opensso`.

Common Criteria Requirements for Administrators

Sun OpenSSO Enterprise 8.0 Update 1 conforms to the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) at Assurance Level EAL4, provided that you follow the requirements listed in Chapter 1, "Getting Started With OpenSSO Enterprise 8.0," in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*. An OpenSSO Enterprise 8.0 Update 1 administrator performs tasks such as installing, configuring, and managing the product. This administrator must be trustworthy, non-hostile, appropriately trained, and willing to follow the following guidance documentation:

- *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*
- Sun OpenSSO Enterprise 8.0 Administration Reference (this guide)
- *Sun OpenSSO Enterprise 8.0 Administration Guide*
- Sun OpenSSO Enterprise 8.0 Online Help

Caution – A administrator must not use the OpenSSO Enterprise 8.0 Update 1 Administration Console or command-line utilities to modify the security functionality of OpenSSO Enterprise 8.0 Update 1. Otherwise, OpenSSO Enterprise 8.0 Update 1 will not conform to the Common Criteria evaluated level.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions.

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

For example, the title of this book is *Sun OpenSSO Enterprise 8.0 Administration Reference*, and the part number is 820–3886.

PART I

Command Line Interface Reference

◆ ◆ ◆ CHAPTER 1

ssoadm Command Line Interface Reference

This chapter provides information on the OpenSSO Enterprise `ssoadm` command line interface. This interface is new to the 8.0 release and replaces the `amadmin` command line tool used in previous releases. `ssoadm` has a multitude of sub commands that perform specific tasks for creating, deleting, and managing all OpenSSO Enterprise data. These sub commands are grouped by functional area.

Note – `amadmin` is still supported for backwards computability for versions that have been upgraded to OpenSSO. See Chapter 2, "The amadmin Command Line Tool," for more information.

The primary purpose of `ssoadm` is to load data configuration data into the data store and to perform batch administrative tasks on the DIT. For information and instructions to unpack and set up `ssoadm`, see "Installing the OpenSSO Enterprise Utilities and Scripts in the ssoAdminTools.zip File" in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*.

`ssoadm` is primarily used to:

- Load XML service files - Administrators load services into OpenSSO Enterprise that use the XML service file format defined in the `sms.dtd`. .

Note – XML service files are stored in the data store as static *blobs* of XML data that is referenced by OpenSSO Enterprise. This information is not used by Directory Server, which only understands LDAP.

- Perform batch updates of identity objects to the DIT - Administrators can perform batch updates to the Directory Server DIT using the `do-batch` subcommand. For example, if an administrator wants to create 10 organizations, 1000 users, and 100 groups, it can be done in one attempt by putting the requests in one or more batch processing XML files and loading them using `ssoadm`.

When ssoadm is executed, the command performs a version check of the OpenSSO Enterprise server. If the expected server version does not match, the ssoadm command will fail.

Using the ssoadm Command Line Interface

ssoadm contains many subcommands to perform specific tasks for a services, plug-ins, polices federation profiles, and so forth. Each subcommand contains a number of options, both required and non-required, that are defined to carry out these tasks. The following sections describe the usage of the subcommands and their associated options.

The basic syntax for the ssoadm command is:

```
ssoadm subcommand --options [--global-options]
```

The following global options are common to all subcommands, but are not required for the command to function:

[--locale, -l]	Name of the locale to display the results.
[--debug, -d]	Run in debug mode. Results sent to the debug file.
[--verbose, -v]	Run in verbose mode. Results sent to standard output.

Password File

In most ssoadm subcommands, the password file is required option. The password file is a simple file that contains the administrator password for the given task. To create a password file:

1. Create the password file in a location you will remember. For example:

   ```
   echo "" > /tmp/testpwd
   ```

2. It is recommended to change the permissions to read-only:

   ```
   chmod 400 /tmp/testpwd
   ```

ssoadm Usage Example

This section provides an example of how you can use the ssoadm command-line for a subcommand. This example highlights the update-agent option. The update-agent option allows you to configure agent properties. The following is an example of how the ssoadm command can be issued with the update-agent option.

```
# ./ssoadm update-agent -e testRealm1 -b testAgent1 -u amadmin -f
/tmp/testpwd -a "com.sun.identity.agents.config.notenforced.url[0]=/exampledir/public/*"
```

Caution – When issuing the `ssoadm` command, if you include values that contain wildcards (* or `-*-`), then the property name/value pair should be enclosed in double quotes to avoid substitution by the shell. This applies when you use the `-a` (`--attributevalues`) option. The double quotes are not necessary when you list the properties in a data file and access them with the `-D` option.

Listing Options for an ssoadm Subcommand

You can read the options for a subcommand from this section or you can list the options yourself while using the command. On the machine hosting OpenSSO Enterprise, in the directory containing the `ssoadm` utility, issue the `ssoadm` command with the appropriate subcommand. For example:

```
# ./ssoadm update-agent
```

Since the preceding command is missing required options, the utility merely lists all the options available for this subcommand. The global options are common to all subcommands. For example:

```
ssoadm update-agent --options [--global-options]
Update agent configuration.
Usage:
ssoadm
    --realm|-e
    --agentname|-b
    --adminid|-u
    --password-file|-f
    [--set|-s]
    [--attributevalues|-a]
    [--datafile|-D]

Global Options:
    --locale, -l
        Name of the locale to display the results.

    --debug, -d
        Run in debug mode. Results sent to the debug file.

    --verbose, -v
        Run in verbose mode. Results sent to standard output.

Options:
    --realm, -e
```

```
    Name of realm.

--agentname, -b
    Name of agent.

--adminid, -u
    Administrator ID of running the command.

--password-file, -f
    File name that contains password of administrator.

--set, -s
    Set this flag to overwrite properties values.

--attributevalues, -a
    properties e.g. homeaddress=here.

--datafile, -D
    Name of file that contains attributes and corresponding values as in attribute-name=attribute-value. Enter one attr
```

Subcommand Usage

By looking at the usage information of a subcommand, you can determine which options are required and which are optional. You can list an option for the command with either a single letter, such as `-e` or with an entire word, such as `--realm`. The following is a list of the usage information for the `update-agent` subcommand:

```
ssoadm update-agent
    --realm|-e
    --agentname|-b
    --adminid|-u
    --password-file|-f
    [--set|-s]
    [--attributevalues|-a]
    [--datafile|-D]
```

The options not bounded by square brackets are required. Therefore, `realm`, `agentname`, `adminid`, `password-file`. However, even though the three options in brackets (the global options) are considered optional, you must use either `--attributevalues` or `--datafile` to provide a property name and the corresponding value. The `--attributevalues` option is appropriate for assigning values to a single property. The `--datafile` option is appropriate for setting several properties at once. The `realm` and `agentname` options identify the specific agent you are configuring. The `adminid` and `password-file` commands identify you as someone who has the right to configure this agent.

The following command serves as an example of how you can change several agent properties at once. In this scenario the properties and their respective values are stored in a file, `/tmp/testproperties`, to which the command points:

```
# ./ssoadm update-agent -e testRealm1 -b testAgent1 -u amadmin -f
/tmp/testpwd -D /tmp/testproperties
```

For subcommand options that accept multiple values, the values are space-separated and placed within quotation marks. For example, the `--attrubutevalues` option, uses the following format:

`–attributevalues "`*attributename*`=value" "`*attributename*`=value2"`

ssoadm Subcommands and Options

The following section lists the `ssoadm` subcommands and their associated options. The sub commands are grouped under the following functional areas:

Agent Configuration

The following subcommands execute operations for the supported agent profile types defined in the OpenSSO Centralized Agent Configuration service.

add-agent-to-grp

Add agents to an agent group.

Syntax

```
ssoadm add-agent-to-grp --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentgroupname, -b`	The name of the agent group.
`--agentnames, -s`	The names of the agent.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

agent-remove-props

Remove an agent's properties.

Syntax

```
ssoadm agent-remove-props --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentname, -b`	The name of the agent.
`--attributenames, -a`	The names of the properties.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

create-agent

Create a new agent configuration.

Syntax

```
ssoadm create-agent --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentname, -b`	The name of the agent.
`--agenttype, -t`	The type of agent. For example, J2EEAgent or WebAgent.
`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The properties. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

create-agent-grp

Create a new agent group.

Syntax

```
ssoadm create-agent-grp --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentgroupname, -b`	The name of the agent's group.
`--agenttype, -t`	The type of agent. For example, J2EEAgent or WebAgent.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The properties. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

delete-agent-grps

Delete existing agent groups.

Syntax

```
ssoadm delete-agent-grps --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentgroupnames, -s`	The names of the agent group.
`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.

delete-agents

Delete existing agent configurations.

Syntax

```
ssoadm delete-agents --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentnames, -s`	The names of the agent.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

list-agent-grp-members

List the agents in an agent group.

Syntax

```
ssoadm list-agent-grp-members --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentgroupname, -b`	The name of the agent group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--filter, -x]`	Filter by a pattern.

list-agent-grps

List the agent groups.

Syntax

```
ssoadm list-agent-grps --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--filter, -x]`	Filter by a pattern.
`[--agenttype, -t]`	The type of agent. For example, J2EEAgent or WebAgent.

list-agents

List the agent configurations.

Syntax

```
ssoadm list-agents --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--filter, -x]`	Filter by a pattern.
`[--agenttype, -t]`	The type of agent. For example, J2EEAgent or WebAgent.

remove-agent-from-grp

Remove agents from an agent group.

Syntax

```
ssoadm remove-agent-from-grp --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentgroupname, -b`	The name of the agent group.
`--agentnames, -s`	The names of the agent.
`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.

show-agent

Show the agent profile.

Syntax

```
ssoadm show-agent --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentname, -b`	The name of the agent.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--outfile, -o]`	The filename where configuration is written.
`[--inherit, -i]`	Set this option to inherit properties from the parent group.

show-agent-grp

Show the agent group profile.

Syntax

```
ssoadm show-agent-grp --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentgroupname, -b`	The name of the agent group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--outfile, -o]`	The filename where configuration is written.

show-agent-membership

List the agent's membership.

Syntax

```
ssoadm show-agent-membership --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentname, -b`	The name of the agent.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

show-agent-types

Show the agent types.

Syntax

```
ssoadm show-agent-types --options [--global-options]
```

Options

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

update-agent

Update the agent's configuration.

Syntax

```
ssoadm update-agent --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentname, -b`	The name of the agent.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--set, -s]`	Set this flag to overwrite a property's values.
`[--attributevalues, -a]`	The properties. For example, `homeaddress=here`.

`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

update-agent-grp

Update the agent group's configuration.

Syntax

```
ssoadm update-agent-grp --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--agentgroupname, -b`	The name of the agent group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--set, -s]`	Set this flag to overwrite a property's values.
`[--attributevalues, -a]`	The properties. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

Authentication Service Management

The following subcommands execute operations for the OpenSSO Enterprise Authentication service.

add-auth-cfg-entr

Add an authentication configuration entry.

Syntax

```
ssoadm add-auth-cfg-entr --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.

`--name, -m`	The name of the authentication configuration.
`--modulename, -o`	The module name.
`--criteria, -c`	The criteria for this entry. Possible values are `REQUIRED`, `OPTIONAL`, `SUFFICIENT`, and `REQUISITE`.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--options, -t]`	The options for this entry.
`[--position, -p]`	The position where the new entry is to be added.

create-auth-cfg

Create an authentication configuration.

Syntax

```
ssoadm create-auth-cfg --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--name, -m`	The name of the authentication configuration.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

create-auth-instance

Create an authentication instance.

Syntax

```
ssoadm create-auth-instance --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--name, -m`	The name of the authentication instance.
`--authtype, -t`	The type of authentication instance. For example LDAP or DataStore.

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

delete-auth-cfgs

Delete existing authentication configurations.

Syntax

```
ssoadm delete-auth-cfgs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--names, -m`	The names of the authentication configurations.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

delete-auth-instances

Delete existing authentication instances.

Syntax

```
ssoadm delete-auth-instances --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--names, -m`	The names of the authentication instances.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

get-auth-cfg-entr

Get the authentication configuration entries.

Syntax

```
ssoadm get-auth-cfg-entr --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--name, -m`	The name of the authentication configuration.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

get-auth-instance

Get the authentication instance values.

Syntax

```
ssoadm get-auth-instance --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--name, -m`	The name of the authentication instance.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

list-auth-cfgs

List the authentication configurations.

Syntax

```
ssoadm list-auth-cfgs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

list-auth-instances

List the authentication instances.

Syntax

```
ssoadm list-auth-instances --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

register-auth-module

Register an authentication module.

Syntax

```
ssoadm register-auth-module --options [--global-options]
```

Options

`--authmodule, -a`	The Java class name of the authentication module.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

unregister-auth-module

Unregister the authentication module.

Syntax

```
ssoadm unregister-auth-module --options [--global-options]
```

Options

`--authmodule, -a`	The Java class name of the authentication module.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

update-auth-cfg-entr

Set the authentication configuration entries.

Syntax

```
ssoadm update-auth-cfg-entr --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--name, -m`	The name of the authentication configuration.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--entries, -a]`	The formatted authentication configuration entries.
`[--datafile, -D]`	The filename that contains the formatted authentication configuration entries. Enter one *attribute-name=attribute-value* per line.

update-auth-instance

Update the authentication instance values.

Syntax

```
ssoadm update-auth-instance --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--name, -m`	The name of the authentication instance.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

Datastore Management

The following subcommands execute operations for managing OpenSSO Enterprise datastores.

add-amsdk-idrepo-plugin

Create the AMSDK IdRepo plug-in.

Syntax

```
ssoadm add-amsdk-idrepo-plugin --options [--global-options]
```

Options

`--directory-servers, -s`	Contains the Directory Servers, and can contain multiple entries. Use the following format: *protocol*`://`*hostname*`:`*port*
`--basedn, -b`	The Directory Server base distinguished name.
`--dsame-password-file, -x`	The filename that contains the password of the dsameuser.
`--puser-password-file, -p`	The filename that contains the password of the puser.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--user, -a]`	The user objects naming attribute (defaults to `uid`).
`[--org, -o]`	the organization objects naming attribute (defaults to `o`).

create-datastore

Create a datastore under a realm.

Syntax

```
ssoadm create-datastore --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--name, -m`	The name of the datastore.
`--datatype, -t`	The type of the datastore.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

`[--attributevalues, -a]`	The attribute values. For example, `sunIdRepoClass=com.sun.identity.idm.plugins.ldapv3.LDAPv3Re`
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

delete-datastores

Delete the data stores under a realm.

Syntax

```
ssoadm delete-datastores --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--names, -m`	The names of the data stores.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

list-datastore-types

List the supported data store types.

Syntax

```
ssoadm list-datastore-types --options [--global-options]
```

Options

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

list-datastores

List the data stores under a realm.

Syntax

```
ssoadm list-datastores --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

show-datastore

Show the data store profile.

Syntax

```
ssoadm show-datastore --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--name, -m`	The name of the datastore.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

update-datastore

Update the datastore profile.

Syntax

```
ssoadm update-datastore --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--name, -m`	The name of the datastore.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `sunIdRepoClass=com.sun.identity.idm.plugins.files.FilesRepo`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and

value per line.

Identity Management

The following subcommands execute operations for managing identities associated with OpenSSO Enterprise.

add-member

Add an identity as a member of another identity.

Syntax

```
ssoadm add-member --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--memberidname, -m`	The name of the member's identity.
`--memberidtype, -y`	The type of the member's identity. For example, User, Role or Group.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

add-privileges

Add privileges to an identity.

Syntax

```
ssoadm add-privileges --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.

`--privileges, -g`	The names of the privileges to be added.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

add-svc-identity

Add a service to an identity.

Syntax

```
ssoadm add-svc-identity --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

create-identity

Create an identity in a realm.

Syntax

```
ssoadm create-identity --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `inetuserstatus=Active`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

delete-identities

Delete the identities in a realm.

Syntax

```
ssoadm delete-identities --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

get-identity

Get the identity property values.

Syntax

```
ssoadm get-identity --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

`--attributenames, -a`	The attribute names. All attribute values will be returned if this option is not provided.

get-identity-svcs

Get the service in an identity.

Syntax

```
ssoadm get-identity-svcs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributenames, -a]`	Attribute name(s). All attribute values shall be returned if the option is not provided.

list-identities

List the identities in a realm.

Syntax

```
ssoadm list-identities --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--filter, -x`	Filter by a pattern.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

list-identity-assignable-svcs

List the assignable services for an identity.

Syntax

```
ssoadm list-identity-assignable-svcs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

remove-member

Remove the membership of an identity from another identity.

Syntax

```
ssoadm remove-member --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--memberidname, -m`	The name of the member's identity.
`--memberidtype, -y`	The type of the member's identity. For example, User, Role or Group.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

remove-privileges

Remove the privileges from an identity.

Syntax

```
ssoadm remove-privileges --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--privileges, -g`	The names of the privileges to be removed.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

remove-svc-identity

Remove a service from an identity.

Syntax

```
ssoadm remove-svc-identity --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

set-identity-attrs

Set the attribute values of an identity.

Syntax

```
ssoadm set-identity-attrs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

set-identity-svc-attrs

Set the service attribute values of an identity.

Syntax

```
ssoadm set-identity-svc-attrs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

show-identity-ops

Show the allowed operations of an identity in a realm.

Syntax

```
ssoadm show-identity-ops --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

show-identity-svc-attrs

Show the service attribute values of an identity.

Syntax

```
ssoadm show-identity-svc-attrs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

show-identity-types

Show the supported identity types in a realm.

Syntax

```
ssoadm show-identity-types --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.

show-members

Show the members of an identity. For example, the members of a role.

Syntax

```
ssoadm show-members --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--membershipidtype, -m`	The membership identity type.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

show-memberships

Show the memberships of an identity. For example, the memberships of a user.

Syntax

```
ssoadm show-memberships --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--membershipidtype, -m`	The membership identity type.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

show-privileges

Show the privileges assigned to an identity.

Syntax

```
ssoadm show-privileges --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--idname, -i`	The name of the identity.
`--idtype, -t`	The type of the identity. For example, User, Role or Group.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

Realm and Policy Management

The following subcommands execute operations for managing realms and policies in OpenSSO Enterprise.

add-svc-attrs

Add service attribute values in a realm.

Syntax

```
ssoadm add-svc-attrs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

add-svc-realm

Add a service to a realm.

Syntax

```
ssoadm add-svc-realm --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

create-policies

Create policies in a realm.

Syntax

```
ssoadm create-policies --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--xmlfile, -X`	The filename that contains the policy XML definition.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

create-realm

Create a realm.

Syntax

```
ssoadm create-realm --options [--global-options]
```

Options

`--realm, -e`	The name of the realm to be created.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

delete-policies

Delete policies from a realm.

Syntax

```
ssoadm delete-policies --options [--global-options]
```

Options

`--realm, -e`	The name of the realm to which the policy belongs.
`--policynames, -p`	The names of the policies to be deleted.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

delete-realm

Delete a realm.

Syntax

```
ssoadm delete-realm --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--recursive, -r]`	Deletes the descendent realms recursively.

delete-realm-attr

Delete an attribute from a realm.

Syntax

```
ssoadm delete-realm-attr --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--servicename, -s`	The name of the service.
`--attributename, -a`	The name of the attribute to be removed.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

get-realm

Get the realm property values.

Syntax

```
ssoadm get-realm --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

get-realm-svc-attrs

Get the realm's service attribute values.

Syntax

```
ssoadm get-realm-svc-attrs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.

list-policies

List the policy definitions in a realm.

Syntax

```
ssoadm list-policies --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--policynames, -p]`	The names of the policy. This can be used as a wildcard. All policy definitions in the realm will be returned.
`[--outfile, -o]`	The filename where the policy definition will be written. The definitions will be printed in standard output.

list-realm-assignable-svcs

List the realm's assignable services.

Syntax

```
ssoadm list-realm-assignable-svcs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

list-realms

List the realms by name.

Syntax

```
ssoadm list-realms --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--filter, -x]`	Filter by a pattern.
`[--recursive, -r]`	Search recursively.

remove-svc-attrs

Remove a realm's service attribute values.

Syntax

```
ssoadm remove-svc-attrs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values to be removed. For example, `homeaddress=here`.
`[--datafile, -D]`	The filename that contains the attribute values to be removed, configured as in *attribute-name=attribute-value*. Enter one attribute and value per line.

remove-svc-realm

Remove a service from a realm.

Syntax

```
ssoadm remove-svc-realm --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.

`--servicename, -s`	The name of the service to be removed.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

set-realm-attrs

Set a realm's attribute values.

Syntax

```
ssoadm set-realm-attrs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--append, -p]`	Set this flag to append the values to existing ones.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

set-svc-attrs

Set the realm's service attribute values.

Syntax

```
ssoadm set-svc-attrs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.
`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

show-auth-modules

Show the supported authentication modules in the system.

Syntax

```
ssoadm show-auth-modules --options [--global-options]
```

Options

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

show-data-types

Show the supported data types in the system.

Syntax

```
ssoadm show-data-types --options [--global-options]
```

Options

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

show-realm-svcs

Show the services in a realm.

Syntax

```
ssoadm show-realm-svcs --options [--global-options]
```

Options

`--realm, -e`	The name of the realm.

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--mandatory, -y]`	Include mandatory services.

Service Management

The following subcommands execute operations for managing realms and policies in OpenSSO Enterprise.

add-attr-defs

Add the default attribute values in a schema.

Syntax

```
ssoadm add-attr-defs --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.
`[--subschemaname, -c]`	The name of the sub schema.

add-attrs

Add an attribute schema to an existing service.

Syntax

```
ssoadm add-attrs --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributeschemafile, -F`	An XML file containing the attribute schema definition.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

add-plugin-interface

Add the plug-in interface to a service.

Syntax

```
ssoadm add-plugin-interface --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--interfacename, -i`	The name of the interface.
`--pluginname, -g`	The name of the plug-in.
`--i18nkey, -k`	The i18n key plug-in.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

add-sub-schema

Add a sub schema.

Syntax

```
ssoadm add-sub-schema --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.

`--filename, -F`	The filename that contains the schema.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

create-boot-url

Create a bootstrap URL that can bootstrap the product web application.

Syntax

```
ssoadm create-boot-url --options [--global-options]
```

Options

`--dshost, -t`	The Directory Server hostname.
`--dsport, -p`	The Directory Server port number.
`--basedn, -b`	The Directory Server base distinguished name.
`--dsadmin, -a`	The Directory Server base distinguished name.
`--dspassword-file, -x`	The filename that contains the Directory Server administrator password.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--ssl, -s]`	Set this flag for LDAPS.

create-sub-cfg

Create a new sub configuration.

Syntax

```
ssoadm create-sub-cfg --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--subconfigname, -g`	The name of the sub configuration.
`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.
`[--realm, -e]`	The name of the realm. The sub configuration will be added to the global configuration if this option is not selected.
`[--subconfigid, -b]`	The ID of the parent configuration. The sub configuration will be added to the root configuration if this option is not selected.
`[--priority, -p]`	The priority of the sub configuration.

create-svc

Create a new service in the server.

Syntax

```
ssoadm create-svc --options [--global-options]
```

Options

`--xmlfile, -X`	The XML file that contains the schema.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--continue, -c]`	Continue adding services if one or more previous services can not be added.

create-svrcfg-xml

Create the `serverconfig.xml` file.

Syntax

```
ssoadm create-svrcfg-xml --options [--global-options]
```

Options

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

`[--dshost, -t]`	The Directory Server hostname.
`[--dsport, -p]`	The Directory Server port number.
`[--basedn, -b]`	The Directory Server base distinguished name.
`[--dsadmin, -a]`	The Directory Server base distinguished name.
`[--dspassword-file, -x]`	The filename that contains the Directory Server administrator password.
`[--outfile, -o]`	The filename where serverconfig.xml is written.

delete-attr

Delete the attribute schemas from a service.

Syntax

```
ssoadm delete-attr --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributeschema, -a`	The name of the attribute schema to be removed.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

delete-attr-def-values

Delete the attribute schema default values.

Syntax

```
ssoadm delete-attr-def-values --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--defaultvalues, -e`	The default values to be deleted.

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

delete-sub-cfg

Delete the sub configuration.

Syntax

```
ssoadm delete-sub-cfg --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--subconfigname, -g`	The name of the sub configuration.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`--attributevalues, -a`	The attribute values. For example, `homeaddress=here`.
`--datafile, -D`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.
`--realm, -e`	The name of the realm. The sub configuration will be added to the global configuration if this option is not selected.
`--subconfigid, -b`	The ID of the parent configuration. The sub configuration will be added to the root configuration if this option is not selected.
`--priority, -p`	The priority of the sub configuration.

delete-svc

Delete the service from the server.

Syntax

```
ssoadm delete-svc --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--continue, -c]`	Continue deleting services if one or more previous services can not be deleted.
`[--deletepolicyrule, -r]`	Delete the policy rule.

export-svc-cfg

Export the service configuration.

Syntax

```
ssoadm export-svc-cfg --options [--global-options]
```

Options

`--encryptsecret, -e`	The secret key for encrypting a password.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--outfile, -o]`	The filename where configuration is written.

get-attr-defs

Get the default attribute values in a schema.

Syntax

```
ssoadm get-attr-defs --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.
`[--attributenames, -a]`	The names of the attribute.

get-revision-number

Get the service schema revision number.

Syntax

```
ssoadm get-revision-number --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

import-svc-cfg

Import the service configuration.

Syntax

```
ssoadm import-svc-cfg --options [--global-options]
```

Options

`--encryptsecret, -e`	The secret key for decrypting the password.
`--xmlfile, -X`	The XML file that contains the configuration data.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

remove-attr-choicevals

Remove choice values from the attribute schema.

Syntax

```
ssoadm remove-attr-choicevals --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.

`--attributename, -a`	The name of the attribute.
`--choicevalues, -k`	The choice values. For example, inactive.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

remove-attr-defs

Remove the default attribute values in a schema.

Syntax

```
ssoadm remove-attr-defs --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributenames, -a`	The names of the attribute.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

remove-sub-schema

Remove the sub schema.

Syntax

```
ssoadm remove-sub-schema --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--subschemanames, -a`	The names of the sub schema to be removed.
`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the parent sub schema.

set-attr-any

Set any member of the attribute schema.

Syntax

```
ssoadm set-attr-any --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributeschema, -a`	The name of the attribute schema.
`--any, -y`	The attribute schema. Any value.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

set-attr-bool-values

Set the boolean values of the attribute schema.

Syntax

```
ssoadm set-attr-bool-values --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributename, -a`	The name of the attribute.
`--truevalue, -e`	The value for true.
`--truei18nkey, -k`	The internationalization key for the true value.
`--falsevalue, -z`	The value for false.

`--falsei18nkey, -j`	The internationalization key for the false value.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

set-attr-choicevals

Set choice values for the attribute schema.

Syntax

```
ssoadm set-attr-choicevals --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributename, -a`	The name of the attribute.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--add, -p]`	Set this flag to append the choice values to existing ones.
`[--subschemaname, -c]`	The name of the sub schema.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.
`[--choicevalues, -k]`	The choice values. For example, `0102=Inactive`.

set-attr-defs

Set the default attribute values in a schema.

Syntax

```
ssoadm set-attr-defs --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.

`--schematype, -t`	The type of schema.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

set-attr-end-range

Set the attribute schema end range.

Syntax

```
ssoadm set-attr-end-range --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributeschema, -a`	The name of the attribute schema.
`--range, -r`	The end range.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

set-attr-i18n-key

Set the i18nkey member of the attribute schema.

Syntax

```
ssoadm set-attr-i18n-key --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.

`--schematype, -t`	The type of schema.
`--attributeschema, -a`	The name of the attribute schema.
`--i18nkey, -k`	The attribute schema i18n key.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

set-attr-start-range

Set the attribute schema start range.

Syntax

```
ssoadm set-attr-start-range --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributeschema, -a`	The name of the attribute schema.
`--range, -r`	The start range.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

set-attr-syntax

Set the syntax member of the attribute schema.

Syntax

```
ssoadm set-attr-syntax --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.

`--attributeschema, -a`	The name of the attribute schema.
`--syntax, -x`	The attribute schema syntax.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

set-attr-type

Set the type member of the attribute schema.

Syntax

```
ssoadm set-attr-type --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributeschema, -a`	The name of the attribute schema.
`--type, -p`	The attribute schema type.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

set-attr-ui-type

Set the UI type member of the attribute schema.

Syntax

```
ssoadm set-attr-ui-type --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributeschema, -a`	The name of the attribute schema.

`--uitype, -p`	The attribute schema UI type.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

set-attr-validator

Set the attribute schema validator.

Syntax

```
ssoadm set-attr-validator --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributeschema, -a`	The name of the attribute schema.
`--validator, -r`	The validator class name.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

set-attr-view-bean-url

Set the properties view bean URL member of the attribute schema.

Syntax

```
ssoadm set-attr-view-bean-url --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--attributeschema, -a`	The name of the attribute schema.
`--url, -r`	The attribute schema properties view bean URL.

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--subschemaname, -c]`	The name of the sub schema.

set-inheritance

Set the inheritance value of the sub schema.

Syntax

```
ssoadm set-inheritance --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--schematype, -t`	The type of schema.
`--subschemaname, -c`	The name of the sub schema.
`--inheritance, -r`	The value of inheritance.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

set-plugin-viewbean-url

Set the properties view bean URL of the plug-in schema.

Syntax

```
ssoadm set-plugin-viewbean-url --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--interfacename, -i`	The name of the interface.
`--pluginname, -g`	The name of the plug-in.
`--url, -r`	The properties view bean URL.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

set-revision-number

Set the service schema revision number.

Syntax

```
ssoadm set-revision-number --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--revisionnumber, -r`	The revision number.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

set-sub-cfg

Set the sub configuration.

Syntax

```
ssoadm set-sub-cfg --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--subconfigname, -g`	The name of the sub configuration.
`--operation, -o`	The operation (either add/set/modify) to be performed on the sub configuration.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.
`[--realm, -e]`	The name of the realm. The sub configuration will be added to the global configuration if this option is not selected.

set-svc-i18n-key

Set the service schema i18n key.

Syntax

```
ssoadm set-svc-i18n-key --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--i18nkey, -k`	The i18n key.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

set-svc-view-bean-url

Set the service schema properties view bean URL.

Syntax

```
ssoadm set-svc-view-bean-url --options [--global-options]
```

Options

`--servicename, -s`	The name of the service.
`--url, -r`	The service schema properties view bean URL.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

update-svc

Update the service.

Syntax

```
ssoadm update-svc --options [--global-options]
```

Options

`--xmlfile, -X`	The XML file that contains the schema.

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--continue, -c]`	Continue updating services if one or more previous services can not be updated.

Server Configuration

The following subcommands execute operations for configuring and managing OpenSSO Enterprise servers and sites within your enterprise.

add-site-members

Add members to a site.

Syntax

```
ssoadm add-site-members --options [--global-options]
```

Options

`--sitename, -s`	The name of the site. For example, mysite.
`--servernames, -e`	The server name. For example, `http://www.example.com:8080/opensso`.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

add-site-sec-urls

Add site secondary URLs.

Syntax

```
ssoadm add-site-sec-urls --options [--global-options]
```

Options

`--sitename, -s`	The name of the site. For example, mysite.
`--secondaryurls, -a`	The secondary URLs.
`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.

clone-server

Clone a server instance.

Syntax

```
ssoadm clone-server --options [--global-options]
```

Options

`--servername, -a`	The server name.
`--cloneservername, -o`	The clone server name.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

create-server

Create a server instance.

Syntax

```
ssoadm create-server --options [--global-options]
```

Options

`--servername, -a`	The server name. For example, `http://www.example.com:8080/opensso`.
`--serverconfigxml, -X`	The server configuration XML filename.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

create-site

Create a site.

Syntax

```
ssoadm create-site --options [--global-options]
```

Options

`--sitename, -s`	The site name. For example, mysite.
`--siteurl, -i`	The site's primary URL. For example, `http://www.example.com:8080`.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--secondaryurls, -a]`	The secondary URLs.

delete-server

Delete a server instance.

Syntax

```
ssoadm delete-server --options [--global-options]
```

Options

`--servername, -s`	The server name. For example, `http://www.example.com:8080/opensso`.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

delete-site

Delete a site.

Syntax

```
ssoadm delete-site --options [--global-options]
```

Options

`--sitename, -s`	The site name. For example, mysite.
`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.

export-server

Export a server instance.

Syntax

```
ssoadm export-server --options [--global-options]
```

Options

`--servername, -s`	The server name. For example, `http://www.example.com:8080/opensso`.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--outfile, -o]`	The filename where configuration is written.

get-svrcfg-xml

Get the server configuration XML from the centralized data store.

Syntax

```
ssoadm get-svrcfg-xml --options [--global-options]
```

Options

`--servername, -s`	The server name.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--outfile, -o]`	The filename where serverconfig.XML is written.

import-server

Import a server instance.

Syntax

```
ssoadm import-server --options [--global-options]
```

Options

`--servername, -s`	The server name.
`--xmlfile, -X`	The XML file that contains the configuration.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

list-server-cfg

List the server configuration.

Syntax

```
ssoadm list-server-cfg --options [--global-options]
```

Options

`--servername, -s`	The server name.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--withdefaults, -w]`	Set this flag to get the default configuration.

list-servers

List all the server instances.

Syntax

```
ssoadm list-servers --options [--global-options]
```

Options

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

list-sites

List all the sites.

Syntax

```
ssoadm list-sites --options [--global-options]
```

Options

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

remove-server-cfg

Remove the server configuration.

Syntax

```
ssoadm remove-server-cfg --options [--global-options]
```

Options

`--servername, -s`	The server name. For example, `http://www.example.com:8080/opensso`.
`--propertynames, -a`	The names of the properties to be removed.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

remove-site-members

Remove members from a site.

Syntax

```
ssoadm remove-site-members --options [--global-options]
```

Options

`--sitename, -s`	The site name. For example, mysite.
`--servernames, -e`	The server name. For example, `http://www.example.com:8080/opensso`.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

remove-site-sec-urls

Remove the site secondary URLs.

Syntax

```
ssoadm remove-site-sec-urls --options [--global-options]
```

Options

`--sitename, -s`	The site name. For example, mysite.
`--secondaryurls, -a`	The secondary URLs.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

set-site-pri-url

Set the primary URL of a site.

Syntax

```
ssoadm set-site-pri-url --options [--global-options]
```

Options

`--sitename, -s`	The site name. For example, mysite.
`--siteurl, -i`	The site's primary URL. For example, `http://www.example.com:8080`.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

set-site-sec-urls

Set the site secondary URLs.

Syntax

```
ssoadm set-site-sec-urls --options [--global-options]
```

Options

`--sitename, -s`	The site name. For example, mysite.
`--secondaryurls, -a`	The secondary URLs.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

set-svrcfg-xml

Set the server configuration XML to the centralized data store.

Syntax

```
ssoadm set-svrcfg-xml --options [--global-options]
```

Options

`--servername, -s`	The server name.
`--xmlfile, -X`	The XML file that contains the configuration.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--outfile, -o]`	The filename where serverconfig XML is written.

show-site

Show the site profile.

Syntax

```
ssoadm show-site --options [--global-options]
```

Options

`--sitename, -s`	The site name. For example, mysite.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

show-site-members

Display the members of a site.

Syntax

```
ssoadm show-site-members --options [--global-options]
```

Options

`--sitename, -s`	The site name. For example, mysite.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

update-server-cfg

Update the server configuration.

Syntax

```
ssoadm update-server-cfg --options [--global-options]
```

Options

`--servername, -s`	The server name.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--attributevalues, -a]`	The attribute values. For example, `homeaddress=here`.
`[--datafile, -D]`	Name of file that contains attributes and corresponding values as in *attribute-name=attribute-value*. Enter one attribute and value per line.

Federation Management

The following subcommands execute operations for configuring and managing Federation-related data.

add-cot-member

Add a member to a circle of trust.

Syntax

```
ssoadm add-cot-member --options [--global-options]
```

Options

`--cot, -t`	The circle of trust.
`--entityid, -y`	The entity ID.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--realm, -e]`	The name of the realm that contains the circle of trust.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is `saml2`.

create-cot

Create a circle of trust.

Syntax

```
ssoadm create-cot --options [--global-options]
```

Options

`--cot, -t`	The circle of trust.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--realm, -e]`	The name of the realm that contains the circle of trust.
`[--trustedproviders, -k]`	The trusted providers.
`[--prefix, -p]`	The prefix URL for the idp discovery reader and the writer URL.

create-metadata-templ

Create a new metadata template.

Syntax

```
ssoadm create-metadata-templ --options [--global-options]
```

Options

`--entityid, -y`	The entity ID.

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--meta-data-file, -m]`	Specifies the filename for the standard metadata to be created.
`[--extended-data-file, -x]`	Specifies the filename for the extended metadata to be created.
`[--serviceprovider, -s]`	Specifies the metaAlias for the hosted service provider to be created. The format must be `<realm name>/`.
`[--identityprovider, -i]`	Specifies the metaAlias for the hosted identity provider to be created. The format must be `<realm name>/`.
`[--attrqueryprovider, -S]`	Specifies the metaAlias for the hosted attribute query provider to be created. The format must be `<realm name>/`.
`[--attrauthority, -I]`	Specifies the metaAlias for the hosted attribute authority to be created. The format must be `<realm name>/`.
`[--authnauthority, -C]`	Specifies the metaAlias for the hosted authentication authority to be created. The format must be `<realm name>/`.
`[--xacmlpep, -e]`	Specifies the metaAlias for the policy enforcement point to be created. The format must be `<realm name>/`.
`[--xacmlpdp, -p]`	Specifies the metaAlias for the policy decision point to be created. The format must be `<realm name>/`.
`[--affiliation, -F]`	Specifies the metaAlias for the hosted affiliation to be created. The format must be `<realm name>/<identifier`.
`[--affiownerid, -N]`	The affiliation owner ID.
`[--affimembers, -M]`	The affiliation members.
`[--spscertalias, -a]`	The service provider signing certificate alias.
`[--idpscertalias, -b]`	The identity provider signing certificate alias.
`[--attrqscertalias, -A]`	The attribute query provider signing certificate alias.
`[--attrascertalias, -B]`	The attribute authority signing certificate alias.
`[--authnascertalias, -D]`	The authentication authority signing certificate alias.
`[--affiscertalias, -J]`	The affiliation signing certificate alias.
`[--xacmlpdpscertalias, -t]`	The policy decision point signing certificate alias.

`[--xacmlpepscertalias, -k]`	The policy enforcement point signing certificate alias.
`[--specertalias, -r]`	The service provider encryption certificate alias.
`[--idpecertalias, -g]`	The identity provider encryption certificate alias.
`[--attrqecertalias, -R]`	The attribute query provider encryption certificate alias.
`[--attraecertalias, -G]`	The attribute authority encryption certificate alias.
`[--authnaecertalias, -E]`	The authentication authority encryption certificate alias.
`[--affiecertalias, -K]`	The affiliation encryption certificate alias.
`[--xacmlpdpecertalias, -j]`	The policy decision point encryption certificate alias.
`[--xacmlpepecertalias, -z]`	The policy enforcement point encryption certificate alias.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is`saml2`.

delete-cot

Delete the circle of trust.

Syntax

```
ssoadm delete-cot --options [--global-options]
```

Options

`--cot, -t`	The circle of trust.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--realm, -e]`	The name of the realm that contains the circle of trust.

delete-entity

Delete an entity.

Syntax

```
ssoadm delete-entity --options [--global-options]
```

Options

`--entityid, -y`	The entity ID.

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--realm, -e]`	The name of the realm that contains the circle of trust.
`[--extendedonly, -x]`	Set this flag to only delete extended data.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is `saml2`.

do-bulk-federation

Perform bulk federation.

Syntax

```
ssoadm do-bulk-federation --options [--global-options]
```

Options

`--metaalias, -m`	Specify a metaAlias for the local provider.
`--remoteentityid, -r`	The remote entity ID.
`--useridmapping, -g`	The filename that contains the local to remote user ID mapping. Format as follows: `<local-user-id>|<remote-user-id>`.
`--nameidmapping, -e`	The filename that will be created by this sub command. It contains remote the user ID to name the identifier.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is `saml2`.

export-entity

Export an entity.

Syntax

```
ssoadm export-entity --options [--global-options]
```

Options

`--entityid, -y`	The entity ID.

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--realm, -e]`	The name of the realm to which the entity belongs.
`[--sign, -g]`	Set this flag to sign the metadata.
`[--meta-data-file, -m]`	The metadata.
`[--extended-data-file, -x]`	The extended data.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is `saml2`.

import-bulk-fed-data

Import the bulk federation data that is generated by the `do-bulk-federation` sub command.

Syntax

```
ssoadm import-bulk-fed-data --options [--global-options]
```

Options

`--metaalias, -m`	Specifies the metaAlias for the local provider.
`--bulk-data-file, -g`	The filename that contains the bulk federation data that is generated by the `do-bulk-federation` sub command.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is`saml2`.

import-entity

Import an entity.

Syntax

```
ssoadm import-entity --options [--global-options]
```

Options

`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.
`[--realm, -e]`	The name of the realm to which the entity belongs.
`[--meta-data-file, -m]`	Specifies the filename for the standard metadata to be imported.
`[--extended-data-file, -x]`	Specifies the filename for the extended entity configuration to be imported.
`[--cot, -t]`	The circle of trust.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is`saml2`.

list-cot-members

List the members in a circle of trust.

Syntax

```
ssoadm list-cot-members --options [--global-options]
```

Options

`--cot, -t`	The circle of trust.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--realm, -e]`	The name of the realm to which the circle of trust belongs.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is`saml2`.

list-cots

List the circles of trust.

Syntax

```
ssoadm list-cots --options [--global-options]
```

Options

`--adminid, -u`	The administrator ID running the command.

`--password-file, -f`	The filename that contains the password of the administrator.
`[--realm, -e]`	The name of the realm to which the circle of trust belongs.

list-entities

List the entities under a realm.

Syntax

```
ssoadm list-entities --options [--global-options]
```

Options

`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--realm, -e]`	The name of the realm to which the entities belong.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is`saml2`.

remove-cot-member

Remove a member from a circle of trust.

Syntax

```
ssoadm remove-cot-member --options [--global-options]
```

Options

`--cot, -t`	The circle of trust.
`--entityid, -y`	The entity ID.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--realm, -e]`	The name of the realm to which the circle of trust belongs.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is`saml2`.

update-entity-keyinfo

Update the XML signing and encryption key information in the hosted entity metadata.

Syntax

```
ssoadm update-entity-keyinfo --options [--global-options]
```

Options

`--entityid, -y`	The entity ID.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--spscertalias, -a]`	The service provider signing certificate alias.
`[--idpscertalias, -b]`	The identity provider signing certificate alias.
`[--specertalias, -r]`	The service provider encryption certificate alias.
`[--idpecertalias, -g]`	The identity provider encryption certificate alias.
`[--spec, -c]`	Specifies the metadata specification, either `idff` or `saml2`. The default is`saml2`.

Miscellaneous

Lists the agent configurations.

add-res-bundle

Add a resource bundle to the data store.

Syntax

```
ssoadm add-res-bundle --options [--global-options]
```

Options

`--bundlename, -b`	The resource bundle name.
`--bundlefilename, -B`	The resource bundle physical file name.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

`[--bundlelocale, -o]`	The locale of the resource bundle.

do-batch

Do multiple requests in one command.

Syntax

```
ssoadm do-batch --options [--global-options]
```

Options

`--batchfile, -D`	The filename that contains the commands and options.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--batchstatus, -b]`	The name of the status file.
`[--continue, -c]`	Continue processing the rest of the request when the previous request was erroneous.

do-migration70

Migrate the organization to a realm.

Syntax

```
ssoadm do-migration70 --options [--global-options]
```

Options

`--entrydn, -e`	The distinguished name of the organization to be migrated.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.

list-res-bundle

List a resource bundle in a data store.

Syntax

```
ssoadm list-res-bundle --options [--global-options]
```

Options

`--bundlename, -b`	The resource bundle name.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--bundlelocale, -o]`	The locale of the resource bundle.

list-sessions

List the sessions.

Syntax

```
ssoadm list-sessions --options [--global-options]
```

Options

`--host, -t`	The host name.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`--filter, -x`	Filter by a pattern.
`[--quiet, -q]`	Do not prompt for session invalidation.

remove-res-bundle

Remove a resource bundle from a data store.

Syntax

```
ssoadm remove-res-bundle --options [--global-options]
```

Options

`--bundlename, -b`	The resource bundle name.
`--adminid, -u`	The administrator ID running the command.
`--password-file, -f`	The filename that contains the password of the administrator.
`[--bundlelocale, -o]`	The locale of the resource bundle.

◆ ◆ ◆ CHAPTER 2

The amadmin Command Line Tool

Note – In the 8.0 release, the amadmin command line tool has been replaced by the `ssoadm` command line utility. This section is provided as reference for backwards compatibility for upgraded systems.

This chapter provides information on the `amadmin` command line tool.

The amadmin Command Line Executable

The primary purposes of the command line executable `amadmin` is to load XML service files into the data store and to perform batch administrative tasks on the DIT. It is used to:

- Load XML service files - Administrators load services into OpenSSO Enterprise that use the XML service file format defined in the `sms.dtd`. All services must be loaded using `amadmin`; they cannot be imported through the OpenSSO Enterprise console.

Note – XML service files are stored in the data store as static *blobs* of XML data that is referenced by OpenSSO Enterprise. This information is not used by Directory Server, which only understands LDAP.

- Perform batch updates of identity objects to the DIT - Administrators can perform batch updates to the Directory Server DIT using the batch processing XML file format defined in the `amadmin.dtd`. For example, if an administrator wants to create 10 organizations, 1000 users, and 100 groups, it can be done in one attempt by putting the requests in one or more batch processing XML files and loading them using `amadmin`.

Note – `amadmin` only supports a subset of features that the OpenSSO Enterprise console supports and is not intended as a replacement. It is recommended that the console be used for small administrative tasks while `amadmin` is used for larger administrative tasks.

If there is an environment variable named OPTIONS on the system, you must remove it. This command line utility will not function properly with this environment variable.

The amadmin Syntax

There are a number of structural rules that must be followed in order to use `amadmin`. The generic syntaxes for using the tool are:

- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d |--debug]] -t | --data` *xmlfile1* `[` *xmlfile2* `...]`
- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d | --debug]] -s | --schema` *xmlfile1* `[`*xmlfile2* `...]`
- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d | --debug]] -r | --deleteService` *serviceName1* `[`*serviceName2* `...]`
- amadmin -u | --runasdn *dnname* -w | --password *password* or -f | --passwordfile *passwordfile* [-c | --continue] [-l | --locale *localename*] [[-v | --verbose] | [-d | --debug]] -m | --session *servername pattern*
- `amadmin -h | --help`
- `amadmin -n | --version`
- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `or - f |--passwordfile` *passwordfile* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d] |--debug]] -a |--addattributes` *serviceName schemaType xmlfile*`[`*xmlfile2* `] ...`

Note – Two hyphens must be entered exactly as shown in the syntax.

amadmin Options

Following are definitions of the `amadmin` command line parameter options:

--runasdn (-u)

`--runasdn` is used to authenticate the user to the LDAP server. The argument is a value equal to that of the Distinguished Name (DN) of the user authorized to run `amadmin`; for example

`--runasdn uid=amAdmin,ou=People,o=example.com,o=isp .`

The DN can also be formatted by inserting spaces between the domain components and double quoting the entire DN such as: `--runasdn "uid=amAdmin, ou=People, o=iplanet.com, o=isp"`.

--password (-w)

`--password` is a mandatory option and takes a value equal to that of the password of the DN specified with the `--runasdn` option.

--locale (-l)

`--locale` is an option that takes a value equal to that of the name of the locale. This option can be used for the customization of the message language. If not provided, the default locale, `en_US`, is used.

--continue (-c)

--continue is an option that will continue to process the next request within an XML file even if there are errors. For example, if a request within an XML file fails, then amadmin will continue to the next request in the same XML file. When all operations in the first XML file are completed, amadmin will continue to the second XML file.

--session (-m)

`--session` (`-m`) is an option to manage the sessions, or to display the current sessions. When specifying `--runasdn` , it must be the same as the DN for the super user in `AMConfig.properties` , or just ID for the top-level admin user.

The following example will display all sessions for a particular service host name,:

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com
-v  -w 12345678 -m http://sun.com:58080
```

The following example will display a particular user's session:

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com -v
 -w 12345678 -m http://sun.com:58080 username
```

You can terminate a session by entering the corresponding index number, or enter multiple index numbers (with spaces) to terminate multiple sessions.

While using the following option:

`amadmin -m | --session` servername pattern

The pattern may be a wildcard (*). If this pattern is using a wildcard (*), it has to be escaped with a meta character (\\) from the shell.

--debug (-d)

`--debug` is an option that will write messages to the `amAdmin` file created under the `/var/opt/SUNWam/debug` directory. These messages are technically-detailed but not i18n-compliant. To generate `amadmin` operation logs, when logging to database, the classpath for the database driver needs to be added manually. For example, add the following lines when logging to `mysql` in `amadmin`:

```
CLASSPATH=$CLASSPATH:/opt/IS61/SUNWam/lib/mysql-connector-java-3.0.6-stable-bin.jar
export CLASSPATH
```

--verbose (-v)

`--verbose` is an option that prints to the screen the overall progress of the `amadmin` command. It does not print to a file the detailed information. Messages output to the command line are i18n- compliant.

--data (-t)

`--data` is an option that takes as its value the name of the batch processing XML file being imported. One or more XML files can be specified. This XML file can create, delete and read various directory objects as well as register and unregister services. .

--schema (-s)

`--schema` is an option that loads the attributes of an OpenSSO Enterprise service into the Directory Server. It takes as an argument an XML service file in which the service attributes are defined. This XML service file is based on the `sms.dtd` . One or more XML files can be specified.

Note – Either the `--data` or `--schema` option must be specified, depending on whether configuring batch updates to the DIT, or loading service schema and configuration data.

--addattributes (-a)

Adds a new attribute to the specified serviceName and schemaType(global, dynamic, organization, or user). The attribute schema being added is defined in the XML file.

--deleteservice (-r)

`--deleteservice` is an option for deleting a service and its schema only.

--serviceName

`--serviceName` is an option that takes a value equal to the service name which is defined under the `Service name=...` tag of an XML service file. This portion is displayed in `--–servicename`.

EXAMPLE 2–1 Portion of `sampleMailService.xml`

```
...
<ServicesConfiguration>
    <Service name="sampleMailService" version="1.0">
        <Schema
 serviceHierarchy="/other.configuration/sampleMailService"
            i18nFileName="sampleMailService"
            i18nKey="iplanet-am-sample-mail-service-description">
...
```

--help (-h)

`--help` is an argument that displays the syntax for the `amadmin` command.

--version (-n)

`--version` is an argument that displays the utility name, product name, product version and legal notice.

Using amadmin for Federation Management

This section lists the parameters of amadmin for use with Federation Management.

Loading the Liberty meta compliance XML into Directory Server

```
amadmin -u|--runasdn <user's DN>
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-g|--import <xmlfile>
```

--runasdn (-u)

The user's DN

--password (-w)

The user's password.

--passwordfile (-f)

The name of file that contains user's password. This file is not encrypted and should be protected as a read-only file owned by the web container runtime user (which may not necessarily be root). The default owner is root but it is not required to be. . Any encryption method you use must be managed outside of `amadmin`.

--entityname (-e)

The entity name. For example, `http://www.example.com`. An entity should belong to only one organization.

--import (-g)

The name of an XML file that contains the meta information. This file should adhere to Liberty meta specification and XSD.

Exporting an Entity to an XML File (Without XML Digital Signing)

```
amadmin -u|--runasdn <user's DN>

-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-o|--export <filename>
```

--runasdn (-u)

The user's DN

--password (-w)

The user's password.

--passwordfile (-f)

The name of file that contains user's password.

--entityname (--e)

The name of Entity that resides in the Directory Server

--export (-o)

The name of the file to contain the XML of the entity. The XML file must be Liberty meta XSD-compliant.

Exporting an Entity to an XML File (With XML Digital Signing)

```
amadmin -u|--runasdn <user's DN>
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name> -x|--xmlsig -o|--export <filename>
```

--runasdn (-u)

The user's DN

--password (-w)

The user's password.

--passwordfile (-f)

The name of file that contains user's password.

--entityname (--e)

The name of Entity that resides in the Directory Server

--export (-o)

The name of the file to contain the XML of the entity. The XML file must be Liberty meta XSD-compliant.

--xmlsig (-x)

Used in with the `--export` option and if specified, the exported file will be signed

Changing from Legacy Mode to Realm Mode

If you install OpenSSO Enterprise in Legacy Mode, you can change to Realm Mode by using the amadmin command with the `-M` option. For example:

```
amadmin -u cn=amAdmin,ou=People,dc=example,dc=com -w amadmin-password -M
dc=example,dc=com
```

Caution – If you install OpenSSO Enterprise 8.0 in Realm Mode, you cannot revert to Legacy Mode.

Using amadmin for Resource Bundles

The following section shows the `amadmin` syntax for adding, locating and removing resource bundles.

Add resource bundle.

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-b|--addresourcebundle <name-of-resource-bundle>

-i|--resourcebundlefilename <resource-bundle-file-name>
```

```
[-R|--resourcelocale] <locale>
```

Get resource strings.

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-z|--getresourcestrings <name-of-resource-bundle>

[-R|--resourcelocale] <locale>
```

Remove resource bundle.

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-j|--deleteresourcebundle <name-of-resource-bundle>

[-R|--resourcelocale] <locale>
```

◆ ◆ ◆ CHAPTER 3

The ampassword Command Line Tool

This chapter provides information on the `amPassword` command line too.

The ampassword Command Line Executable

OpenSSO Enterprise contains an `ampassword` utility in your server's tools directory. For information on unpacking and setting up this utility, see Chapter 6, "Installing the OpenSSO Enterprise Utilities and Scripts," in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*. This tool allows you change the Directory Server password for the administrator or user.

▼ To Run ampassword with OpenSSO Enterprise in SSL mode

1 **Use the `ssoadm get-svrcfg-xml` command to retrieve the serverconfig.xml file.**

2 **Edit this file to change the protocol of the directory server**

For example:

```
<iPlanetDataAccessLayer>
<ServerGroup name="default" minConnPool="1" maxConnPool="10">
    <Server name="Server1" host="sun.com" port="636" type="SSL" />
    <User name="User1" type="proxy">
        <DirDN>
                cn=puser,ou=DSAME Users,dc=iplanet,dc=com
        </DirDN>
        <DirPassword>
                 AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
         </DirPassword>
 </User> ...
```

You can also edit Directory Server configuration data in the Servers and Sites tab in the OpenSSO console. For more information, see "Servers and Sites" on page 258.

3 **Import the edited serverconfig.xml file using** `ssoadm set-svrcfg-xml`

`ampassword` only changes the password in Directory Server. You will have to manually change passwords and all authentication templates for OpenSSO Enterprise.

◆ ◆ ◆ CHAPTER 4

The amverifyarchive Command Line Tool

This chapter provides information on the `amverifyarchive` command line tool and contains the following section:

The amverifyarchive Command Line Executable

The purpose of `amverifyarchive` is to verify the log archives. A log archive is a set of timestamped logs and their corresponding key stores (keystores contain the keys used to generate the MACs and the Digital Signatures which are used to detect tampering of the log files). Verification of an archive detects possible tampering and/or deletion of any file in the archive.

`amverifyarchive` extracts all of the archive sets, and all files belonging to each archive set, for a given `logName`. When executed, `amverifyarchive` searches each log record to for tampering If tampering is detected, it prints a message specifying which file and the number of the record that has been tampered with.

`amverifyarchive` also checks for any files that have been deleted from the archive set. If a deleted file is detected, it prints a message explaining that verification has failed. If no tampering or deleted files are detected, it returns a message explaining that the archive verification has been successfully completed.

Note – An error may occur if you run `amamverifyarchive` as a user without administrator privileges.

---

amverifyarchive Syntax

All of the parameters options are required. The syntax is as follows:

```
amamverifyarchive -l logName -p path -u
uname -w password
```

amverifyarchive Options

logName

`logName` refers to the name of the log which is to be verified (such as, `amConsole`, `amAuthentication` and so forth). `amverifyarchive` verifies the both the access and error logs for the given logName. For example, if `amConsole` is specified, the verifier verifies the `amConsole.access` and `amConsole.error` files. Alternatively, the `logName` can be specified as `amConsole.access` or `amConsole.error` to restrict the verification of those logs only.

path

`path` is the full directory path where the log files are stored.

uname

`uname` is the user id of the OpenSSO Enterprise administrator.

password

`password` is the password of the OpenSSO Enterprise administrator.

PART II

OpenSSO Attribute Reference

This section of the OpenSSO Enterprise 8.0 Administration Reference lists and describe the configurable attributes for entities and services in the OpenSSO Enterprise console. In previous releases, many of these attributes were only configurable through the `AMConfig.properties` file. This file has been deprecated, and all of its properties are now defined in the OpenSSO Enterprise console and stored in the configuration directory datastore.

◆ ◆ ◆ CHAPTER 5

Centralized Agent Configuration Attributes

The Centralized Agent Configuration provides an agent administrator with a means to manage multiple agent configurations from one central place. The agent configurations are stored in OpenSSO Enterprise's data repository and managed by an administrator via the OpenSSO Enterprise Console.

Agent Configuration Attributes

Once you have created an agent, you can customize each agent's behavior. To do so, first click the name of the agent you wish to configure, and then modify the agent's attributes. See the following sections for definitions for each agent type:

Web Policy Agent

A web agent instance can be configured using this interface. The properties described only apply if during agent creation, centralized configuration was chosen. If local configuration was selected, the properties related to this agent must be edited in the `OpenSSOAgentConfiguration.properites` file in the agent installation directory.

For definitions of the Web Policy Agent attributes, see the *Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide for Web Agents*, or the online help.

J2EE Policy Agent

A J2EE agent instance can be configured using this interface. The properties described only apply if during agent creation, centralized configuration was chosen. If local configuration was selected, the properties related to this agent must be edited in the `OpenSSOAgentConfiguration.properites` file in the agent installation directory.

For definitions of the J2EE Policy Agent attributes, see the *Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide for J2EE Agents*, or the online help.

Web Service Provider

The Web Service Provider agent profile describes the configuration that is used for validating web service requests from web service clients and securing web service responses from a web service provider. The name of the web service provider must be unique across all agents.

General

The following General attributes define basic web service provider properties:

Group

The Group mechanism allows you to define a collection of similar types of agents. The group must be defined before including the particular agent into a collection.

Password

Defines the password for the web service provider agent

Password Confirm

Confirm the password.

Status

Defines whether the web service provider agent will be Active or Inactive in the system. By default, it is set to Active, meaning that the agent will participate in validating web service requests from web service clients and securing service responses from a web service provider.

Universal Identifier

Lists the basic LDAP properties, that uniquely defines the web service provider agent.

Security

The following attributes define web service provider security attributes:

Security Mechanism

Defines the type of security credential that are used to validate the web service request. The type of security mechanism is part of the web service request from a web service client and is accepted by a web service provider. Choose from the following types:

- Anonymous — The anonymous security mechanism contains no security credentials.
- KerberosToken — Uses Kerberos security tokens.
- LibertyBearerToken – Uses the Liberty-defined bearer token.
- LibertySAMLToken – Uses the Liberty-defined SAML token.
- LibertyX509Token – Uses the Liberty-defined X509 certificate.
- SAML-HolderOfKey - Uses the SAML 1.1 assertion type Holder-Of-Key..
- SAML-SenderVouches - Uses the SAML 1.1 assertion type Sender Vouches.
- SAML2–HolderOfKey – Uses the SAML 2.0 assertion token type Holder-Of-Key.
- SAML2–SenderVouches – Uses the SAML 2.0 assertion token type Sender Vouches.
- UserNameToken – Uses a user name token.
- UserNameToken-Plain – Uses a user name token with a clear text password.
- X509Token – Uses the X509 certificate.

Authentication Chain

Defines the authentication chain or service name that can be used to authenticate to the OpenSSO Enterprise authentication service using the credentials from an incoming web service request's security token to generate OpenSSO Enterprise's authenticated SSOToken.

Token Conversion Type

Defines the type of token that will be converted when a web service provider requests a token conversion from the Security Token service. The token is converted to the specified SAML or SSOToken (session token) with the same identity, but with attribute definitions specific to the token type. This new token can be used by the web service provider making a web service call to another web service provider. The token types you can define are:

- SAML 1.1 token
- SAML2 token
- SSOToken

In order to use this attribute, any SAML token must be selected in the Security Mechanism attribute and any authentication chain defined for the web service provider.

Preserve Security Headers in Message

When enabled, this attribute defines that the SOAP security headers are preserved by the web service provider for further processing.

Private Key Type

Defines the key type used by the web service provider during the web service request signature verification process. The default value is `PublicKey`.

Liberty Service Type URN

The URN (Universal Resource Name) describes a Liberty service type that the web service provider will use for service lookups.

Credential for User Token

This attribute represents the username/password shared secrets that are used by the web service provider to validate a username security token from an incoming web service request. These credentials are compared against the credentials from the username security token from an incoming web service request.

SAML Configuration

The following attributes configure the Security Assertion Markup Language (SAML) for the web service provider:

SAML Attribute Mapping

This configuration represents a SAML attribute that needs to be generated as an Attribute Statement during SAML assertion creation by the Security Token Service for a web service provider. The format is *SAML_attr_name*=*Real_attr_name*.

SAML_attr_name is the SAML attribute name from a SAML assertion from an incoming web service request. *Real_attr_name* is the attribute name that is fetched from either the authenticated SSOToken or the identity repository.

SAML NameID Mapper Plugin

Defines the NameID mapper plug-in class that is used for SAML account mapping.

SAML Attributes Namespace

Defines the name space used for generating SAML attributes.

Include Memberships

If enabled, this attribute defines that the principal's membership must be included as a SAML attribute.

Signing and Encryption

The following attributes define signing and encryption configuration for web provider security:

Is Response Signed

When enabled, the web service provider signs the response using its X509 certificate.

Is Response Encrypted

When enabled, the web service response will be encrypted.

Is Request Signature Verified

When enabled, the web service request signature is verified.

Is Request Header Decrypted

When enabled, the web service client request's security header will be decrypted.

Is Request Decrypted

When enabled, the web service client request will be decrypted.

Signing Reference Type

Defines the reference types used when the Security Token service signs the wsp response. The possible reference types are `DircectReference`, `KeyIdentifier`, and `X509`.

Encryption Algorithm

Defines the encryption algorithm used to encrypt the web service response.

Encryption Strength

Sets the encryption strength used by he Security Token service to encrypt the web service response. Select a greater value for greater encryption strength.

Key Store

The following attributes configure the keystore to be used for certificate storage and retrieval:

Public Key Alias of Web Service Client

This attribute defines the public certificate key alias that is sued to encrypt the web service response or verify the signature of the web service request.

Private Key Alias

This attribute defines the private certificate key alias that is used to sign the web service response or decrypt the web service request.

Key Storage Usage

This configuration defines whether to use the default keystore, or a custom keystore. The following values must be defined for a custom key store:

- Location of Key Store
- Password of Key Store
- Password of Key

End Points

The following attributes define web service endpoints:

Web Service Proxy End Point

This attribute defines a web service end point to which the web service client is making a request. The end point is optional unless it is configured to use web security proxy.

Web Service End Point

This attribute defines a web service end point to which the web service client is making a request.

Kerberos Configuration

Kerberos is a security profile supported by the web services security to secure web services communications between a web service client and a web service provider. In a typical scenario, a user authenticates to the desktop and invokes a web service and the web service client. This requires a Kerberos ticket to secure the request to web service provider by identifying his principal as Kerberos token. Typically, Kerberos-based web services security is used in same the context of Kerberos domain (realm) as opposed to across boundaries, for example SAML-based web services security. However, Kerberos is one of the strongest authentication mechanisms, especially in the Windows Domain Controller environment.

Kerberos Domain Server

This attribute specifies the Kerberos Distribution Center (the domain controller) hostname. You must enter the fully qualified domain name (FQDN) of the domain controller.

Kerberos Domain

This attribute specifies the Kerberos Distribution Center (domain controller) domain name. Depending up on your configuration, the domain name of the domain controller may be different than the OpenSSO Enterprise domain name.

Kerberos Service Principal

Specifies the Kerberos principal as the owner of the generated Security token.

Use the following format:

`HTTP/hostname.domainname@dc_domain_name`

`hostname` and `domainame` represent the hostname and domain name of the OpenSSO Enterprise instance. `dc_domain_name` is the Kerberos domain in which the Windows Kerberos server (domain controller) resides. It is possible that the Kerberos server is different from the domain name of the OpenSSO Enterprise instance.

Kerberos Key Tab File

This attribute specifies the Kerberos keytab file that is used for issuing the token. Use the following format, although the format is not required:

`hostname.HTTP.keytab`

`hostname` is the hostname of the OpenSSO Enterprise instance.

Verify Kerberos Signature

If enabled, this attribute specifies that the Kerberos token is signed.

Web Service Client Attributes

The Web Service Client agent profile describes the configuration that is used for securing outbound web service requests from a web service client. The name of the web service client must be unique across all agents.

General

The following General attributes define basic web service client properties:

Group

The Group mechanism allows you to define a collection of similar types of agents. The group must be defined before including the particular agent into a collection.

Password

Defines the password for the web service client agent.

Password Confirm

Confirm the password.

Status

Defines whether the web service client agent will be active or inactive in the system. By default, this attribute is set to active, meaning that the agent will participate in securing outbound web service requests from web service clients and will validate web service responses from a web service provider.

Universal Identifier

Lists the basic LDAP properties, that uniquely defines the web service client agent.

Security

The following attributes define web service client security attributes:

Security Mechanism

Defines the type of security credential that is used to secure the web service client request. You can choose one of the following security credential types:

- Anonymous — The anonymous security mechanism contains no security credentials.
- KerberosToken — Uses Kerberos security tokens.
- LibertyDiscoverySecurity — Uses Liberty-based security tokens.
- SAML-HolderOfKey — Uses the SAML 1.1 assertion type Holder-Of-Key.
- SAML-SenderVouches — Uses the SAML 1.1 assertion type Sender Vouches.
- SAML2–HolderOfKey — Uses the SAML 2.0 assertion token type Holder-Of-Key.
- SAML2–SenderVouches — Uses the SAML 2.0 assertion token type Sender Vouches.
- STSSecurity — Uses the security token generated from the Security Token service for a given web service provider.
- UserNameToken — Uses User Name Token with digest password.
- UserNameToken-Plain — Uses a user name token with a clear text password for securing web service requests.
- X509Token — Uses the X509 certificate.

STS Configuration

This attribute is enabled when the web service client uses Security Token service (STS) as the Security Mechanism. This configuration describes a list of STS agent profiles that are used to communicate with and secure the web service requests to the STS service.

Discovery Configuration

This attribute is enabled when the web service client is enabled for Discovery Service security. This configuration describes a list of Discovery Agent profiles that are used to secure requests made to the Discovery service.

User Authentication Required

When enabled, this attribute defines that the services client's protected page requires a user to be authenticated in order to gain access.

Preserve Security Headers in Message

When enabled, this attribute defines that the SOAP security headers are preserved by the web service client for further processing.

Use Pass Through Security Token

When enabled, this attribute indicates that the web service client will pass through the received Security token from the Subject. It will not try to create the token locally or from STS communication.

Liberty Service Type URN

The URN (Universal Resource Name) describes a Liberty service type that the web service client will use for service lookups.

Credential for User Token

The attribute represents the username/password shared secrets that are used by the web service client to generate a Username security token.

Signing and Encryption

The following attributes define signing and encryption configuration for web service security:

Is Request Signed

When enabled, the web services client signs the request using a given token type.

Is Request Header Encrypted

When enabled, the web services client security header will be encrypted.

Is Request Encrypted

When enabled, the web services client request will be encrypted.

Is Response Signature Verified

When enabled, the web services response signature is verified.

Is Response Decrypted

When enabled, the web services response will be decrypted.

Signing Reference Type

Defines the reference types used when the Security Token service signs the WSC response. The possible reference types are `DircectReference`, `KeyIdentifier`, and `X509`.

Encryption Algorithm

Defines the encryption algorithm used to encrypt the web service response.

Encryption Strength

Sets the encryption strength used by he Security Token service to encrypt the web service response. Select a greater value for greater encryption strength.

Key Store

The following attributes configure the keystore to be used for certificate storage and retrieval:

Public Key Alias of Web Service Provider

This attribute defines the public certificate key alias that is used to encrypt the web service request or verify the signature of the web service response.

Private Key Alias

This attribute defines the private certificate key alias that is used to sign the web service request or decrypt the web service response.

Key Storage Usage

This configuration defines whether to use the default keystore, or a custom keystore. The following values must be defined for a custom key store:

- Location of Key Store
- Password of Key Store
- Password of Key

End Points

The following attributes define web service endpoints:

Web Service Security Proxy End Point

This attribute defines a web service end point to which the web service client is making a request. This end point is optional unless it is configured as a web security proxy.

Web Service End Point

This attribute defines a web service end point to which the web service client is making a request.

Kerberos Configuration

Kerberos is a security profile supported by the web services security to secure web services communications between a web service client and a web service provider. In a typical scenario, a user authenticates to the desktop and invokes a web service and the web service client. This requires a Kerberos ticket to secure the request to web service provider by identifying his principal as Kerberos token. Typically, Kerberos-based web services security is used in same the context of Kerberos domain (realm) as opposed to across boundaries, for example SAML-based web services security. However, Kerberos is one of the strongest authentication mechanisms, especially in the Windows Domain Controller environment.

Kerberos Domain Server

This attribute specifies the Kerberos Distribution Center (the domain controller) hostname. You must enter the fully qualified domain name (FQDN) of the domain controller.

Kerberos Domain

This attribute specifies the Kerberos Distribution Center (KDC) domain name. Depending up on your configuration, the domain name of the domain controller may be different than the OpenSSO Enterprise domain name.

Kerberos Service Principal

Specifies the web service principal registered with the KDC.

Use the following format:

```
HTTP/hostname.domainname@dc_domain_name
```

`hostname` and `domainame` represent the hostname and domain name of the OpenSSO Enterprise instance. `dc_domain_name` is the Kerberos domain in which the Windows Kerberos server (domain controller) resides. It is possible that the Kerberos server is different from the domain name of the OpenSSO Enterprise instance.

Kerberos Ticket Cache Directory

Specifies the Kerberos TGT (Ticket Granting Ticket) cache directory. When the user authenticates to the desktop or initializes using `kinit` (the command used to obtain the TGT from KDC), the TGT is stored in the local cache, as defined in this attribute.

STS Client

The Security Token Service (STS) Client interface allows you to create and configure a client that communicates with OpenSSO Enterprise's Security Token service in order to obtain a Security Token. OpenSSO Enterprise provides the mechanism to create the following types of STS client agents:

Discovery Agent — Allows you to configure a Discovery Agent Client that communicates with the Liberty Discovery Service to obtain a Liberty-based security token. This configuration defines the attributes for securing Liberty requests from the Discovery client to the Liberty Discovery end point.

Security Token Service Agent — Allows you to configure a Security Token Service agent that communicates with OpenSSO Enterprise's Security Token Service to obtain web service-based security tokens. This configuration defines the attributes for securing web service Trust requests from the STS client to the STS end point.

Discovery Agent Attributes

The Discovery Agent profile holds a trust authority configuration that is used by the web services' client/profile to communicate with the Liberty Discovery service for web service lookups, registration, and for obtaining security credentials.

Group

The Group mechanism allows you to define a collection of similar types of agents. The group must be defined before including the particular agent into a collection.

Password

Defines the password for the Discovery Agent.

Password Confirm

Confirm the password.

Status

Defines whether the agent will be active or inactive in the system. By default, this attribute is set to active, meaning that the agent will participate in securing outbound web service requests from web service clients and will validate web service responses from a web service provider.

Location of Agent Configuration Repository

This attribute defines the agent location of the configuration repository for the Discovery Agent.

Private Key Alias

This attribute defines the private certificate key alias that is used to sign the web service request or decrypt the web service response.

Discovery Service End Point

This attribute defines the Discovery service end point where the trust authority client establishes communications for service registrations and lookups.

Authentication Web Service End Point

This attribute defines the authentication service end point which the web services client uses to authenticate using the end user's SSOToken to receive the Discovery service resource offering (also referred to as bootstrap resource offering.)

Security Token Service Agent Attributes

A Security Token Service is a Web service that provides issuance and management of security tokens. That is, it makes security statements or claims often, although not required to be, in encrypted sets. These statements are based on the receipt of evidence that it can directly verify security tokens from authorities that it trusts. To assert trust, a service might prove its right to assert a set of claims by providing a security token or set of security tokens issued by an STS, or it could issue a security token with its own trust statement (note that for some security token formats this can just be a re-issuance or co-signature). This forms the basis of trust brokering.

General

The following General attributes define basic Security Token service properties:

Group

The Group mechanism allows you to define a collection of similar types of agents. The group must be defined before including the particular agent into a collection.

Password

Defines the password for the Security Token service agent.

Password Confirm

Confirm the password.

Status

Defines whether the agent will be active or inactive in the system. By default, this attribute is set to active, meaning that the agent will participate in securing outbound web service requests from web service clients and will validate web service responses from a web service provider.

WS-Trust Version

Specifies the version of WS-Trust to use, either 1.0 or 1.3.

Universal Identifier

Lists the basic LDAP properties, that uniquely defines the Security Token service agent.

Security

The following attributes define Security Token service security attributes:

Security Mechanism

Defines the type of security credential that is used to secure the STS request. You can choose one of the following security credential types:

- Anonymous — The anonymous security mechanism contains no security credentials.
- KerberosToken — Uses Kerberos security tokens.
- LibertyDiscoverySecurity — Uses Liberty-based security tokens.
- SAML-HolderOfKey — Uses the SAML 1.1 assertion type Holder-Of-Key.
- SAML-SenderVouches — Uses the SAML 1.1 assertion type Sender Vouches.
- SAML2–HolderOfKey — Uses the SAML 2.0 assertion token type Holder-Of-Key.

- SAML2–SenderVouches — Uses the SAML 2.0 assertion token type Sender Vouches.
- STSSecurity — Uses the security token generated from the Security Token service for a given web service provider.
- UserNameToken — Uses User Name Token with digest password.
- UserNameToken-Plain — Uses a user name token with a clear text password for securing web service requests.
- X509Token — Uses the X509 certificate.

STS Configuration

This attribute is enabled when the Security Token service agent uses Security Token service (STS) as the Security Mechanism. This configuration describes a list of STS agent profiles that are used to communicate with and secure the requests to the STS service.

Preserve Security Headers in Message

When enabled, this attribute defines that the SOAP security headers are preserved by the Security Token service agent for further processing.

Credential for User Token

The attribute represents the username/password shared secrets that are used by the Security Token service agent to generate a Username security token.

Signing and Encryption

The following attributes define signing and encryption configuration for the Security Token service:

Is Request signed

When enabled, the Security Token service agent signs the request using a given token type.

Is Request Header Encrypted

When enabled, the Security Token service agent security header will be encrypted.

Is Request Encrypted

When enabled, the Security Token service request will be encrypted.

Is Response Signature Verified

When enabled, the Security Token service response signature is verified.

Is Response Decrypted

When enabled, the Security Token service response will be decrypted.

Signing Reference Type

Defines the reference types used when the Security Token service signs the WSC response. The possible reference types are `DircectReference`, `KeyIdentifier`, and `X509`.

Encryption Algorithm

Defines the encryption algorithm used to encrypt the response.

Encryption Strength

Sets the encryption strength to encrypt the response. Select a greater value for greater encryption strength.

Key Store

The following attributes configure the keystore to be used for certificate storage and retrieval:

Public Key Alias of Web Service Provider

This attribute defines the public certificate key alias that is sued to encrypt the web service request or verify the signature of the web service response.

Private Key Alias

This attribute defines the private certificate key alias that is used to sign the web service request or decrypt the web service response.

Key Storage Usage

This configuration defines whether to use the default keystore, or a custom keystore. The following values must be defined for a custom key store:

- Location of Key Store
- Password of Key Store
- Password of Key

End Points

The following attributes define web service endpoints:

Security Token Service End Point

This field takes a value equal to:

```
%protocol://%host:%port%uri/sts
```

This syntax allows for dynamic substitution of the Security Token Service Endpoint URL based on the specific session parameters.

Security Token Service MEX End Point

This field takes a value equal to:

```
%protocol://%host:%port%uri/sts/mex
```

This syntax allows for dynamic substitution of the Security Token Service MEX Endpoint URL based on the specific session parameters.

Kerberos Configuration

Kerberos is a security profile supported by the web services security to secure web services communications between a web service client and a web service provider. In a typical scenario, a user authenticates to the desktop and invokes a web service and the web service client. This requires a Kerberos ticket to secure the request to web service provider by identifying his principal as Kerberos token. Typically, Kerberos-based web services security is used in same the context of Kerberos domain (realm) as opposed to across boundaries, for example SAML-based web services security. However, Kerberos is one of the strongest authentication mechanisms, especially in the Windows Domain Controller environment.

Kerberos Domain Server

This attribute specifies the Kerberos Distribution Center (the domain controller) hostname. You must enter the fully qualified domain name (FQDN) of the domain controller.

Kerberos Domain

This attribute specifies the Kerberos Distribution Center (KDC) domain name. Depending up on your configuration, the domain name of the domain controller may be different than the OpenSSO Enterprise domain name.

Kerberos Service Principal

Specifies the Security Token Service principal registered with the KDC.

Use the following format:

```
HTTP/hostname.domainname@dc_domain_name
```

`hostname` and `domainame` represent the hostname and domain name of the OpenSSO Enterprise instance. `dc_domain_name` is the Kerberos domain in which the Windows Kerberos server (domain controller) resides. It is possible that the Kerberos server is different from the domain name of the OpenSSO Enterprise instance.

Kerberos Ticket Cache Directory

Specifies the Kerberos TGT (Ticket Granting Ticket) cache directory. When the user authenticates to the desktop or initializes using `kinit` (the command used to obtain the TGT from KDC), the TGT is stored in the local cache, as defined in this attribute.

2.2 Policy Agent

OpenSSO Enterprise is backward compatible with Policy Agent 2.2. Policy Agent 2.2 must be configured locally from the deployment container on which it is installed. Therefore, from the OpenSSO Enterprise Console, a very limited number of Policy Agent 2.2 options can be configured.

Password

The password was set when you created the agent profile. However, you can change the password at any time in the future.

Password Confirm

The confirmation of the password was performed when you created the agent profile. If you change the password, you must confirm the change.

Status

The `Active` option is selected when the agent is created. Choose `Inactive` only if you want to remove the protection the agent provides.

Description

A description of the agent, which you can add if desired.

Agent Key Value

A required setting when enabling CDSSO and when configuring the deployment to prevent cookie hijacking.

This attribute serves as a key in a pairing of a key and a value. This attribute is used by OpenSSO Enterprise to receive agent requests for credential assertions about users. Only one attribute is valid in this key-value pairing. All other attributes are ignored. Use the following format:

`agentRootURL=protocol://`*hostname*`:`*port*`/`

The entry must be precise. For example, the string representing the key, `agentRootURL`, is case sensitive.

Agent Authenticator

An agent authenticator is a type of agent that, once it is authenticated, can obtain the read-only data of agent profiles that are selected for the agent authenticator to read. The agent profiles can be of any type (J2EE, WSP, Discovery, and so forth), but must exist in the same realm. Users that have the agent authenticator's credentials (username and password) can read the agent profile data, but do not have the create, update, or delete permissions of the Agent Admin.

The agent Authenticator contains the following attributes:

Password

The password was set when you created the agent authenticator profile. However, you can change the password at any time in the future.

Password Confirm

The confirmation of the password was performed when you created the agent authenticator profile. If you change the password, you must confirm the change.

Status

The `Active` option is selected when the agent authenticator is created. Choose `Inactive` only if you want to remove the protection the agent provides.

Agent Profiles Allowed to Read

This attribute defines a list of OpenSSO Enterprise agents whose profile data is read by the agent authenticator. The agents can be of any type (J2EE, WSP, Discovery, and so forth), but must exist in the same realm. To add an agent to the list, select the agent name and click Add.

◆ ◆ ◆ CHAPTER 6

Federation Attributes for Entity Providers

This section lists and describes the attributes available in the OpenSSO Enterprise console for entity provider customization. For instructions for creating the entity providers and entity provider roles, see "Creating an Entity" in *Sun OpenSSO Enterprise 8.0 Administration Guide*

SAMLv2 Entity Provider Attributes

The SAMLv2 entity provider type is based on the OASIS Security Assertion Markup Language (SAML) version 2 specification. This entity supports various profiles (single sign-on, single logout, and so forth) when interacting with remote SAMLv2 entities. The SAMLv2 provider entity allows you to assign and configure the following roles:

SAMLv2 Service Provider Customization

SAMLv2 service providers contain the following attribute groups:

Assertion Content

Request/Response Signing

Select any checkbox to enable signing for the following SAMLv2 service prover requests or responses:

Authentication Requests Signed	All authentication requests received by this service provider must be signed.
Assertions Signed	All assertions received by this service provider must be signed.
POST Response Signed	The identity provider must sign the single sign-on Response element when POST binding is used
Artifact Response	The identity provider must sign the `ArtifactResponse` element.
Logout Request	The identity provider must sign the `LogoutRequest` element.
Logout Response	The identity provider must sign the `LogoutResponse` element.
Manage Name ID Request	The identity provider must sign the `ManageNameIDRequst` element.
Manage Name ID Response	The identity provider must sign the `ManageNameIDResponse` element.

Encryption

Select any checkbox to enable encryption for the following elements:

Attribute	The identity provider must encrypt all `AttributeStatement` elements.
Assertion	The identity provider must encrypt all `Assertion` elements.
NameID	The identity provider must encrypt all `NameID` elements.

Certificate Aliases

This attribute defines the certificate alias elements for the service provider. `signing` specifies the provider certificate alias used to find the correct signing certificate in the keystore. `Encryption` specifies the provider certificate alias used to find the correct encryption certificate in the keystore.

Name ID Format

Defines the name identifier formats supported by the service provider. Name identifiers are a way for providers to communicate with each other regarding a user. Single sign-on interactions support the following types of identifiers:

- `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
- `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName`
- `urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos`
- `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`

The Name ID format list is an ordered list, the first Name ID has the highest priority in determining the Name ID format to use. If the user does not specify a Name ID to use when initiating single sign-on, the first one in this list is chosen and supported by the remote Identity Provider.

A *persistent identifier* is saved to a particular user's data store entry as the value of two attributes. A *transient identifier* is temporary and no data will be written to the user's persistent data store

Authentication Context

This attribute maps the SAMLv2-defined authentication context classes to the authentication level set for the user session for the service provider .

Mapper
: Specifies the implementation of the `SPAuthnContextMapper` interface used to create the requested authentication context. The default implementation is `com.sun.identity.saml2.plugins.DefaultSPAuthnContexteMapper`.

Supported
: Select the check box next to the authentication context class if the identity provider supports it.

Context Reference
: The SAMLv2-defined authentication context classes are:

  - InternetProtocol
  - InternetProtocolPassword
  - Kerberos
  - MobileOneFactorUnregistered
  - MobileTwoFactorUnregistered
  - MobileOneFactorContract
  - MobileTwoFactorContract

- Password
- Password-ProtectedTransport
- Previous-Session
- X509
- PGP
- SPKI
- XMLDSig
- Smartcard
- Smartcard-PKI
- Software-PKI
- Telephony
- NomadTelephony
- PersonalTelephony
- AuthenticaionTelephony
- SecureRemotePassword
- TLSClient
- Time-Sync-Token
- Unspecified

Level
: Takes as a value a positive number that maps to an authentication level defined in the OpenSSO Enterprise Authentication Framework. The authentication level indicates how much to trust a method of authentication.

  In this framework, each service provider is configured with a default authentication context (preferred method of authentication). However, the provider might like to change the assigned authentication context to one that is based on the defined authentication level. For example, provider B would like to generate a local session with an authentication level of 3 so it requests the identity provider to authenticate the user with an authentication context assigned that level. The value of this query parameter determines the authentication context to be used by the identity provider.

Comparison Type
: Specifies what the resulting authentication context must be when compared to the value of this property. Accepted values include:

  - *exact* where the authentication context statement in the assertion must be the exact match of, at least, one of the authentication contexts specified.
  - *minimum* where the authentication context statement in the assertion must be, at least, as strong (as deemed by the identity provider) one of the authentication contexts specified.
  - *maximum* where the authentication context statement in the assertion must be no stronger than any of the authentication contexts specified.
  - *better* where the authentication context statement in the assertion must be stronger than any of the authentication contexts specified.

The default value is *exact*.

Assertion Time Skew

Assertions are valid for a period of time and not before or after. This attribute specifies a grace period (in seconds) for the `notBefore` value. The default value is `300`. It has no relevance to the `notAfter` value.

Basic Authentication

Basic authentication can be enabled to protect SOAP endpoints. Any provider accessing these endpoints must have the user and password defined in the following two properties: `User Name` and `Password`.

Assertion Processing

Attribute Mapper

Specifies the values to define the mappings used by the default attribute mapper plug-in. The default plug-in class is `com.sun.identity.saml2.plugins.DefaultSPAttributeMapper`.

Mappings should be configured in the format:

```
SAML_Assertion_Attribute_Name=User_Profile_Attribute_Name
```

For example, `EmailAddress=mail` or `Address=postaladdress`. Type the mapping as a New Value and click Add.

Auto Federation

If enabled, Auto-federation automatically federates a user's different provider accounts based on a common attribute. The Attribute field specifies the attribute used to match a user's different provider accounts when auto-federation is enabled.

Account Mapper

Specifies the implementation of the `AccountMapper` interface used to map a remote user account to a local user account for purposes of single sign-on. The default value is `com.sun.identity.saml2.plugins.DefaultSPAccountMapper`, the default implementation.

Artifact Message Encoding

This attribute defines the message encoding format for artifact, either `URI` or `FORM`.

Transient User

This attribute specifies the identifier of the user to which all identity provider users will be mapped on the service provider side in cases of single sign-on using the transient name identifier.

URL

The Local Authentication URL specifies the URL of the local login page.

The Intermediate URL specifies a URL to which a user can be directed after authentication and before the original request's URL. An example might be a successful account creation page after the auto-creation of a user account.

The External Application Logout URL defines the logout URL for an external application. Once the server receives logout request from the remote partner, a request will be sent to the logout URL using back channel `HTTP POST` with all cookies. Optionally, a user session property could be sent as `HTTP header` and `POST` parameter if a query parameter `appsessionproperty` (set to the session property name) is included in the URL.

Default Relay State

After a successful SAML v2 operation (single sign-on, single logout, or federation termination), a page is displayed. This page, generally the originally requested resource, is specified in the initiating request using the `RelayState` element. If a `RelayState` is not specified, the value of this `defaultRelayState` property is displayed.

Caution – When `RelayState` or `defaultRelayState` contains special characters (such as &), it must be URL-encoded. For example, if the value of `RelayState` is `http://www.sun.com/apps/myapp.jsp?param1=abc&param2=xyz`, it must be URL-encoded as:

```
http%3A%2F%2Fwww.sun.com%2Fapps%2Fmyapp.jsp
%3Fparam1%3Dabc%26param2%3Dxyz
```

and then appended to the URL. For example, the service provider initiated single sign-on URL would be:

```
http://host:port/deploy-uri/saml2/jsp/spSSOInit.jsp?
metaAlias=/sp&idpEntityID=http://www.idp.com&RelayState=
http%3A%2F%2Fwww.sun.com%2Fapps%2Fmyapp.jsp%3Fparam1
%3Dabc%26param2%3Dxyz
```

Adapter

Defines the implementation class for the `com.sun.identity.saml2.plugins.SAML2ServiceProviderAdapter` interface, used to add application-specific processing during the federation process.

Services

- "Meta Alias" on page 135
- "Single Logout Service" on page 135
- "Manage Name ID Service" on page 136
- "Assertion Artifact Consumer Service" on page 136

Meta Alias

Specifies a `metaAlias` for the provider being configured. The `metaAlias` is used to locate the provider's entity identifier and the organization in which it is located. The value is a string equal to the realm or organization name coupled with a forward slash and the provider name. For example, `/suncorp/travelprovider`.

Caution – The names used in the `metaAlias` must not contain a `/`.

Single Logout Service

The Single Logout Service synchronizes the logout functionality across all sessions authenticated by the service provider.

`Location` specifies the URL of the provider to which the request is sent. `Response Location` specifies the URL the expected response provider. The binding types are:

- HTTP Redirect
- POST
- SOAP

Manage Name ID Service

This services defines the URLs that will be used when communicating with the service provider to specify a new name identifier for the principal. (Registration can occur only after a federation session is established.)

`Location` specifies the URL of the provider to which the request is sent. `Response Location` specifies the URL the expected response provider. The binding types are:

- HTTP Redirect
- POST
- SOAP

Assertion Artifact Consumer Service

This service processes the responses that a service provider receives from an identity provider. When a service provider wants to authenticate a user, it sends an authentication request to an identity provider.

- HTTP-Artifact specifies a non-browser SOAP-based protocol.
- HTTP-Post specifies a browser-based HTTP POST protocol.
- PAOS defines the URL location for PAOS binding.

`Location` specifies the URL of the provider to which the request is sent. `Index` specifies the URL in the standard metadata. `Default`is the default URL to be used for the binding.

Advanced

- "SP URL" on page 137
- "SP Logout URL" on page 137
- "App Secret List" on page 137
- "Request IDP List Finder Implementation" on page 137
- "Request IDP List Get Complete" on page 137
- "Request IDP List" on page 137
- "IDP Proxy" on page 137
- "Introduction" on page 137
- "Proxy Count" on page 137
- "IDP Proxy List" on page 138

SP URL

Defines URL endpoint on Service Provider that can handle SAE (Secure Attribute Exchange) requests. If this URL is empty (not configured), SAE single sign-on will not be enabled. Normal SAMLv2 single sign-on responses will be sent to the service provider.

SP Logout URL

Defines the URL endpoint on a Service Provider that can handle SAE global logout requests.

App Secret List

This attribute defines the application security configuration. Each application must have one entry. Each entry has the following format:

`url=SPAppURL|type=`*`symmetric_orAsymmetric`*`|secret=`*`ampassword encoded shared secret`*

Request IDP List Finder Implementation

Defines the implementation class of the IDP list finder SPI. This returns a list of preferred identity providers that are trusted by the ECP.

Request IDP List Get Complete

Specifies a URI reference that can be used to retrieve the complete identity provider list if the `IDPList` element is not complete.

Request IDP List

Defines a list of identity providers for the ECP to contact. This is used by the default implementation of the IDP Finder (for example, `com.sun.identity.saml2.plugins.ECPIDPFinder`).

IDP Proxy

Proxy Authentication Configuration attributes define values for dynamic identity provider proxying. Select the check box to enable proxy authentication for a service provider.

Introduction

Select the check box if you want introductions to be used to find the proxying identity provider.

Proxy Count

Enter the maximum number of identity providers that can be used for proxy authentication.

IDP Proxy List

Add a list of identity providers that can be used for proxy authentication. Type the URI defined as the provider's identifier in New Value and click Add.

SAMLv2 Identity Provider Customization

SAMLv2 identity providers contain the following attribute groups:

Assertion Content

Request/Response Signing

Setting the following flags indicate to the identity provider how the service provider signs specific messages:

Authentication Request	All authentication requests received by this identity provider must be signed.
Artifact Resolve	The service provider must sign the `ArtifactResolve` element.
Logout Request	The service provider must sign the `LogoutRequest` element.
Logout Response	The service provider must sign the `LogoutResponse` element.
Manage Name ID Request	The service provider must sign the `ManageNameIDRequst` element.
Manage Name ID Response	The service provider must sign the `ManageNameIDResponse` element.

Encryption

Select the checkbox to enable encryption for the following elements:

NameID	The service provider must encrypt all `NameID` elements.

Certificate Aliases

This attribute defines the certificate alias elements for the identity provider. `Signing` specifies the provider certificate alias used to find the correct signing certificate in the keystore. `Encryption` specifies the provider certificate alias used to find the correct encryption certificate in the keystore.

Name ID Format

Defines the name identifier formats supported by the identity provider. Name identifiers are a way for providers to communicate with each other regarding a user. Single sign-on interactions support the following types of identifiers:

- `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
- `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName`
- `urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos`
- `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`

The Name ID format list is an ordered list and the first Name ID has the highest priority in determining the Name ID format to use. If the user does not specify a Name ID to use when initiating single sign-on, the first one in this list is chosen and supported by the remote Identity Provider.

A *persistent identifier* is saved to a particular user's data store entry as the value of two attributes. A *transient identifier* is temporary and no data will be written to the user's persistent data store

Name ID Value Map

This attribute specifies mapping between the NameID Format attribute and a user profile attribute. If the defined Name ID format is used in protocol, the profile attribute value will be used as NameID value for the format in the Subject. The syntax of each entry is:

NameID Format=User profile attribute

For example:

```
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress=mail
```

To add new NameID format, the NameID Value Map attribute needs to be updated with a corresponding entry. The exceptions are `persistent`, `transient` and `unspecified`. For `persistent` and `transient`, the NameID value will be generated randomly. For this attribute, `unspecified` is optional. If it is specified, the NameID value will be the value of the user profile attribute. If it is not specified, an random number will be generated.

Authentication Context

This attribute maps the SAMLv2-defined authentication context classes to authentication methods available from the identity provider.

Mapper
: Specifies the implementation of the `IDPAuthnContextMapper` interface used to create the requested authentication context. The default implementation is `com.sun.identity.saml2.plugins.DefaultIDPAttributeMapper`.

Default Authentication Context
: Specifies the default authentication context type used by the identity provider if the service provider does not send an authentication context request.

Supported
: Select the check box next to the authentication context class if the identity provider supports it.

Context Reference
: The SAMLv2-defined authentication context classes are:

- InternetProtocol
- InternetProtocolPassword
- Kerberos
- MobileOneFactorUnregistered
- MobileTwoFactorUnregistered
- MobileOneFactorContract
- MobileTwoFactorContract
- Password
- Password-ProtectedTransport
- Previous-Session
- X509
- PGP
- SPKI
- XMLDSig
- Smartcard
- Smartcard-PKI
- Software-PKI
- Telephony
- NomadTelephony

- PersonalTelephony
- AuthenticaionTelephony
- SecureRemotePassword
- TLSClient
- Time-Sync-Token
- Unspecified

Key
: Choose the OpenSSO Enterprise authentication type to which the context is mapped.

Value
: Type the OpenSSO Enterprise authentication option.

Level
: Takes as a value a positive number that maps to an authentication level defined in the OpenSSO Enterprise Authentication Framework. The authentication level indicates how much to trust a method of authentication.

  In this framework, each identity provider is configured with a default authentication context (preferred method of authentication). However, the provider might like to change the assigned authentication context to one that is based on the defined authentication level. For example, provider B would like to generate a local session with an authentication level of 3 so it requests the identity provider to authenticate the user with an authentication context assigned that level. The value of this query parameter determines the authentication context to be used by the identity provider.

Assertion Time

Assertions are valid for a period of time and not before or after. This attribute specifies a grace period (in seconds) for the `Not Before Time Skew` value. The default value is `600`. It has no relevance to the `notAfter` value.

`Effective Time` specifies (in seconds) the amount of time that an assertion is valid counting from the assertion's issue time. The default value is `600` seconds.

Basic Authentication

Basic authentication can be enabled to protect SOAP endpoints. Any provider accessing these endpoints must have the user and password defined in the following two properties: `User Name` and `Password`.

Assertion Cache

If enabled, this allows the identity provider to cache assertions to be retrieved later.

Bootstrapping

Select the check box if you want a Discovery Service Resource Offering to be generated during the Liberty-based single sign-on process for bootstrapping purposes.

Assertion Processing

Attribute Mapper

Specifies the values to define the mappings used by the default attribute mapper plug-in. The default plug-in class is `com.sun.identity.saml2.plugins.DefaultIDPAttributeMapper`.

Mappings should be configured in the format:

SAML-attribute=local-attribute

For example, `EmailAddress=mail` or `Address=postaladdress`. Type the mapping as a New Value and click Add.

Account Mapper

Specifies the implementation of the `AccountMapper` interface used to map a remote user account to a local user account for purposes of single sign-on. The default value is `com.sun.identity.saml2.plugins.DefaultIDPAccountMapper`, the default implementation.

Local Configuration

These attribute contains configuration specific to the OpenSSO Enterprise instance.

Auth URL

Defines the Authentication URL to which the identity provider will redirect for authentication.

External Application Logout URL

The External Application Logout URL defines the logout URL for an external application. Once the server receives logout request from the remote partner, a request will be sent to the logout URL using back channel `HTTP POST` with all cookies. Optionally, a user session property could be sent as `HTTP header` and `POST` parameter if a query parameter `appsessionproperty` (set to the session property name) is included in the URL.

Services

Meta Alias

Specifies a `metaAlias` for the provider being configured. The `metaAlias` is used to locate the provider's entity identifier and the organization in which it is located. The value is a string equal to the realm or organization name coupled with a forward slash and the provider name. For example, `/suncorp/travelprovider`.

Caution – The names used in the `metaAlias` must not contain a `/`.

Artifact Resolution Service

Defines the endpoint(s) that support the Artifact Resolution profile. `Location` specifies the URL of the provider to which the request is sent. `Index` specifies a unique integer value to the endpoint so that it can be referenced in a protocol message.

Single Logout Service

The Single Logout Service synchronizes the logout functionality across all sessions authenticated by the identity provider.

`Location` specifies the URL of the provider to which the request is sent. `Response Location` specifies the URL of the provider to which the response is sent. The binding types are:

- HTTP Redirect
- POST
- SOAP

Manage Name ID Service

This services defines the URLs that will be used when communicating with the service provider to specify a new name identifier for the principal. (Registration can occur only after a federation session is established.)

`Location` specifies the URL of the provider to which the request is sent. `Response Location` specifies the URL of the provider to which the response is sent. . The binding types are:

- HTTP Redirect

- POST
- SOAP

Single Sign-On Service

Defines the endpoint(s) that support the profiles of the Authentication Request protocol. All identity providers must support at least one such endpoint.

`Location` specifies the URL of the provider to which the request is sent. The binding types are:

- HTTP Redirect
- POST
- SOAP

Advanced

- "IDP URL" on page 144
- "App Secret List" on page 144
- "IDP Mapper Session" on page 144

IDP URL

Defines the URL endpoint on Identity Provider that can handle SAE (Secure Attribute Exchange) requests.

App Secret List

Defines the application security configuration. Each application must one entry. Each entry has the following format:

`url=IDPAppURL|type=`*symmetric_orAsymmetric*`|secret=`*ampassword encoded shared secret*
OR `or pubkeyalias=`*idp app signing cert*

IDP Mapper Session

Defines an implementation class for the session mapper SPI. The mapper finds a valid session from HTTP servlet request on the identity provider with an ECP profile.

SAMLv2 XACML PDP Customization

XACML PDP contains the following attributes for customization:

- "Protocol Support Enumeration" on page 145
- "Signing Key Alias" on page 145
- "Encryption Key Alias" on page 145

Protocol Support Enumeration

Displays the XACML PDP release that is supported by this provider.

`urn:liberty:iff:2003-08` refers to Liberty Identity Federation Framework Version 1.2.

`urn:liberty:iff:2002-12` refers to Liberty Identity Federation Framework Version 1.1.

Signing Key Alias

Defines the key alias that is used to sign requests and responses.

Encryption Key Alias

Defines the key alias to XACML encryption.

Basic Authorization

Basic authorization can be enabled to protect SOAP endpoints. Any provider accessing these endpoints must have the user and password defined in the following two properties: `User Name` and `Password`.

Authorization Decision Query Signed

When enabled, this attribute enforces that all queries be signed for the XACML authorization decision.

Authorization Service

This attribute defines the type (binding) of the authorization request, and the URL endpoint for receiving the request. By default, the binding type is SOAP.

SAMLv2 XACML PEP Customization

XACML PEP contains the following attributes for customization:

- "Assertion Encrypted" on page 146

Protocol Support Enumeration

Displays the XACML PEP release that is supported by this provider.

Signing Key Alias

Defines the key alias that is used to sign requests and responses.

Encryption Key Alias

Defines the key alias to XACML encryption.

Basic Authorization

Basic authorization can be enabled to protect SOAP endpoints. Any provider accessing these endpoints must have the user and password defined in the following two properties: `User Name` and `Password`.

Authorization Decision Response Signed

When enabled, this attribute enforces that all responses be signed for the XACML authorization decision.

Assertion Encrypted

When enabled, this attribute enforces that all assertions are to be encrypted.

SAMLv2 Attribute Authority Customization

SAMLv2 Attribute Authority contains the following attributes for customization:

- "Signing and Encryption" on page 146
- "Attribute Service" on page 147
- "AssertionID Request" on page 147
- "Attribute Profile" on page 147
- "Cert Alias" on page 147
- "Subject Data Store" on page 147

Signing and Encryption

Key Size	The length for keys used by the Attribute Authority entity when interacting with another entity.
Algorithm	The encryption algorithm used to interact with another entity.

Attribute Service

This attribute defines the URL endpoints that will receive attribute query requests. `Location` specifies the URL of the provider to which the request is sent. `Mapper` defines the SPI that finds the attribute mapping authority to return a list of attributes that will be included in a response. The SAMLv2–defined attribute query profiles are:

- Basic
- X509

AssertionID Request

Defines the URLs to which the AssertionIDs are sent from a client to an identity provider in order to retrieve the corresponding assertion. `Location` specifies the URL of the provider to which the request is sent. `Mapper` defines the SPI that finds the AssertionID mapping authority to return a list of attributes that will be included in a response. The bindings are:

- SOAP
- URI

Attribute Profile

Defines the type of SAMLv2–defined supported attribute profile. `Basic` is the default type.

Cert Alias

Defines the certificate alias elements. `Signing` specifies the provider certificate alias used to find the correct signing certificate in the keystore. `Encryption` specifies the provider certificate alias used to find the correct encryption certificate in the keystore.

Subject Data Store

Specifies the data store attribute name which contains the X509 subject DN. It is used to find a user whose attribute value matches the X. 509 subject DN. This field is used in the Attribute Query Profile for X. 509 subject only.

SAMLv2 Attribute Query Customization

SAMLv2 Attribute Query contains the following attributes for customization:

- "NameID Format" on page 148
- "Cert Alias" on page 148

NameID Format

Defines the name identifier formats supported by the attribute query provider. Name identifiers are a way for providers to communicate with each other regarding a user. Single sign-on interactions support three types of identifiers:

- An *X509SubjectName* defines the subject name of the X509 encryption type.
- A *persistent identifier* is saved to a particular user's data store entry as the value of two attributes.
- A *transient identifier* is temporary and no data will be written to the user's persistent data store.

Cert Alias

This attribute defines the certificate alias elements for the provider. `signing` specifies the provider certificate alias used to find the correct signing certificate in the keystore. `Encryption` specifies the provider certificate alias used to find the correct encryption certificate in the keystore.

SAMLv2 Authentication Authority Customization

SAMLv2 Authentication Authority contains the following attributes for customization:

Signing and Encryption

Key Size	The length for keys used by the Attribute Authority entity when interacting with another entity.
Algorithm	The encryption algorithm used to interact with another entity.

Authn Query Service

This attribute defines the URL to which authentication queries are sent.

AssertionID Request

Defines the URLs to which the AssertionIDs are sent from a client to an identity provider in order to retrieve the corresponding assertion. `Location` specifies the URL of the provider to which the request is sent. The AssertionID request types are:

- SOAP
- URI

Cert Alias

This attribute defines the certificate alias elements for the provider. `signing` specifies the provider certificate alias used to find the correct signing certificate in the keystore. `Encryption` specifies the provider certificate alias used to find the correct encryption certificate in the keystore.

ID-FF Entity Provider Attributes

The ID-FF provider entity is based on the Liberty-defined ID-FF (Liberty Identity Federation Framework) for implementing single sign-on with federated identities. The IF-FF provider entity allows you to assign and configure the following roles:

ID-FF Identity Provider Customization

The ID-FF identity provider attributes are grouped as follows:

Common Attributes

Provider Type

The static value of this attribute is the type of provider being configured: hosted or remote

Description

The value of this attribute is a description of the identity provider.

Protocol Support Enumeration

Choose the Liberty ID-FF release that is supported by this provider.

- `urn:liberty:iff:2003-08` refers to the Liberty Identity Federation Framework Version 1.2.
- `urn:liberty:iff:2002-12` refers to the Liberty Identity Federation Framework Version 1.1.

Signing Key

Defines the security certificate alias that is used to sign requests and responses.

Encryption Key

Defines the security certificate alias that is used for encryption for the Signing Key and Encryption Key. Certificates are stored in a Java keystore file. Each specific certificate is mapped to an alias that is used to fetch the certificate.

Name Identifier Encryption

Select the check box to enable encryption of the name identifier.

Communication URLs

- "SOAP Endpoint" on page 151
- "Single Sign-on Service URL" on page 151
- "Single Logout Service " on page 151
- "Single Logout Return" on page 151
- "Federation Termination Service" on page 151
- "Federation Termination Return" on page 151
- "Name Registration Service" on page 151
- "Name Registration Return" on page 151

SOAP Endpoint

Defines a URI to the identity provider's SOAP message receiver. This value communicates the location of the SOAP receiver in non browser communications.

Single Sign-on Service URL

Defines a URL to which service providers can send single sign-on and federation requests.

Single Logout Service

Defines a URL to which service providers can send logout requests. Single logout synchronizes the logout functionality across all sessions authenticated by the identity provider.

Single Logout Return

Defines a URL to which the service providers can send single logout responses.

Federation Termination Service

Defines a URL to which a service provider will send federation termination requests.

Federation Termination Return

Defines a URL to which the service providers can send federation termination responses.

Name Registration Service

Defines a URL to which a service provider will send requests to specify a new name identifier to be used when communicating with the identity provider about a principal. This service can only be used after a federation session is established.

Name Registration Return

Defines a URL to which the service providers can send name registration responses.

Communication Profiles

- "Federation Termination" on page 152
- "Single Logout" on page 152
- "Name Registration" on page 152
- "Single Sign-on/Federation" on page 152

Federation Termination

Select a profile to notify other providers of a principal's federation termination:

- HTTP Redirect
- SOAP

Single Logout

Select a profile to notify other providers of a principal's logout:

- HTTP Redirect
- HTTP Get
- SOAP

Name Registration

Select a profile to notify other providers of a principal's name registration:

- HTTP Redirect
- SOAP

Single Sign-on/Federation

Select a profile for sending authentication requests:

- Browser Post (specifies a browser-based HTTP POST protocol)
- Browser Artifact (specifies a non-browser SOAP-based protocol)
- LECP (specifies a Liberty-enabled Client Proxy)

Note – OpenSSO Enterprise can handle requests that come from a Liberty-enabled client proxy profile, but it requires additional configuration that is beyond the scope of this manual.

Identity Provider Configuration

Provider Alias

Defines the alias name for the local identity provider.

Authentication Type

Select the provider that should be used for authentication requests from a provider hosted locally:

- *Remote* specifies that the provider hosted locally would contact a remote identity provider upon receiving an authentication request.
- *Local* specifies that the provider hosted locally should contact a local identity provider upon receiving an authentication request (essentially, itself).

Assertion Issuer

Defines the name of the host that issues the assertion. This value might be the load balancer's host name if OpenSSO Enterprise is behind one.

Responds With

Specifies the type of statements the identity provider can generate. For example `lib:AuthenticationStatement`.

Provider Status

Defines whether the identity provider is active or inactive. Active, the default, means the identity provider can process requests and generate responses.

Service URL

Home Page URL

Defines the URL of the home page of the identity provider.

Single Sign-on Failure Redirect URL

Defines the URL to which a principal will be redirected if single sign-on has failed.

Federate Page URL

Specifies the URL which performs the federation operation.

Registration Done URL

Defines the URL to which a principal will be directed upon successful Federation registration.

List of COTs Page URL

Defines the URL that lists all of the circle of trusts to which the provider belongs.

Termination URL

Defines the URL to which a principal is directed upon Federation termination.

Termination Done URL

Defines the URL to which a principal is redirected after federation termination is completed.

Error Page URL

Defines the URL to which a principal is directed upon an error.

Logout Done URL

Defines the URL to which a principal is directed after logout.

Plug-ins

Name Identifier Implementation

This field defines the class used by an identity provider to participate in name registration. Name registration is a profile by which service providers specify a principal's name identifier that an identity provider will use when communicating with the service provider. The value is `com.sun.identity.federation.services.util.FSNameIdentifierImpl`.

Attribute Statement Plug-in

Specifies a plug-able class used for adding attribute statements to an assertion that is generated during the Liberty-based single sign-on process.

User Provider Class

Specifies a plug-able class used to provide user operations such as finding a user, getting user attributes, and so forth . The default value is:

`com.sun.identity.federation.accountmgmt.DefaultFSUserProvider`

Identity Provider Attribute Mapper

Attribute Mapper Class

The class used to map user attributes defined locally to attributes in the SAML assertion. There is no default class.

Identity Provider Attribute Mapping

Specify values to define the mappings used by the default attribute mapper plug-in. Mappings should be configured in the format:

SAML-attribute=local-attribute

For example, `Email=emailaddress` or `Address=postaladdress`. Type the mapping as a New Value and click Add.

Bootstrapping

The bootstrapping attribute is:

Generate Discovery Bootstrapping Resource Offering

Select the check box if you want a Discovery Service Resource Offering to be generated during the Liberty-based single sign-on process for bootstrapping purposes.

Auto Federation

Auto Federation

Select the check box to enable auto-federation.

Auto Federation Common Attribute Name

When creating an Auto Federation Attribute Statement, the value of this attribute will be used. The statement will contain the attribute element and this common attribute as its value.

Authentication Context

This attribute defines the identity provider's default authentication context class (method of authentication). This method will always be called when the service provider sends an authentication request. This value also specifies the authentication context used by the service provider when an unknown user tries to access a protected resource.

Supported
: Select the check box next to the authentication context class if the identity provider supports it.

Context Reference
: The Liberty-defined authentication context classes are:

- Mobile Contract
- Mobile Digital ID
- MobileUnregistered
- Password
- Password-ProtectedTransport
- Previous-Session
- Smartcard
- Smartcard-PKI
- Software-PKI
- Time-Sync-Token

Key
: Choose the OpenSSO Enterprise authentication type to which the context is mapped.

Value
: Type the OpenSSO Enterprise authentication option.

Level
: Choose a priority level for cases where there are multiple contexts.

SAML Attributes

- "Assertion Interval" on page 157
- "Cleanup Interval" on page 157
- "Artifact Timeout" on page 157

- "Assertion Limit" on page 157

Assertion Interval

Type the interval of time (in seconds) that an assertion issued by the identity provider will remain valid.

Cleanup Interval

Type the interval of time (in seconds) before a cleanup is performed to expired assertions.

Artifact Timeout

Type the interval of time (in seconds) to specify the timeout for assertion artifacts.

Assertion Limit

Type a number to define how many assertions an identity provider can issue, or how many assertions that can be stored.

ID-FF Service Provider Customization

The ID-FF service provider attributes are grouped into the following sections:

- "Common Attributes" on page 157
- "Communication URLs" on page 158
- "Communication Profiles" on page 160
- "Service Provider Configuration " on page 161
- "Service URL" on page 162
- "Plug-ins" on page 163
- "Service Provider Attribute Mapper" on page 163
- "Auto Federation " on page 164
- "Authentication Context" on page 164
- "Proxy Authentication Configuration" on page 165

Common Attributes

- "Provider Type" on page 158
- "Description" on page 158
- "Protocol Support Enumeration" on page 158
- "Signing Key" on page 158
- "Encryption Key" on page 158
- "Name Identifier Encryption" on page 158
- "Sign Authentication Request" on page 158

Provider Type

The static value of this attribute is the type of provider being configured: hosted or remote

Description

The value of this attribute is a description of the service provider.

Protocol Support Enumeration

Choose the Liberty ID-FF release that is supported by this provider.

- `urn:liberty:iff:2003-08` refers to the Liberty Identity Federation Framework Version 1.2.
- `urn:liberty:iff:2002-12` refers to the Liberty Identity Federation Framework Version 1.1.

Signing Key

Defines the security certificate alias that is used to sign requests and responses. Certificates are stored in a Java keystore file. Each specific certificate is mapped to an alias that is used to fetch the certificate

Encryption Key

Defines the security certificate alias that is used for encryption. Certificates are stored in a Java keystore file. Each specific certificate is mapped to an alias that is used to fetch the certificate.

Name Identifier Encryption

Select the check box to enable encryption of the name identifier.

Sign Authentication Request

If enabled, the service provider will sign all authentication requests.

Communication URLs

- "SOAP Endpoint" on page 159
- "Single Logout Service " on page 159
- "Single Logout Return" on page 159
- "Federation Termination Service" on page 159
- "Federation Termination Return" on page 159
- "Name Registration Service" on page 159
- "Name Registration Return" on page 159

SOAP Endpoint

Defines a URI to the service provider's SOAP message receiver. This value communicates the location of the SOAP receiver in non browser communications.

Single Logout Service

Defines a URL to which identity providers can send logout requests. Single logout synchronizes the logout functionality across all sessions authenticated by the identity provider.

Single Logout Return

Defines a URL to which the identity providers can send single logout responses.

Federation Termination Service

Defines a URL to which an identity provider will send federation termination requests.

Federation Termination Return

Defines a URL to which the identity providers can send federation termination responses.

Name Registration Service

Defines a URL that will be used when communicating with the identity provider to specify a new name identifier for the principal. (Registration can occur only after a federation session is established.)

Name Registration Return

Defines a URL to which the identity providers can send name registration responses. (Registration can occur only after a federation session is established.)

Assertion Consumer URL

Defines the URL to which an Identity Provider can send SAML assertions.

Assertion Consumer Service URL ID

If the value of the Protocol Support Enumeration common attribute is `urn:liberty:iff:2003-08`, type the required ID.

Set Assertion consumer Service URL as Default

Select the check box to use the Assertion Consumer Service URL as the default value when no identifier is provided in the request.

Communication Profiles

Federation Termination

Select a profile to notify other providers of a principal's federation termination:

- HTTP Redirect
- SOAP

Single Logout

Select a profile to notify other providers of a principal's logout:

- HTTP Redirect
- HTTP Get
- SOAP

Name Registration

Select a profile to notify other providers of a principal's name registration:

- HTTP Redirect
- SOAP

Supported SSO Profile

Select a profile for sending authentication requests:

- Browser Post (specifies a browser-based HTTP POST protocol)
- Browser Artifact (specifies a non-browser SOAP-based protocol)
- WML (specifies the Wireless Markup Language protocol)
- LECP (specifies a Liberty-enabled Client Proxy)

Note – OpenSSO Enterprise can handle requests that come from a Liberty-enabled client proxy profile, but it requires additional configuration that is beyond the scope of this manual.

Service Provider Configuration

Provider Alias

Defines an alias name for the local service provider.

Authentication Type

Select the provider that should be used for authentication requests from a provider hosted locally:

- *Remote* specifies that the provider hosted locally would contact a remote identity provider upon receiving an authentication request.
- *Local* specifies that the provider hosted locally should contact a local identity provider upon receiving an authentication request (essentially, itself).

Identity Provider Forced Authentication

Select the check box to indicate that the identity provider must re-authenticate (even during a live session) when an authentication request is received. This attribute is enabled by default.

Request Identity Provider to be Passive

Select the check box to specify that the identity provider must not interact with the principal and must interact with the user.

Name Registration After Federation

This option, if enabled, allows for a service provider to participate in name registration after it has been federated.

Name ID Policy

An enumeration permitting requester influence over name identifier policy at the identity provider.

Affiliation Federation

Select the check box to enable affiliation federation.

Provider Status

Defines whether the service provider is active or inactive. Active, the default, means the service provider can process requests and generate responses.

Responds With

Specifies the type of statements the service provider can generate. For example , `lib:AuthenticationStatement`.

Service URL

List of COTs Page URL

Defines the URL that lists all of the circle of trusts to which the provider belongs.

Federate Page URL

Specifies the URL which performs the federation operation.

Home Page URL

Defines the URL of the home page of the identity provider.

Single Sign-on Failure Redirect URL

Defines the URL to which a principal will be redirected if single sign-on has failed.

Termination Done URL

Defines the URL to which a principal is redirected after federation termination is completed.

Error Page URL

Defines the URL to which a principal is directed upon an error.

Logout Done URL

Defines the URL to which a principal is directed after logout.

Plug-ins

Service Provider Adapter

Defines the implementation class for the `com.sun.identity.federation.plugins.FSSPAdapter` interface. The default value is:

```
com.sun.identity.federation.plugins.FSDefaultSPAdapter
```

Federation SP Adapter Env

Defines a list of environment properties to be used by the service provider adapter SPI implementation class.

User Provider Class

Specifies a plug-able class used to provide user operations such as finding a user, getting user attributes, and so forth. . The default value is:

```
com.sun.identity.federation.accountmgmt.DefaultFSUserProvider
```

Name Identifier Implementation

This field defines the class used by a service provider to participate in name registration. Name registration is a profile by which service providers specify a principal's name identifier that an identity provider will use when communicating with the service provider. The value is `com.sun.identity.federation.services.util.FSNameIdentifierImpl`.

Service Provider Attribute Mapper

Attribute Mapper Class

The class used to map user attributes defined locally to attributes in the SAML assertion. There is no default class.

Service Provider Attribute Mapping

Specify values to define the mappings used by the default attribute mapper plug-in specified above. Mappings should be configured in the format:

SAML-attribute=local-attribute

For example, `Email=emailaddress` or `Address=postaladdress`. Type the mapping as a New Value and click Add.

Auto Federation

Auto Federation

Select the check box to enable auto-federation.

Auto Federation Common Attribute Name

Defines the user's common LDAP attribute name such as `telephonenumber`. For creating an Auto Federation Attribute Statement. When creating an Auto Federation Attribute Statement, the value of this attribute will be used. The statement will contain the attribute element and this common attribute as its value.

Authentication Context

This attribute defines the service provider's default authentication context class (method of authentication). This method will always be called when the service provider sends an authentication request. This value also specifies the authentication context used by the service provider when an unknown user tries to access a protected resource. The options are:

Supported
: Select the check box next to the authentication context class if the service provider supports it.

Context Reference
: The Liberty-defined authentication context classes are:

  - Mobile Contract
  - Mobile Digital ID

- MobileUnregistered
- Password
- Password-ProtectedTransport
- Previous-Session
- Smartcard
- Smartcard-PKI
- Software-PKI
- Time-Sync-Token

Level
Choose a priority level for cases where there are multiple contexts.

Proxy Authentication Configuration

Proxy Authentication Configuration attributes define values for dynamic provider proxying.

Proxy Authentication

Select the check box to enable proxy authentication for a service provider.

Proxy Identity Providers List

Type an identifier for an identity provider(s) that can be used for proxy authentication in New Value and click Add. The value is a URI defined as the provider's identifier.

Maximum Number of Proxies

Enter the maximum number of identity providers that can be used for proxy authentication.

Use Introduction Cookie for Proxying

Select the check box if you want introduction cookies to be used to find the proxying identity provider.

WS-Federation Entity Provider Attributes

The WS-Federation entity provider type is based on the WS-Federation protocol. The implementation of this protocol allows single sign-on between OpenSSO Enterprise and the Microsoft Active Directory Federation Service. The WS-Federation provider entity allows you to assign and configure the following roles:

- Identity Provider
- Service Provider

WS-Federation General Attributes

The following attributes are common to both Identity and Service Provider types:

SP Display Name

This attribute defines the name the WS-Federation service provider. The default is the meta alias given at creation time.

IDP Display Name

This attribute defines the name the WS-Federation identity provider. The default is the meta alias given at creation time.

Realm

Displays the realm to which the provider belongs.

Token Issuer Name

Defines a unique identifier for the identity or service provider.

Token Issuer Endpoint

Specifies the URL at which the identity or service provider is providing WS-Federation services. For example:

```
https://demo.example.com/OpenSSO
Enterprise/WSFederationServlet/metaAlias/example
```

WS-Federation Identity Provider Customization

The following attributes apply to the WS-Federation Identity Provider role:

NameID Format

Defines the format of the name identifier component of the single sign-on response sent from the identity provider to the service provider. WS-Federation single sign-on supports the following identifier formats (default is UPN):

- Email
- Common Name
- UPN – User Principal Name. The syntax is `username@domain`, where an example of `domain`is `example.com`.

NameID Attribute

Defines the attribute in the user's profile that will be used as the name ID value. The default is `uid`.

Name Includes Domain

When using the UPN format defined in the NameID Format attribute, this specifies whether the NameID Attribute in the user's profile includes a domain. If it does, then the NameID Attribute will be used for the UPN as it is currently defined. Otherwise, it is combined with a domain to form a UPN.

Domain Attribute

When using the UPN format, if the Name Includes Domain attribute is not selected, this specifies an attribute in the user's profile to be used as the UPN domain.

UPN Domain

When using UPN format, if the Name Includes Domain attribute is not selected, and if a value for Domain Attribute is not specified, or if there is no value for that attribute for a particular user, then this attribute is used to constructing the UPN.

Signing Cert Alias

This attribute specifies the provider certificate alias used to find the assertion signing certificate in the keystore.

Claim Types

Specifies the claim type so the WS-Federation service can recognize the type of token that is exchanged between federation partners.

The EmailAddress claim type is used to identify a specific security principal by an email address.

The UPN claim type is used to identify a specific security principal via a User Principal Name.

The CommonName claim type is used to identify a security principal via a CN value consistent with X.500 naming conventions. The value of this claim is not necessarily unique and should not be used for authorization purposes.

Account Mapper

This attribute specifies the implementation of the `AccountMapper` interface used to map a remote user account to a local user account for purposes of single sign-on. The default value is `com.sun.identity.wsfed.plugins.DefaultIDPAccountMapper`.

Attribute Mapper

This defines the class used to map attributes in the assertion to user attributes defined locally by the identity provider. The default class is `com.sun.identity.wsfederation.plugins.DefaultIDPAttributeMapper`.

Attribute Map

Specifies values to define the mappings used by the default attribute mapper plug-in. Mappings should be configured in the format:

```
SAML_Assertion_Attribute_Name=User_Profile_Attribute_Name
```

For example, `EmailAddress=mail` or `Address=postaladdress`. Type the mapping as a New Value and click Add.

Assertion Effective Time

Assertions are valid for a period of time and not before or after.

`Effective Time` specifies (in seconds) the amount of time that an assertion is valid counting from the assertion's issue time. The default value is `600` seconds.

WS-Federation Service Provider Customization

The following attributes apply to the WS-Federation service provider role:

Assertion Signed

All assertions received by this service provider must be signed.

Account Mapper

This attribute specifies the implementation of the `AccountMapper` interface used to map a remote user account to a local user account for purposes of single sign-on. The default value is `com.sun.identity.wsfed.plugins.`

`DefaultADFSPartnerAccountMapper` is the default implementation.

Attribute Mapper

This defines the class used to map attributes in the assertion to user attributes defined locally by the identity provider. The default class is `com.sun.identity.wsfederation.plugins.DefaultSPAttributeMapper`.

Attribute Map

Specifies values to define the mappings used by the default attribute mapper plug-in. Mappings should be configured in the format:

SAML_attr=local-attribute

For example, `EmailAddress=mail` or `Address=postaladdress`. Type the mapping as a New Value and click Add.

Assertion Effective Time

Assertions are valid for a period of time and not before or after.

`Effective Time` specifies (in seconds) the amount of time that an assertion is valid counting from the assertion's issue time. The default value is `600` seconds.

Assertion Skew Time

Assertions are valid for a period of time and not before or after. This attribute specifies a grace period (in seconds) for the `notBefore` value. The default value is `300`. It has no relevance to the `notAfter` value.

Default Relay State

After a successful WS-Federation operation (single sign-on, single logout, or federation termination), a page is displayed. This page, generally the originally requested resource, is specified in the initiating request using the `RelayState` element. If a `RelayState` is not specified, the value of this `defaultRelayState` property is displayed.

Caution – When `RelayState` or `defaultRelayState` contains special characters (such as &), it must be URL-encoded. For example, if the value of `RelayState` is `http://www.sun.com/apps/myapp.jsp?param1=abc&param2=xyz`, it must be URL-encoded as:

```
http%3A%2F%2Fwww.sun.com%2Fapps%2Fmyapp.jsp
%3Fparam1%3Dabc%26param2%3Dxyz
```

and then appended to the URL. For example, the service provider initiated single sign-on URL would be:

```
http://host:port/deploy-uri/saml2/jsp/spSSOInit.jsp?
metaAlias=/sp&idpEntityID=http://www.idp.com&RelayState=
http%3A%2F%2Fwww.sun.com%2Fapps%2Fmyapp.jsp%3Fparam1
%3Dabc%26param2%3Dxyz
```

Home Realm Discovery

Specifies the service so that the service provider can identify the preferred identity provider. The service URL is specified as a contact endpoint by the service provider.

Account Realm Selection

Specifies the identity provider selection mechanism and configuration. Either the `cookie` or `HTTP Request` header attribute can be used to locate the identity provider.

◆ ◆ ◆ CHAPTER 7

Configuration Attributes

The Configuration page allows administrators to manage attribute values of the services that OpenSSO Enterprise offers. The attributes that comprise an OpenSSO Enterprise service are classified as one of the following types:

Global – Applied across the OpenSSO Enterprise configuration. They cannot be applied to users, roles or realms as the goal of global attributes is to customize OpenSSO Enterprise.

Realm – Realm attributes are only assigned to realms. No object classes are associated with realm attributes. For instance, attributes listed in the authentication services are defined as realm attributes because authentication is done at the realm level rather than at a subtree or user level.

Dynamic – Applies to an OpenSSO Enterprise configured role or realm. When the role is assigned to a user or a user is created in an realm, the dynamic attribute then becomes a characteristic of the user.

User – Applies directly to each user. They are not inherited from a role or an realm and, typically, are different for each user.

Note – In previous releases, many of attributes were only configurable through the `AMConfig.properties` file. This file has been deprecated, and all of its properties are now defined in the OpenSSO Enterprise console and stored in the configuration directory datastore. For information on `AMConfig.properties` for backwards compatibility for systems that have been upgraded to OpenSSO Enterprise 8.0. see the Sun Java System Access Manager 7.1 Administration Reference.

The Configuration attributes you can modify are:

- "System Properties" on page 247
- "Servers and Sites" on page 258

Authentication

OpenSSO is installed with a set of default authentication module types. An authentication module instance is a plug-in that collects user information such as a user ID and password, checks the information against entries in a database, and allows or denies access to the user. Multiple instances of the same type can be created and configured separately.

This section provides attribute descriptions that configure the default authentication module types.

- "Active Directory" on page 172
- "Anonymous" on page 177
- "Authentication Configuration" on page 178
- "Certificate" on page 178
- "Core" on page 183
- "Data Store" on page 191
- "Federation" on page 192
- "HTTP Basic" on page 192
- "JDBC" on page 193
- "LDAP" on page 196
- "Membership" on page 200
- "MSISDN" on page 201
- "RADIUS" on page 204
- "SAE" on page 206
- "SafeWord" on page 206
- "SecurID" on page 208
- "Unix" on page 209
- "Windows Desktop SSO" on page 210
- "Windows NT" on page 212

See Chapter 3, "Configuring Authentication," in *Sun OpenSSO Enterprise 8.0 Administration Guide* for more information on the authentication modules and configuring an authentication process.

Active Directory

This module type works similarly to the LDAP authentication module type, but uses the Microsoft Active Directory instead of an LDAP directory. Using this module type makes it possible to have both LDAP and Active Directory coexist under the same realm. The Active Directory authentication attributes are realm attributes. The attributes are:

Primary Active Directory Server

Specifies the host name and port number of the primary Active Directory server specified during OpenSSO Enterprise installation. This is the first server contacted for Active Directory authentication. The format is*hostname:port*. If there is no port number, assume `389`.

If you have OpenSSO Enterprise deployed with multiple domains, you can specify the communication link between specific instances of OpenSSO Enterprise and Directory Server in the following format (multiple entries must be prefixed by the local server name):

```
local_servername|server:port local_servername2|server2:port2 ...
```

For example, if you have two OpenSSO Enterprise instances deployed in different locations (L1-machine1-IS and L2- machine2-IS) communicating with different instances of Directory Server (L1-machine1-DS and L2-machine2-DS), it would look the following:

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389

L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

Secondary Active Directory Server

Specifies the host name and port number of a secondary Active Directory server available to the OpenSSO Enterprise platform. If the primary Active Directory server does not respond to a request for authentication, this server would then be contacted. If the primary server is up, OpenSSO Enterprise will switch back to the primary server. The format is also *hostname:port*. Multiple entries must be prefixed by the local server name.

Caution – When authenticating users from a Directory Server that is remote from the OpenSSO Enterprise, it is important that both the Primary and Secondary LDAP Server Ports have values. The value for one Directory Server location can be used for both fields.

DN to Start User Search

Specifies the DN of the node where the search for a user would start. (For performance reasons, this DN should be as specific as possible.) The default value is the root of the directory tree. Any valid DN will be recognized. If OBJECT is selected in the Search Scope attribute, the DN should specify one level above the level in which the profile exists. Multiple entries must be prefixed by the local server name. The format is *servername*|*search dn*.

For multiple entries:

servername1|*search dn servername2*|*search dn servername3*|*search dn* . . .

If multiple entries exist under the root organization with the same user ID, then this parameter should be set so that the only one entry can be searched for or found in order to be authenticated. For example, in the case where the agent ID and user ID is same under root org, this parameter should be `ou=Agents` for the root organization to authenticate using Agent ID and `ou=People,` for the root organization to authenticate using User ID.

DN for Root User Bind

Specifies the DN of the user that will be used to bind to the Directory Server specified in the Primary LDAP Server and Port field as administrator. The authentication service needs to bind as this DN in order to search for a matching user DN based on the user login ID. The default is `amldapuser.` Any valid DN will be recognized.

Make sure that password is correct before you logout. If it is incorrect, you will be locked out. If this should occur, you can login with the super user DN. By default, this the `amAdmin` account with which you would normally log in, although you will use the full DN. For example:

`uid_amAdmin,ou=People,`*OpenSSO-deploy-base*

Password for Root User Bind

Carries the password for the administrator profile specified in the DN for Root User Bind field. There is no default value. Only the administrator's valid Active Directory password is recognized.

Password for Root User Bind (confirm)

Confirm the password.

Attribute Used to Retrieve User Profile

Specifies the attribute used for the naming convention of user entries. By default, OpenSSO Enterprise assumes that user entries are identified by the uid attribute. If your Directory Server uses a different attribute (such as *givenname*) specify the attribute name in this field.

Attributes Used to Search for a User to be Authenticated

Lists the attributes to be used to form the search filter for a user that is to be authenticated, and allows the user to authenticate with more than one attribute in the user's entry. For example, if this field is set to *uid*, *employeenumber* , and *mail*, the user could authenticate with any of these names.

User Search Filter

Specifies an attribute to be used to find the user under the DN to Start User Search field. It works with the User Naming Attribute. There is no default value. Any valid user entry attribute will be recognized.

Search Scope

Indicates the number of levels in the Directory Server that will be searched for a matching user profile. The search begins from the node specified in DN to Start User Search. The default value is SUBTREE. One of the following choices can be selected from the list:

OBJECT	Searches only the specified node.
ONELEVEL	Searches at the level of the specified node and one level down.
SUBTREE	Search all entries at and below the specified node.

SSL Access to Active Directory Server

Enables SSL access to the Directory Server specified in the Primary and Secondary Server and Port field. By default, the box is not checked and the SSL protocol will not be used to access the Directory Server.

If the Active Directory server is running with SSL enabled (LDAPS), you must make sure that OpenSSO Enterprise is configured with proper SSL trusted certificates so that AM could connect to Directory server over LDAPS protocol

Return User DN to Authenticate

When the OpenSSO Enterprise directory is the same as the directory configured for Active Directory, this option may be enabled. If enabled, this option allows the Active Directory authentication module instance to return the DN instead of the User ID, and no search is necessary. Normally, an authentication module instance returns only the User ID, and the

authentication service searches for the user in the local OpenSSO Enterprise instance. If an external Active Directory is used, this option is typically not enabled.

Active Directory Server Check Interval

This attribute is used for Active Directory Server failback. It defines the number of minutes in which a thread will "sleep" before verifying that the primary Active Directory server is running.

User Creation Attributes

This attribute is used by the Active Directory authentication module instance when the Active Directory server is configured as an external Active Directory server. It contains a mapping of attributes between a local and an external Directory Server. This attribute has the following format:

attr1|*externalattr1*

attr2|*externalattr2*

When this attribute is populated, the values of the external attributes are read from the external Directory Server and are set for the internal Directory Server attributes. The values of the external attributes are set in the internal attributes only when the `User Profile`attribute (in the Core Authentication module type) is set to Dynamically Created and the user does not exist in local Directory Server instance. The newly created user will contain the values for internal attributes, as specified in User Creation Attributes List, with the external attribute values to which they map.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

Anonymous

This module type allows a user to log in without specifying credentials. You can create an Anonymous user so that anyone can log in as Anonymous without having to provide a password. Anonymous connections are usually customized by the OpenSSO Enterprise administrator so that Anonymous users have limited access to the server. The Anonymous authentication attributes are realm attributes. The attributes are:

Valid Anonymous Users

Contains a list of user IDs that have permission to login without providing credentials. If a user's login name matches a user ID in this list, access is granted and the session is assigned to the specified user ID.

If this list is empty, accessing the following default module instance login URL will be authenticated as the Default Anonymous User Name:

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Ano
```

If this list is not empty, accessing Default module instance login URL (same as above) will prompt the user to enter any valid Anonymous user name. If this list is not empty, the user can log in without seeing the login page by accessing the following URL:

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Ano
Anonymous username>
```

Default Anonymous User Name

Defines the user ID that a session is assigned to if Valid Anonymous User List is empty and the following default module instance login URL is accessed:

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Ano
```

The default value is anonymous. An Anonymous user must also be created in the realm.

Note – If Valid Anonymous User List is not empty, you can login without accessing the login page by using the user defined in Default Anonymous User Name. This can be done by accessing the following URL:

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymou
```
DefaultAnonymous User Name

Case Sensitive User IDs

If enabled, this option allows for case-sensitivity for user IDs. By default, this attribute is not enabled.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

Authentication Configuration

Once an authentication module instance is defined, the instance can be configured for authentication module chaining, to supply redirect URLs, and a post-processing Java class specification based on a successful or failed authentication process. Before an authentication module instance can be configured, the Core authentication attribute "Organization Authentication Configuration" on page 187 must be modified to include the specific authentication module instance name.

Certificate

This module enables a user to log in through a personal digital certificate (PDC). The module instance can require the use of the Online Certificate Status Protocol (OCSP) to determine the state of a certificate. Use of the OCSP is optional. The user is granted or denied access to a

resource based on whether or not the certificate is valid. The Certificate authentication attributes are realm attributes. The attributes are:

Match Certificate in LDAP

Specifies whether to check if the user certificate presented at login is stored in the LDAP Server. If no match is found, the user is denied access. If a match is found and no other validation is required, the user is granted access. The default is that the Certificate Authentication service does not check for the user certificate.

Note – A certificate stored in the Directory Server is not necessarily valid; it may be on the certificate revocation list. See Match Certificate to CRL. However, the web container may check the validity of the user certificate presented at login.

Subject DN Attribute Used to Search LDAP for Certificates

Specifies the attribute of the certificate's *SubjectDN* value that will be used to search LDAP for certificates. This attribute must uniquely identify a user entry. The actual value will be used for the search. The default is cn.

Match Certificate to CRL

Specifies whether to compare the user certificate against the Certificate Revocation List (CRL) in the LDAP Server. The CRL is located by one of the attribute names in the issuer's *SubjectDN*. If the certificate is on the CRL, the user is denied access; if not, the user is allowed to proceed. This attribute is, by default, not enabled.

Certificates should be revoked when the owner of the certificate has changed status and no longer has the right to use the certificate or when the private key of a certificate owner has been compromised.

Issuer DN Attribute Used to Search LDAP for CRLs

Specifies the attribute of the received certificate's issuer *subjectDN* value that will be used to search LDAP for CRLs. This field is used only when the Match Certificate to CRL attribute is enabled. The actual value will be used for the search. The default is `cn`.

HTTP Parameters for CRL Update

Specifies the HTTP parameters for obtaining a CRL from a servlet for a CRL update. Contact the administrator of your CA for these parameters.

OCSP Validation

Enables OCSP validation to be performed by contacting the corresponding OCSP responder. The OCSP responder is decided as follows during runtime. The attributes mentioned are located in the console at Configuration > Servers and Sites > Security:

- If this value is set to true and the OCSP responder is set in the "Responder URL" on page 265 attribute, the value of the attribute will be used as the OCSP responder.
- If "Online Certificate Status Protocol Check" on page 265 is enabled and if the value of this attribute is not set, the OCSP responder presented in your client certificate is used as the OCSP responder.
- If "Online Certificate Status Protocol Check" on page 265is not enabled or if "Online Certificate Status Protocol Check" on page 265is enabled and if an OCSP responder can not be found, no OCSP validation will be performed.

Before enabling OCSP Validation, make sure that the time of the OpenSSO Enterprise machine and the OCSP responder machine are in sync as close as possible. Also, the time on the OpenSSO Enterprise machine must not be behind the time on the OCSP responder. For example:

```
OCSP responder machine - 12:00:00 pm

OpenSSO Enterprise machine - 12:00:30 pm
```

LDAP Server Where Certificates are Stored

Specifies the name and port number of the LDAP server where the certificates are stored. The default value is the host name and port specified when OpenSSO Enterprise was installed. The host name and port of any LDAP Server where the certificates are stored can be used. The format is `hostname:port`.

LDAP Start Search DN

Specifies the DN of the node where the search for the user's certificate should start. There is no default value. The field will recognize any valid DN.

Multiple entries must be prefixed by the local server name. The format is as follows:

```
servername|search dn
```

For multiple entries:

```
servername1|search dn servername2|search dn servername3|search dn...
```

If multiple entries exist under the root organization with the same user ID, then this parameter should be set so that the only one entry can be searched for or found in order to be authenticated. For example, in the case where the agent ID and user ID is same under root org, this parameter should be `ou=Agents` for the root organization to authenticate using Agent ID and `ou=People,` for the root organization to authenticate using User ID.

LDAP Server Principal User

This field accepts the DN of the principal user for the LDAP server where the certificates are stored. There is no default value for this field which will recognize any valid DN. The principal user must be authorized to read, and search certificate information stored in the Directory Server.

LDAP Server Principal Password

This field carries the LDAP password associated with the user specified in the LDAP Server Principal User field. There is no default value for this field which will recognize the valid LDAP password for the specified principal user. This value is stored as readable text in the directory.

LDAP Server Principal Password (confirm)

Confirm the password.

Use SSL for LDAP Access

Specifies whether to use SSL to access the LDAP server. The default is that the Certificate Authentication service does not use SSL for LDAP access.

Certificate Field Used to Access User Profile

Specifies which field in the certificate's Subject DN should be used to search for a matching user profile. For example, if you choose email address, the certificate authentication service will search for the user profile that matches the attribute *emailAddr* in the user certificate. The user logging in then uses the matched profile. The default field is *subject CN*. The list contains:

- email address
- subject CN
- subject DN
- subject UID
- other

Other Certificate Field Used to Access User Profile

If the value of the Certificate Field Used to Access User Profile attribute is set to other, then this field specifies the attribute that will be selected from the received certificate's *subjectDN* value. The authentication service will then search the user profile that matches the value of that attribute.

SubjectAltNameExt Value Type to Access User Profile

If any value type other than `none` is selected, this attribute has precedence over `Certificate Field Used to Access User Profile` or `Other Certificate Field Used to Access User Profile`attribute.

- RFC822Name
- UPN

Trusted Remote Hosts

Defines a list of trusted hosts that can be trusted to send certificates to OpenSSO Enterprise. OpenSSO Enterprise must verify whether the certificate emanated from one of these hosts. This attribute is used for the Portal Server gateway, for a load balancer with SSL termination and for Distributed Authentication.

none	Disables the attribute. This is set by default.
all	Accepts Portal Server Gateway-style certificate authentication from any client IP address.

IP ADDR Lists the IP addresses from which to accept Portal Server Gateway-style certificate authentication requests (the IP Address of the Gateway(s)). The attribute is configurable on an realm basis.

SSL Port Number

Specifies the port number for the secure socket layer. Currently, this attribute is only used by the Gateway servlet. Before you add or change an SSL Port Number, see the "Policy-Based Resource Management" section in the OpenSSO Enterprise Administration Guide.

HTTP Header Name for Client Certificate

This attribute is used only when the Trusted Remote Hosts attribute is set to all or has a specific host name defined. The administrator must specify the http header name for the client certificate that is inserted by the load balancer or SRA.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core authentication attribute "Default Authentication Level" on page 191

Core

This module is the general configuration base for the OpenSSO Enterprise authentication services. It must be registered and configured to use any of the specific authentication module instances. It enables the administrator to define default values that will be picked up for the values that are not specifically set in the OpenSSO Enterprise default authentication modules. The Core attributes are global and realm. The attributes are:

Pluggable Authentication Module Classes

Specifies the Java classes of the available authentication modules. Takes a text string specifying the full class name (including package) of each authentication module. After writing a custom authentication module (by implementing the OpenSSO Enterprise `AMLoginModule` or the Java Authentication and Authorization Service [JAAS] `LoginModule` service provider interfaces), the new class value must be added to this property.

Supported Authentication Module for Clients

Specifies a list of authentication modules supported for a specific client. Formatted as:

clientType | *module1*,*module2*,*module3*

This attribute is read by the Client Detection Service when it is enabled.

LDAP Connection Pool Size

Specifies the minimum and maximum connection pool to be used on a specific LDAP server and port. Formatted as:

host:*port*:*min*:*max*

This attribute is for LDAP and Membership authentication services only.

Note – This connection pool is different than the SDK connection pool configured in `serverconfig.xml`.

Default LDAP Connection Pool Size

Sets the default minimum and maximum connection pool to be used with all LDAP authentication module configurations. Formatted as:

min:*max*

This value is superseded by a value defined for a specific host and port in the LDAP Connection Pool Size property.

User Profile

This option determines the profile status of a successfully authenticated user.

Dynamic	Specifies that on successful authentication the Authentication Service will create a user profile if one does not already exist. The `SSOToken` will then be issued. The user profile is created in the realm's configured user data store.
Dynamic With User Alias	Specifies that on successful authentication the Authentication Service will create a user profile that contains the User Alias List attribute which defines one or more aliases that for mapping a user's multiple profiles.
Ignore	Specifies that a user profile is not required for the Authentication Service to issue an `SSOToken` after a successful authentication.
Required	Specifies that on successful authentication the user must have a user profile in the realm's configured user data store in order for the Authentication Service to issue an `SSOToken`.

Remote Auth Security

Requires that OpenSSO Enterprise validate the identity of the calling application; thus all remote authentication requests require the calling application's `SSOToken`. This allows the Authentication Service to obtain the username and password associated with the application.

Administrator Authentication Configuration

Defines the authentication chain used by administrators when the process needs to be different from the authentication chain defined for end users. The authentication chain must first be created before it is displayed as an option in this attribute's drop down list.

User Profile Dynamic Creation Default Roles

Specifies the Distinguished Name (DN) of a role to be assigned to a new user whose profile is created when either of the Dynamic options is selected under the User Profile attribute. There are no default values. The role specified must be within the realm for which the authentication process is configured.

Tip – This role can be either an OpenSSO Enterprise or LDAP role, but it cannot be a filtered role. If you wish to automatically assign specific services to the user, you have to configure the Required Services attribute in the User Profile.

Persistent Cookie Mode

Determines whether users can return to their authenticated session after restarting the browser. When enabled, a user session will not expire until its *persistent* cookie expires (as specified by the value of the Persistent Cookie Maximum Time attribute), or the user explicitly logs out. By default, the Authentication Service uses only *memory* cookies (expires when the browser is closed).

Tip – A persistent cookie must be explicitly requested by the client by appending the `iPSPCookie=yes` parameter to the login URL.

Persistent Cookie Maximum Time

Specifies the interval after which a persistent cookie expires. The interval begins when the user's session is successfully authenticated. The maximum value is 2147483647 (time in seconds). The field will accept any integer value less than the maximum.

Alias Search Attribute Name

After a user is successfully authenticated, the user's profile is retrieved. This field specifies a second LDAP attribute to use in a search for the profile if a search using the first LDAP attribute fails to locate a matching user profile. Primarily, this attribute will be used when the user identification returned from an authentication module is not the same as that specified in User Naming Attribute. For example, a RADIUS server might return `abc1234` but the user name is `abc`. There is no default value for this attribute. The field takes any valid LDAP attribute.

Default Authentication Locale

Specifies the default language subtype to be used by the Authentication Service. The default value is `en_US`. See Supported Language Locales for a listing of valid language subtypes. To use a different locale, authentication templates for that locale must first be created. A new directory must then be created for these templates. See "Supported Language Locales" on page 218 for a listing of valid language subtypes.

Organization Authentication Configuration

Defines the default authentication chain used by the realm's users. The authentication chain must first be created before it is displayed as an option in this attribute's drop down list.

Login Failure Lockout Mode

Selecting this attribute enables a *physical lockout*. Physical lockout will inactivate an LDAP attribute (defined in the Lockout Attribute Name property) in the user's profile. This attribute works in conjunction with several other lockout and notification attributes.

Login Failure Lockout Count

Defines the number of attempts that a user has to authenticate, within the time interval defined in Login Failure Lockout Interval, before being locked out.

Login Failure Lockout Interval

Defines (in minutes) the time in which failed login attempts are counted. If one failed login attempt is followed by a second failed attempt, within this defined lockout interval time, the lockout count is begun and the user will be locked out if the number of attempts reaches the number defined in Login Failure Lockout Count. If an attempt within the defined lockout interval time proves successful before the number of attempts reaches the number defined in Login Failure Lockout Count, the lockout count is reset.

Email Address to Send Lockout Notification

Specify one (or more) email address(es) to which notification will be sent if a user lockout occurs. If sending:

- To multiple addresses, separate each address with a space.
- To non-English locales, format the address as *email_address*|*locale*|*charset*.

Warn User After N Failures

Specifies the number of authentication failures that can occur before OpenSSO Enterprise displays a warning message that the user will be locked out.

Login Failure Lockout Duration

Defines (in minutes) how long a user must wait after a lockout before attempting to authenticate again. Entering a value greater than 0, enables memory lockout and disables physical lockout. Memory lockout is when the user's account is locked in memory for the number of minutes specified. The account is unlocked after the time period has passed.

Lockout Duration Multiplier

Defines a value with which to multiply the value of the Login Failure Lockout Duration attribute for each successive lockout. For example, if Login Failure Lockout Duration is set to 3 minutes, and the Lockout Duration Multiplier is set to 2, the user will be locked out of the account for 6 minutes. Once the 6 minutes has elapsed, if the user again provides the wrong credentials, the lockout duration would then be 12 minutes. With the Lockout Duration Multiplier, the lockout duration is incrementally increased based on the number of times the user has been locked out.

Lockout Attribute Name

Defines the LDAP attribute used for physical lockout. The default value is `inetuserstatus` (although the field in the OpenSSO Enterprise console is empty). The Lockout Attribute Value field must also contain an appropriate value.

Lockout Attribute Value

Specifies the action to take on the attribute defined in Lockout Attribute Name. The default value is `inactive` (although the field in the OpenSSO Enterprise console is empty). The Lockout Attribute Name field must also contain an appropriate value.

Default Success Login URL

Accepts a list of values that specifies where users are directed after successful authentication. The format of this attribute is *client-type*|*URL* although the only value you can specify at this time is a URL which assumes the type HTML. The default value is `/opensso/console`. Values that don't specify HTTP or HTTP(s) will be appended to the deployment URI.

Default Failure Login URL

Accepts a list of values that specifies where users are directed after an attempted authentication has failed. The format of this attribute is *client-type*|*URL* although the only value you can specify at this time is a URL which assumes the type HTML. Values that don't specify HTTP or HTTP(s) will be appended to the deployment URI.

Authentication Post Processing Class

Specifies one or more Java classes used to customize post authentication processes for successful or unsuccessful logins. The Java class must implement the `com.sun.identity.authentication.spi.AMPostAuthProcessInterface` OpenSSO Enterprise interface. Additionally, add a JAR containing the post processing class to the classpath of the web container instance on which OpenSSO Enterprise is configured. If the web container on which OpenSSO Enterprise is configured explodes the WAR follow this procedure.

1. Stop the web container instance.
2. Change to the `WEB-INF/lib` directory in the exploded OpenSSO Enterprise WAR directory.

   For example, if using Sun Application Server, *AS=Deploy=BaseAS=Domain-Dir/AS-Domain*`/applications/j2ee-modules/opensso/WEB-INF/l`
3. Copy the JAR that contains the post processing class to the `lib` directory.
4. Restart the web container instance.

Generate UserID Mode

When enabled, the Membership module will generate a list of alternate user identifiers if the one entered by a user during the self-registration process is not valid or already exists. The user identifiers are generated by the class specified in the Pluggable User Name Generator Class property.

Pluggable User Name Generator Class

Specifies the name of the class used to generate alternate user identifiers when Generate UserID Mode is enabled. The default value is `com.sun.identity.authentication.spi.DefaultUserIDGenerator`.

Identity Types

Lists the type or types of identities for which OpenSSO Enterprise will search. Options include:

- Agent
- agentgroup
- agentonly
- Group
- User

Pluggable User Status Event Classes

Specifies one or more Java classes used to provide a callback mechanism for user status changes during the authentication process. The Java class must implement the `com.sun.identity.authentication.spi.AMAuthCallBack` OpenSSO Enterprise interface. Account lockout and password changes are supported — the latter through the LDAP authentication module as the feature is only available for the module.

Store Invalid Attempts in Data Store

Enables the storage of information regarding failed authentication attempts as the value of the `sunAMAuthInvalidAttemptsData` attribute in the user data store. In order to store data in this attribute, the OpenSSO Enterprise schema has to be loaded. Information stored includes number of invalid attempts, time of last failed attempt, lockout time and lockout duration. Storing this information in the identity repository allows it to be shared among multiple instances of OpenSSO Enterprise.

Module-based Authentication

Enables users to authenticate using module-based authentication. Otherwise, all attempts at authentication using the **`module=`***module-instance-name* login parameter will result in failure.

User Attribute Mapping to Session Attribute

Enables the authenticating user's identity attributes (stored in the identity repository) to be set as session properties in the user's `SSOToken`. The value takes the format *User-Profile-Attribute*`|`*Session-Attribute-Name*. If *Session-Attribute-Name* is not specified, the value of *User-Profile-Attribute* is used. All session attributes contain the `am.protected` prefix to ensure that they cannot be edited by the Client SDK.

For example, if you define the user profile attribute as `mail` and the user's email address (available in the user session) as `user.mail`, the entry for this attribute would be `mail|user.mail`. After a successful authentication, the `SSOToken.getProperty(`*String*`)` method is used to retrieve the user profile attribute set in the session. The user's email address is

retrieved from the user's session using the `SSOToken.getProperty("am.protected.user.mail")` method call.

Properties that are set in the user session using User Attribute Mapping to Session Attributes can not be modified (for example, `SSOToken.setProperty(`*String, String*`)`). This will result in an `SSOException`. Multi-value attributes, such as `memberOf`, are listed as a single session variable separated by the pipe symbol. For example, *Value1*|*Value2*|*Value3*

Default Authentication Level

The authentication level value indicates how much to trust authentications. Once a user has authenticated, this value is stored in the user's `SSOToken`. When the `SSOToken` is presented to an application, the application can use the stored value to determine whether the level is sufficient to grant the user access. If the authentication level does not meet the minimum value required by the application, it can prompt the user to authenticate again in order to attain a higher authentication level. The authentication level should be set within a realm's specific authentication template. The Default Authentication Level value described here will apply only when no authentication level has been specified in the Authentication Level field for a specific realm's authentication template. The Default Authentication Level default value is 0. The value of this attribute is not used by OpenSSO Enterprise but by any external application that may chose to use it.

Data Store

The Data Store authentication module allows a login using the Identity Repository of the realm to authenticate users. Using the Data Store module removes the requirement to write an authentication plug- in module, load, and then configure the authentication module if you need to authenticate against the same data store repository. Additionally, you do not need to write a custom authentication module where flat-file authentication is needed for the corresponding repository in that realm.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

Federation

The Federation authentication module is used by a service provider to create a user session after validating single sign-on protocol messages. This authentication module is used by the SAML, SAMLv2, ID-FF, and WS-Federation protocols.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

HTTP Basic

The HTTP authentication module allows a login using the HTTP basic authentication with no data encryption. A user name and password are requested through the use of a web browser. Credentials are validated internally using any LDAP or Data Store authentication module to verify the user's credentials.

Backend Module Name

Specifies the authentication module used to validate the credentials.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not

meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

JDBC

The Java Database Connectivity (JDBC) authentication module allows OpenSSO Enterprise to authenticate users through any Structured Query Language (SQL) databases that provide JDBC-enabled drivers. The connection to the SQL database can be either directly through a JDBC driver or through a JNDI connection pool. The JDBC attributes are realm attributes. The attributes are:

Connection Type

Specifies the connection type to the SQL database, using either a JNDI (Java Naming and Directory Interface) connection pool or JDBC driver. The options are:

- Connection pool is retrieved via JNDI
- Non-persistent JDBC connection

The JNDI connection pool utilizes the configuration from the underlying web container.

Connection Pool JNDI Name

If JNDI is selected in Connection Type, this field specifies the connection pool name. Because JDBC authentication uses the JNDI connection pool provided by the web container, the setup of JNDI connection pool may not be consistent among other web containers. See the OpenSSO Enterprise Administration Guide for examples

JDBC Driver

If JDBC is selected in Connection Type, this field specifies the JDBC driver provided by the SQL database. For example, `com.mysql.jdbc.Driver`. The class specified by JDBC Driver must be accessible to the web container instance on which OpenSSO has been deployed and configured. Include the .jar file that contains the JDBC driver class in the *OpenSSO-deploy-base*`/WEB-INF/lib` directory.

JDBC URL

Specifies the database URL if JDBC is select in Connection Type. For example, the URL for mySQL is `jdbc.mysql://hostname:port/databaseName`.

Connect This User to Database

Specifies the user name from whom the database connection is made for the JDBC connection.

Password for Connecting to Database

Defines the password for the user specified in User to Connect to Database.

Password for Connecting to Database Confirm

Confirm the password.

Password Column String

Specifies the password column name in the SQL database.

Prepared Statement

Specifies the SQL statement that retrieves the password of the user that is logging in. For example:

```
select Password from Employees where USERNAME = ?
```

Class to Transform Password Syntax

Specifies the class name that transforms the password retrieved from the database, to the format of the user input, for password comparison. This class must implement the `JDBCPasswordSyntaxTransform` interface.

By default, the value of this attribute is `com.sun.identity.authentication.modules.jdbc.ClearTextTransform` which expects the password to be in clear text.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

▼ To Configure a Connection Pool — Example

The following example shows how to set up a connection pool for Web Server and MySQL 4.0:

1 In the Web Server console, create a JDBC connection pool with the following attributes:

poolName	`samplePool`
DataSource Classname	`com.mysql.jdbc.jdbc2.optional.MysqlDatacSource`
serverName	Server name of the mySQL server.
port	Port number on which mySQL server is running.
user	User name of the database password.
password	The password of the user.
databaseName	The name of the database.

Note – The jar file which contain the *DataSource* class and the JDBC Driver class mentioned in the following steps should be added to the application class path

---

2 Configure the JDBC Resources. In the Web Server console, create a JDBC resource with the following attributes:

JNDI name	*jdbc/samplePool*
Pool name	*samplePool*
Data Resource Enabled	*on*

3 Add the following lines to the `sun-web.xml` file of the application:

```
<resource-ref>
      <res-ref-name>jdbc/mySQL</res-ref-name>
```

```
      <jndi-name>jdbc/samplePool</jndi-name>
</resource-ref>
```

4 **Add the following lines to the web.xml file of the application:**

```
<resource-ref>
       <description>mySQL Database</description>
       <res-ref-name>jdbc/mySQL</res-ref-name>
       <res-type>javax.sql.DataSource</res-type>
       <res-auth>Container</res-auth>
</resource-ref>
```

5 **Once you have completed the settings the value for this attribute is becomes** *java:comp/env/jdbc/mySQL*.

LDAP

This module enables authentication using LDAP bind, a Directory Server operation which associates a user ID password with a particular LDAP entry. You can define multiple LDAP authentication configurations for a realm. The LDAP authentication attributes are realm attributes. The attributes are:

Primary LDAP Server

Specifies the host name and port number of the primary LDAP server specified during OpenSSO Enterprise installation. This is the first server contacted for authentication. The format is*hostname:port*. If there is no port number, assume 389.

If you have OpenSSO Enterprise deployed with multiple domains, you can specify the communication link between specific instances of OpenSSO Enterprise and Directory Server in the following format (multiple entries must be prefixed by the local server name):

```
local_servername|server:port local_servername2|server2:port2 ...
```

For example, if you have two OpenSSO Enterprise instances deployed in different locations (L1-machine1-IS and L2- machine2-IS) communicating with different instances of Directory Server (L1-machine1-DS and L2-machine2-DS), it would look the following:

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389

L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

Secondary LDAP Server

Specifies the host name and port number of a secondary LDAP server available to the OpenSSO Enterprise platform. If the primary LDAP server does not respond to a request for authentication, this server would then be contacted. If the primary server is up, OpenSSO Enterprise will switch back to the primary server. The format is also *hostname:port*. Multiple entries must be prefixed by the local server name.

Caution – When authenticating users from a Directory Server that is remote from the OpenSSO Enterprise, it is important that both the Primary and Secondary LDAP Server Ports have values. The value for one Directory Server location can be used for both fields.

DN to Start User Search

Specifies the DN of the node where the search for a user would start. (For performance reasons, this DN should be as specific as possible.) The default value is the root of the directory tree. Any valid DN will be recognized. If OBJECT is selected in the Search Scope attribute, the DN should specify one level above the level in which the profile exists. Multiple entries must be prefixed by the local server name. The format is *servername*|*search dn*.

For multiple entries:

servername1|*search dn servername2*|*search dn servername3*|*search dn* . . .

If multiple entries exist under the root organization with the same user ID, then this parameter should be set so that the only one entry can be searched for or found in order to be authenticated. For example, in the case where the agent ID and user ID is same under root org, this parameter should be `ou=Agents` for the root organization to authenticate using Agent ID and `ou=People,` for the root organization to authenticate using User ID.

DN for Root User Bind

Specifies the DN of the user that will be used to bind to the Directory Server specified in the Primary LDAP Server and Port field as administrator. The authentication service needs to bind as this DN in order to search for a matching user DN based on the user login ID. The default is `amldapuser`. Any valid DN will be recognized.

Password for Root User Bind

Carries the password for the administrator profile specified in the DN for Root User Bind field. There is no default value. Only the administrator's valid LDAP password will be recognized.

Password for Root User Bind (confirm)

Confirm the password.

Attribute Used to Retrieve User Profile

Specifies the attribute used for the naming convention of user entries. By default, OpenSSO Enterprise assumes that user entries are identified by the uid attribute. If your Directory Server uses a different attribute (such as *givenname*) specify the attribute name in this field.

Attributes Used to Search for a User to be Authenticated

Lists the attributes to be used to form the search filter for a user that is to be authenticated, and allows the user to authenticate with more than one attribute in the user's entry. For example, if this field is set to *uid*, *employeenumber* , and *mail*, the user could authenticate with any of these names. These attributes must be set separately.

User Search Filter

Specifies an attribute to be used to find the user under the DN to Start User Search field. It works with the User Naming Attribute. There is no default value. Any valid user entry attribute will be recognized.

Search Scope

Indicates the number of levels in the Directory Server that will be searched for a matching user profile. The search begins from the node specified in the DN to Start User Search attribute. The default value is SUBTREE. One of the following choices can be selected from the list:

OBJECT	Searches only the specified node.
ONELEVEL	Searches at the level of the specified node and one level down.
SUBTREE	Search all entries at and below the specified node.

SSL to Access LDAP Server

Enables SSL access to the Directory Server specified in the Primary and Secondary LDAP Server and Port field. By default, the box is not checked and the SSL protocol will not be used to access the Directory Server.

If the LDAP Server is running with SSL enabled (LDAPS), you must make sure that OpenSSO Enterprise is configured with proper SSL trusted certificates so that AM could connect to Directory server over LDAPS protocol

Return User DN to Authenticate

When the OpenSSO Enterprise directory is the same as the directory configured for LDAP, this option may be enabled. If enabled, this option allows the LDAP authentication module to return the DN instead of the User ID, and no search is necessary. Normally, an authentication module returns only the User ID, and the authentication service searches for the user in the local OpenSSO Enterprise LDAP. If an external LDAP directory is used, this option is typically not enabled.

LDAP Server Check Interval

This attribute is used for LDAP Server failback. It defines the number of minutes in which a thread will "sleep" before verifying that the LDAP primary server is running.

User Creation Attribute List

This attribute is used by the LDAP authentication module when the LDAP server is configured as an external LDAP server. It contains a mapping of attributes between a local and an external Directory Server. This attribute has the following format:

attr1|*externalattr1*

attr2|*externalattr2*

When this attribute is populated, the values of the external attributes are read from the external Directory Server and are set for the internal Directory Server attributes. The values of the external attributes are set in the internal attributes only when the `User Profile`attribute (in the Core Authentication module) is set to Dynamically Created and the user does not exist in local Directory Server instance. The newly created user will contain the values for internal attributes, as specified in User Creation Attributes List, with the external attribute values to which they map.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is

stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

Membership

The Membership Authentication module is implemented for personalized sites that allow a user to self-register. This means the user can create an account, personalize it, and access it as a registered user without the help of an administrator. The attributes are realm attributes. The attributes are:

Minimum Password Length

Specifies the minimum number of characters required for a password set during self-registration. The default value is 8.

Default User Roles

Specifies the roles assigned to new users whose profiles are created through self-registration. There is no default value. The administrator must specify the DNs of the roles that will be assigned to the new user.

Note – The role specified must be under the realm for which authentication is being configured. Only the roles that can be assigned to the user will be added during self-registration. All other DNs will be ignored. The role can be either an OpenSSO Enterprise role or an LDAP role, but filtered roles are not accepted.

User Status After Registration

Specifies whether services are immediately made available to a user who has self-registered. The default value is Active and services are available to the new user. By selecting Inactive, the administrator chooses to make no services available to a new user.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

MSISDN

The Mobile Station Integrated Services Digital Network (MSISDN) authentication module enables authentication using a mobile subscriber ISDN associated with a device such as a cellular telephone. It is a non-interactive module. The module retrieves the subscriber ISDN and validates it against the Directory Server to find a user that matches the number. The MSISDN Authentication attributes are realm attributes. The MSISDN Authentication attributes are:

Trusted Gateway IP Address

Specifies a list of IP addresses of trusted clients that can access MSIDSN modules. You can set the IP addresses of all clients allows to access the MSISDN module by entering the address (for example, `123.234.123.111`) in the entry field and clicking Add. By default, the list is empty. If the attribute is left empty, then all clients are allowed. If you specify none, no clients are allowed.

MSISDN Number Argument

Specifies a list of parameter names that identify which parameters to search in the request header or cookie header for the MSISDN number. For example, if you define *x-Cookie-Param*, *AM_NUMBER*, and *COOKIE-ID*, the MSISDN authentication services will search those parameters for the MSISDN number.

LDAP Server and Port

Specifies the host name and port number of the Directory Server in which the search will occur for the users with MSISDN numbers. The format is*hostname:port*. If there is no port number, assume `389`.

If you have OpenSSO Enterprise deployed with multiple domains, you can specify the communication link between specific instances of OpenSSO Enterprise and Directory Server in the following format (multiple entries must be prefixed by the local server name):

```
local_servername|server:port local_servername2|server2:port2 ...
```

For example, if you have two OpenSSO Enterprise instances deployed in different locations (L1-machine1-IS and L2- machine2-IS) communicating with different instances of Directory Server (L1-machine1-DS and L2-machine2-DS), it would look the following:

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389
```

```
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

LDAP Start Search DN

Specifies the DN of the node where the search for the user's MSISDN number should start. There is no default value. The field will recognize any valid DN. Multiple entries must be prefixed by the local server name. The format is *servername*|*search dn*.

For multiple entries:

servername1|*search dn servername2*|*search dn servername3*|*search dn* . . .

If multiple entries exist under the root organization with the same user ID, then this parameter should be set so that the only one entry can be searched for or found in order to be authenticated. For example, in the case where the agent ID and user ID is same under root org, this parameter should be `ou=Agents` for the root organization to authenticate using Agent ID and `ou=People,` for the root organization to authenticate using User ID.

Attribute To Use To Search LDAP

Specifies the name of the attribute in the user's profile that contains the MSISDN number to search for a particular user. The default value is *sunIdentityMSISDNNumber*. This value should not be changed, unless you are certain that another attribute in the user's profile contains the same MSISDN number.

LDAP Server Principal User

Specifies the LDAP bind DN to allow MSISDN searches in the Directory Server. The default bind DN is `cn=amldapuser,ou=DSAME Users,dc=sun,dc=com`.

LDAP Server Principal Password

Specifies the LDAP bind password for the bind DN, as defined in LDAP Server Principal User.

LDAP Server Principal Password (confirm)

Confirm the password.

SSL for LDAP Access

Enables SSL access to the Directory Server specified in the LDAP Server and Port attribute. By default, this is not enabled and the SSL protocol will not be used to access the Directory Server. However, if this attribute is enabled, you can bind to a non-SSL server.

MSISDN Header Search Attribute

Specifies the headers to use for searching the request for the MSISDN number. The supported values are as follows:

Cookie Header	Performs the search in the cookie.
RequestHeader	Performs the search in the request header.
RequestParameter	Performs the search in the request parameter. By default, all options are selected.

LDAP Attribute Used to Retrieve User Profile

Specifies the LDAP attribute that is used during a search to return the user profile for MSISDN authentication service. The default is `uid`.

Return User DN on Authentication

When the OpenSSO Enterprise directory is the same as the directory configured for MSISDN, this option may be enabled. If enabled, this option allows the authentication module to return

the DN instead of the User ID, and no search is necessary. Normally, an authentication module returns only the User ID, and the authentication service searches for the user in the local OpenSSO Enterprise. If an external directory is used, this option is typically not enabled.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

RADIUS

This module allows for authentication using an external Remote Authentication Dial-In User Service (RADIUS) server. The RADIUS Authentication attributes are realm attributes. The attributes are:

Server 1

Displays the IP address or fully qualified host name of the primary RADIUS server. The default IP address is 127.0.0.1. The field will recognize any valid IP address or host name. Multiple entries must be prefixed by the local server name as in the following syntax:

```
local_servername|ip_address local_servername2|ip_address ...
```

Server 2

Displays the IP address or fully qualified domain name (FQDN) of the secondary RADIUS server. It is a failover server which will be contacted if the primary server could not be contacted. The default IP address is 127.0.0.1. Multiple entries must be prefixed by the local server name as in the following syntax:

```
local_servername|ip_address local_servername2|ip_address ...
```

Shared Secret

Carries the shared secret for RADIUS authentication. The shared secret should have the same qualifications as a well-chosen password. There is no default value for this field.

Shared Secret Confirm

Confirmation of the shared secret for RADIUS authentication.

Port Number

Specifies the port on which the RADIUS server is listening. The default value is 1645.

Timeout

Specifies the time interval in seconds to wait for the RADIUS server to respond before a timeout. The default value is 3 seconds. It will recognize any number specifying the timeout in seconds.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

SAE

The Secure Attribute Exchange (SAE) authentication module is used when a external entity (such as an existing application) has already authenticated the user and wishes to securely inform a local OpenSSO Enterprise instance about the authentication to trigger the creation of a OpenSSO Enterprise session for the user. The SAE authentication module is also used by the Virtual Federation functionality where the existing entity instructs the local OpenSSO Enterprise instance to use federation protocols to transfer authentication and attribute information to a partner application. The SAE attribute is a realm attribute.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

SafeWord

This module allows for users to authenticate using Secure Computing's SafeWord or SafeWord PremierAccess authentication servers. The SafeWord Authentication Attributes are realm attributes. The attributes are:

Server

Specifies the SafeWord or SafeWord PremiereAccess server name and port. Port 7482 is set as the default for a SafeWord server. The default port number for a SafeWord PremierAccess server is 5030.

Server Verification Files Directory

Specifies the directory into which the SafeWord client library places its verification files. The default is as follows:

ConfigurationDirectory`/`*uri*`/auth/safeword/serverVerification`

If a different directory is specified in this field, the directory must exist before attempting SafeWord authentication.

Logging

Enables SafeWord logging. By default, SafeWord logging is enabled.

Logging Level

Specifies the SafeWord logging level. Select a level in the Drop-down menu. The levels are DEBUG, ERROR, INFO and NONE .

Log File

Specifies the directory path and log file name for SafeWord client logging. The default path is*ConfigurationDirectory*`/`*uri*`/auth/safeword/safe.log` .

If a different path or filename is specified, it must exist before attempting SafeWord authentication. If more than one realm is configured for SafeWord authentication, and different SafeWord servers are used, then different paths must be specified or only the first realm where SafeWord authentication occurs will work. Likewise, if a realm changes SafeWord servers, the `swec.dat` file in the specified directory must be deleted before authentications to the newly configured SafeWord server will work.

Authentication Connection Timeout

Defines the timeout period (in seconds) between the SafeWord client (OpenSSO Enterprise) and the SafeWord server. The default is 120 seconds.

Client Type

Defines the Client Type that the SafeWord server uses to communicate with different clients, such as Mobile Client, VPN, Fixed Password, Challenge/Response, and so forth.

EASSP Version

This attribute specifies the Extended Authentication and Single Sign-on Protocol (EASSP) version. This field accepts either the standard (101), SSL-encrypted premier access (200), or premier access (201) protocol versions.

Minimum Authenticator Strength

Defines the minimum authenticator strength for the client/SafeWord server authentication. Each client type has a different authenticator value, and the higher the value, the higher the authenticator strength. 20 is the highest value possible. 0 is the lowest value possible.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

SecurID

This module allows for authentication using RSA (a division of EMC) ACE/Server software and RSA SecurID authenticators. For this release of OpenSSO Enterprise, the SecurID Authentication module is available for Solaris/SPARC, Solaris/x86, Linux, and Windows platforms supported by OpenSSO Enterprise. The SecurID authentication attributes are realm attributes. The attributes are:

ACE/Server Configuration Path

Specifies the directory in which the SecurID ACE/Server `sdconf.rec` file is located, by default in *ConfiugrationDirectory*`/`*uri*`/auth/ace/data` If you specify a different directory in this field, the directory must exist before attempting SecurID authentication.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is

stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

Unix

This module allows for authentication using a user's Unix identification and password. If any of the Unix authentication attributes are modified, both OpenSSO Enterprise and the amunixd helper must be restarted. For more information on starting the `amunixid` helper, see "Running the Unix Authentication Helper (amunixd Daemon)" in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*. This authentication module is supported on Solaris and Linux. The Unix authentication attributes are:

Configuration Port

This attribute specifies the port to which the Unix Helper 'listens' upon startup for the configuration information contained in the UNIX Helper Authentication Port, Unix Helper Timeout, and Unix Helper Threads attributes. The default is 58946.

Authentication Port

This attribute specifies the port to which the Unix Helper 'listens' for authentication requests after configuration. The default port is 57946.

Timeout

This attribute specifies the number of minutes that users have to complete authentication. If users surpass the allotted time, authentication automatically fails. The default time is set to 3 minutes.

Threads

This attribute specifies the maximum number of permitted simultaneous Unix authentication sessions. If the maximum is reached at a given moment, subsequent authentication attempts are not allowed until a session is freed up. The default is set to 5.

Authentication Level

This is a realm attribute. The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

PAM Service Name

This is a realm attribute. It defines the PAM (Pluggable Authentication Module) configuration or stack that is shipped for you operating system and is used for Unix authentication. For Solaris, the name is defaulted to `other` and for Linux, the name is `password`.

For more information on PAM, please consult the documentation for your system. For Solaris, see `pam.conf(4)` and for Linux, see the PAM files in `/etc/pam.d`.

Windows Desktop SSO

This module is specific to Windows and is also known as Kerberos authentication. The user presents a Kerberos token to OpenSSO Enterprise through the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) protocol. The Windows Desktop SSO authentication plug-in module provides a client (user) with desktop single sign-on. This means that a user who has already authenticated with a key distribution center can be authenticated with OpenSSO Enterprise without having to provide the login information again. The Windows Desktop SSO attributes are global attributes. The attributes are:

- "Service Principal" on page 211
- "Keytab File Name" on page 211
- "Kerberos Realm" on page 211
- "Kerberos Server Name" on page 211

Service Principal

Specifies the Kerberos principal that is used for authentication. Use the following format:

HTTP/*hostname.domainname@dc_domain_name*

hostname and *domainame* represent the hostname and domain name of the OpenSSO Enterprise instance. *dc_domain_name* is the Kerberos domain in which the Windows Kerberos server (domain controller) resides. It is possibly different from the domain name of the OpenSSO Enterprise.

Keytab File Name

This attribute specifies the Kerberos keytab file that is used for authentication and takes the absolute path to the keytab file.

Kerberos Realm

This attribute specifies the Kerberos Distribution Center (domain controller) domain name. Depending up on your configuration, the domain name of the domain controller may be different than the OpenSSO Enterprise domain name.

Kerberos Server Name

This attribute specifies the Kerberos Distribution Center (the domain controller) hostname. You must enter the fully qualified domain name (FQDN) of the domain controller.

Return Principal with Domain Name

If enabled, this attributes allows OpenSSO Enterprise to automatically return the Kerberos principal with the domain controller's domain name during authentication.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

Windows NT

The Windows NT Authentication module allows for authentication against a Microsoft Windows NT server. The attributes are realm attributes. The values applied to them under Service Configuration become the default values for the Windows NT Authentication template. The service template needs to be created after registering the service for the realm. The default values can be changed after registration by the realm's administrator. Realm attributes are not inherited by entries in the subtrees of the realm.

In order to activate the Widows NT Authentication module, Samba Client 2.2.2 or 3.x must be downloaded and installed to the following directory:

ConfigurationDirectory/*uri*/`bin`

The Samba Client is a file and print server for blending Windows and UNIX machines without requiring a separate Windows NT/2000 Server.

Red Hat Linux ships with a Samba client, located in the`/usr/bin` directory.

In order to authenticate using the Windows NT Authentication service for Linux, copy the client binary to`/bin`.

The Windows NT attributes are:

- "Authentication Domain" on page 212
- "Authentication Host" on page 212
- "Samba Configuration File Name" on page 213
- "Authentication Level" on page 213

Authentication Domain

Defines the Domain name to which the user belongs.

Authentication Host

Defines the Windows NT authentication hostname. The hostname should be the netBIOS name, as opposed to the fully qualified domain name (FQDN). By default, the first part of the FQDN is the netBIOS name.

If the DHCP (Dynamic Host Configuration Protocol) is used, you would put a suitable entry in the HOSTS file on the Windows 2000 machine.

Name resolution will be performed based on the netBIOS name. If you do not have any server on your subnet supplying netBIOS name resolution, the mappings should be hardcoded. For example, the hostname should be `example1` not `example1.company1.com`.

Samba Configuration File Name

Defines the Samba configuration filename and supports the `-s` option in the `smbclient` command. The value must be the full directory path where the Samba configuration file is located.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 191.

Console Properties

The Console properties contain services that enable you to configure the OpenSSO Enterprise console and to define console properties for different locales and character sets. The Console properties contain the following:

Administration

The Administration service enables you to configure the OpenSSO Enterprise console at both the global level as well as at a configured realm level (Preferences or Options specific to a configured realm). The Administration service attributes are global and realm attributes.

Note – If you have upgraded to OpenSSO Enterprise 8.0 and are running in legacy mode, a large number attributes will be displayed in the console. The complete list of attributes and their descriptions are listed in the OpenSSO Enterprise 8.0 online help and in the Sun Java System Access Manager 7.1 Administration Reference (`http://docs.sun.com/app/docs/coll/1292.2`).

The attributes are:

Federation Management

Enables Federation Management. It is selected by default. To disable this feature, deselect the field The Federation Management tab will not appear in the console.

Default Agents Container

Specifies the default agent container into which the agent is created. The default is `Agents`.

Maximum Results Returned From Search

This field defines the maximum number of results returned from a search. The default value is 100.

Do not set this attribute to a large value (greater than 1000) unless sufficient system resources are allocated.

Note – OpenSSO Enterprise is preconfigured to return a maximum size of 4000 search entries. This value can be changed through the console or by using `ldapmodify`. If you wish to change it using `ldapmodify`, create a `newConfig.xml`, with the following values (in this example, `nsSizeLimit`: -1 means unlimited):

```
dn: cn=puser,ou=DSAME Users,ORG_ROOT_SUFFIX
changetype: modify
replace:nsSizeLimit
nsSizeLimit: -1
```

Then, run `ldapmodify`. For example:

```
setenv LD_LIBRARY_PATH /opt/SUNWam/lib/:
/opt/SUNWam/ldaplib/ldapsdk:/usr/lib/mps:/usr/share/lib/mps/secv1:/usr/lib/mps/secv1:
$LD_LIBRARY_PATH

./ldapmodify -D "cn=Directory Manager" -w "iplanet333" -c -a
-h hostname.domain -p 389 -f  newConfig.xml
```

Modifications to this attribute done through `LDAPModify` will take precedence to those made through the OpenSSO Enterprise Console.

Timeout For Search

Defines the amount of time (in number of seconds) that a search will continue before timing out. It is used to stop potentially long searches. After the maximum search time is reached, the search terminates and returns an error. The default is 5 seconds.

Note – Directory Server is been preconfigured with a timeout value of 120 seconds. This value can be changed through the Directory Server console or by using `ldapmodify`. If you wish to change it using `ldapmodify`, create a `newConfig.xml`, with the following values (this example changes the timeout from 120 seconds to 3600 seconds):

```
dn: cn=config
changetype: modify
replace:nsslapd-timelimit
nsslapd-timelimit: 3600
```

Then, run `ldapmodify`. For example:

```
setenv LD_LIBRARY_PATH /opt/SUNWam/lib/:
/opt/SUNWam/ldaplib/ldapsdk:/usr/lib/mps:/usr/share/lib/mps/secv1:/usr/lib/mps/secv1:
$LD_LIBRARY_PATH

./ldapmodify -D "cn=Directory Manager" -w "iplanet333"
-c -a -h hostname.domain -p 389 -f  newConfig.xml
```

User Search Key

This attribute defines the attribute name that is to be searched upon when performing a simple search in the Navigation page. The default value for this attribute is `cn`.

For example, if you enter `j*` in the Name field in the Navigation frame, users whose names begins with "j" or "J" will be displayed.

Search Return Attribute

This field defines the attribute name used when displaying the users returned from a simple search. The default of this attribute is uid cn. This will display the user ID and the user's full name.

The attribute name that is listed first is also used as the key for sorting the set of users that will be returned. To avoid performance degradation, use an attribute whose value is set in a user's entry.

Maximum Entries Displayed per Page

This attribute allows you to define the maximum rows that can be displayed per page. The default is 25. For example, if a user search returns 100 rows, there will be 4 pages with 25 rows displayed in each page.

External Attributes Fetch

This option enables callbacks for plug-ins to retrieve external attributes (any external application-specific attribute). External attributes are not cached in the OpenSSO Enterprise SDK, so this attribute allows you enable attribute retrieval per realm level. By default, this option is not enabled

Globalization Settings

The Globalization Settings service contains global attributes that enable you to configure OpenSSO Enterprise for different locales and character sets. The attributes are:

Charsets Supported By Each Locale

This attribute lists the character sets supported for each locale, which indicates the mapping between locale and character set. The format is as follows:

To add a New Supported Charset, click Add and define the following parameters:

Locale	The new locale you wish to add. See"Supported Language Locales" on page 218 for more information.
Supported Charsets	Enter the supported charset for the specified locale. Charsets are delimited by a semicolon. For example, `charset=charset1;charset2;charset3;...;charsetn`

To edit any existing Supported Charset, click the name in the Supported Charset table. Click OK when you are finished.

Charset Aliases

This attribute lists the codeset names (which map to IANA names) that will be used to send the response. These codeset names do not need to match Java codeset names. Currently, there is a hash table to map Java character sets into IANA charsets and vice versa.

To add a New Charset Alias, click Add button and define the following parameters:

MIME name	The IANA mapping name. For example, `Shift_JIS`
Java Name	The Java character set to map to the IANA character set.

To edit any existing Charset Alias, click the name in the table. Click OK when you are finished.

Auto Generated Common Name Format

This display option allows you to define the way in which a name is automatically generated to accommodate name formats for different locales and character sets. The default syntax is as follows (please note that including commas and/or spaces in the definition will display in the name format):

```
en_us = {givenname} {initials} {sn}
```

For example, if you wanted to display a new name format for a user (User One) with a uid (11111) for the Chinese character set, define:

```
zh = {sn}{givenname}({uid})
```

The display is:

```
OneUser 11111
```

Supported Language Locales

The following table lists the language locales that OpenSSO Enterprise supports:

Language Tag	Language
af	Afrikaans
be	Byelorussian
bg	Bulgarian
ca	Catalan
cs	Czechoslovakian
da	Danish
de	German
el	Greek
en	English
es	Spanish
eu	Basque
fi	Finnish
fo	Faroese

fr	French
ga	Irish
gl	Galician
hr	Croatian
hu	Hungarian
id	Indonesian
is	Icelandic
it	Italian
ja	Japanese
ko	Korean
nl	Dutch
no	Norwegian
pl	Polish
pt	Portuguese
ro	Romanian
ru	Russian
sk	Slovakian
sl	Slovenian
sq	Albanian
sr	Serbian
sv	Swedish
tr	Turkish
uk	Ukrainian
zh	Chinese

Global Properties

Global Properties contain services that enable to define password reset functionality and policy configuration for OpenSSO Enterprise. The services you can configure are:

- "Common Federation Configuration" on page 220
- "Liberty ID-FF Service Configuration" on page 221

Common Federation Configuration

Datastore SPI Implementation Class

This attribute specifies the implementation class for the `com.sun.identity.plugin.datastore.DataStoreProvider` SPI which is used for managing federation user data store information.

Configuration Instance SPI Implementation Class

This attribute specifies the implementation class for the `com.sun.identity.plugin.configuration.ConfigurationInstance` SPI which is used for managing federation service configuration data.

Logger SPI Implementation Class

This attribute specifies the implementation class for the `com.sun.identity.plugin.log.Logger` SPI which is used for managing federation logging.

Session Provider SPI Implementation Class

This specifies the implementation class for the `com.sun.identity.plugin.session.SessionProvider` SPI which is used for managing federation session.

Maximum Allowed Content Length

This attribute specifies the maximum allowed content length for an HTTP Request that will be used in federation services. Any request whose content exceeds the specified maximum content length will be rejected.

Password Decoder SPI Implementation Class

This attribute specifies the implementation class for the `com.sun.identity.saml.xmlsig.PasswordDecoder` interface which is used to decode stored password for XML signing keystore and password for basic authentication under SAML 1.x.

Signature Provider SPI Implementation Class

This attribute specifies the SAML XML signature provider class. The default SPI is `com.sun.identity.saml.xmlsig.AMSignatureProvider`.

Key Provider SPI Implementation Class

This attribute specifies the XML signature key provider class. The default SPI is `com.sun.identity.saml.xmlsig.JKSKeyProvider`.

Check Presence of Certificates

If set to on, the certificate must be presented to the keystore for XML signature validation. If set to `off`, presence checking of the certificate is skipped. This applies to SAML1.x only.

XML Cannonicalization Algorithm

This attribute specifies XML cannonicalization algorithm used for SAML XML signature generation and verification. The default value is `http://www.w3.org/2001/10/xml-exc-c14n#`.

XML Signature Algorithm

This attribute specifies XML signature algorithm used for SAML XML Signature generation and verification. When not specified or value is empty, the default value (`http://www.w3.org/2000/09/xmldsig#rsa-sha1`) is used.

XML Transformation Algorithm

This attribute specifies transformation algorithm used for SAML XML signature generation and verification. When not specified or the value is empty, the default value (`http://www.w3.org/2001/10/xml-exc-c14n#`) is used.

Liberty ID-FF Service Configuration

Federation Cookie Name

This attribute specifies the name of the ID-FF Services cookie. The cookie is used to remember if the user is federated already.

IDP Proxy Finder SPI Implementation Class

This attribute specifies the implementation class for finding a preferred identity provider to be proxied.

Request Cache Cleanup Interval

This attribute specifies the cleanup interval (in seconds) for ID-FF internal request cleanup thread.

Request Cache Timeout

This attribute specifies the timeout value (in seconds) for the ID-FF Authentication Request. Any`AuthnRequest` object will be purged from the memory if it exceeds the timeout value.

IDP Login URl

This attribute specifies the login URL to which the IDP will redirect if a valid session is not found while processing the Authentication Request. If the key is not specified, a default login URL is used.

XML Signing On

This attribute specifies the level of signature verification for Liberty requests and responses.

Liberty ID-WSF Security Service

Security Attribute Plugin Class

This attribute specifies the implementation class name for the `com.sun.identity.liberty.ws.security.SecurityAttributePlugin` interface. The class returns a list of SAML attributes to be included in the credentials generated by the Discovery Service.

Key Info Type

The value set in this attribute is used in the `com.sun.identity.liberty.ws.security.LibSecurityTokenProvider` implementation class. It specifies the data type to be put into the `KeyInfo` block inside the XML signature. If value is `certificate`, the signer's X059 Certificate will be included inside `KeyInfo`. Otherwise, corresponding DSA/RSA key will be included in `KeyInfo`.

Security Token Provider Class

This attribute specifies the implementation class for the security token provider.

Default WSC Certificate Alias

This attribute specifies default certificate alias for the issuing web service security token for this web service client.

Trusted Authority Signing Certificate Alias

This attribute specifies the certificate alias for the trusted authority that will be used to sign the SAML or SAML BEARER token of response message.

Trusted CA Signing Certificate Aliases

This attribute specifies the certificate aliases for trusted CA. SAML or SAML BEARER tokens of an incoming request. The message must be signed by a trusted CA in this list. The syntax is `cert alias 1[:issuer 1]|cert alias 2[:issuer 2]|.....`

Example: `myalias1:myissuer1|myalias2|myalias3:myissuer3`.

The value issuer is used when the token does not have a `KeyInfo` inside of the signature. The issuer of the token must be in this list and the corresponding certificate alias will be used to verify the signature. If `KeyInfo` exists, the keystore must contain a certificate alias that matches the `KeyInfo` and the certificate alias must be in this list.

Liberty Interaction Service

WSP to Redirect User for Interaction

This attribute indicates whether the web service provider will redirect the user for consent. The default value is yes.

WSP to Redirect User for Interaction for Data

This initiates an interaction to get user consent or to collect additional data. This property indicates whether the web service provider will redirect the user to collect additional data. The default value is yes.

WSP's Expected Duration for Interaction

This attribute indicates the length of time (in seconds) that the web service provider expects to take to complete an interaction and return control back to the web service client. For example, the web service provider receives a request indicating that the web service client will wait a maximum 30 seconds (set in WSC's Expected Duration for Interaction) for interaction. If this attribute is set to 40 seconds, the web service provider returns a SOAP fault (`timeNotSufficient`), indicating that the time is insufficient for interaction.

WSP to Enforce That returnToURL must be SSL

This attribute indicates whether the web service provider will enforce a HTTPS `returnToURL`specified by the web service client. The Liberty Alliance Project specifications state that the value of this property is always yes. The false value is primarily meant for ease of deployment in a phased manner.

WSP to Enforce Return to Host be the Same as Request Host

This attribute indicates whether the web service provider would enforce the address values of `returnToHost` and `requestHost` if they are the same. The Liberty Alliance Project specifications state that the value of this property is always yes. The false value is primarily meant for ease of deployment in a phased manner.

HTML Style Sheet Location

This attribute points to the location of the style sheet that is used to render the interaction page in HTML.

WML Style Sheet Location

This attribute points to the location of the style sheet that is used to render the interaction page in WML.

WSP Interaction URL

This attribute specifies the URL where the `WSPRedirectHandler` servlet is deployed. The servlet handles the service provider side of interactions for user redirects.

WSP Interaction URL if Behind Load Balancer

Defines the WSP redirect handler URL exposed by a Load Balancer.

List of Interaction URLs of the WSP Cluster (site) Behind the Load Balancer

Defines the WSP redirect handler URLs of trusted servers in the cluster.

Interaction Configuration Class

This attribute specifies the class that provides access methods to read interaction configurations.

Options for WSC to Participate in Interaction

This attribute indicates the level of interaction in which the WSC will participate if configured to participate in user redirects. The possible values are interactIfNeeded, doNotInteract, and doNotInteractForData. The affirmative interactIfNeeded is the default.

WSC to Include userInteractionHeader

This attribute indicates whether the web service client will include a SOAP header to indicate certain preferences for interaction based on the Liberty specifications. The default value is yes.

WSC to redirect user for Interaction

This attribute defines whether the WSC will participate in user redirections. The default value is yes.

WSC's Expected Duration for Interaction

This attribute defines the maximum length of time (in seconds) that the web service client is willing to wait for the web service provider to complete its portion of the interaction. The web service provider will not initiate an interaction if the interaction is likely to take more time than what is set. For example, the web service provider receives a request where this property is set to a maximum 30 seconds. If the web service provider property WSP's Expected Duration for Interaction is set to 40 seconds, the web service provider returns a SOAP fault (`timeNotSufficient`), indicating that the time is insufficient for interaction.

WSC to Enforce that Redirection URL Must be SSL

This attribute specifies whether the web service client will enforce HTTPS in redirected URLs. The Liberty Alliance Project specifications state that the value of this property is always yes, which indicates that the web service provider will not redirect the user when the value of `redirectURL` (specified by the web service provider) is not an HTTPS URL. The false value is primarily meant for easy, phased deployment.

Multi Federation Protocol

Single Logout Handler List

This attribute defines a list of values each specifying a Single Logout Handler implementation class for an individual federation protocol. Each value has following format: `key=`*Federation_Protocol_Name*`|class=`*SPI_Implementation_Class_Name*

The default is, OASIS SAMLv2 (key=SAML2),

Liberty ID-FF (key=IDFF) and WS-Federation (key=WSFED) are defined in the list. For example:

```
key=SAML2|class=com.sun.identity.multiprotocol.SAML2SingleLogoutHandler
key=IDFF|class=com.sun.identity.multiprotocol.IDFFSingleLogoutHandler
key=WSFED|class=com.sun.identity.multiprotocol.WSFederationSingleLogoutHandler
```

Password Reset

OpenSSO Enterprise provides a Password Reset service to allow users to receive an email message containing a new password or to reset their password for access to a given service or application protected by OpenSSO Enterprise. The Password Reset attributes are realm attributes. The attributes are:

User Validation

This attribute specifies the name of user attribute that is used to search for the user whose password is to be reset.

Secret Question

This field allows you to add a list of questions that the user can use to reset his/her password. To add a question, type it in the Secret Question filed and click Add. The selected questions will appear in the user's User Profile page. The user can then select a question for resetting the password. Users may create their own question if the Personal Question Enabled attribute is selected.

Search Filter

This attribute specifies the search filter to be used to find user entries.

Base DN

This attribute specifies the DN from which the user search will start. If no DN is specified, the search will start from the realm DN. You should not use `cn=directorymanager` as the base DN, due to proxy authentication conflicts.

Bind DN

This attribute value is used with Bind Password to reset the user password.

Bind Password

This attribute value is used with Bind DN to reset the user password.

Bind Password Confirm

Confirm the password.

Password Reset Option

This attribute determines the classname for resetting the password. The default classname is `com.sun.identity.password.RandomPasswordGenerator` . The password reset class can be customized through a plug-in. This class needs to be implemented by the `PasswordGenerator` interface.

Password Change Notification Option

This attribute determines the method for user notification of password resetting. The default classname is: `com.sun.identity.password.EmailPassword` The password notification class can be customized through a plug-in. This class needs to be implemented by the `NotifyPassword` interface. See the OpenSSO Enterprise Developer's Guide for more information.

Password Reset

Selecting this attribute will enable the password reset feature.

Personal Question

Selecting this attribute will allow a user to create a unique question for password resetting.

Maximum Number of Questions

This value specifies the maximum number of questions to be asked in the password reset page.

Force Change Password on Next Login

When enabled, this option forces the user to change his or her password on the next login. If you want an administrator, other than the top-level administrator, to set the force password reset option, you must modify the Default Permissions ACIs to allow access to that attribute.

Password Reset Failure Lockout

This attribute specifies whether to disallow users to reset their password if that user initially fails to reset the password using the Password Reset application. By default, this feature is not enabled.

Password Reset Failure Lockout Count

This attributes defines the number of attempts that a user may try to reset a password, within the time interval defined in Password Reset Failure Lockout Interval, before being locked out. For example, if Password Reset Failure Lockout Count is set to 5 and Login Failure Lockout Interval is set to 5 minutes, the user has five chances within five minutes to reset the password before being locked out.

Password Reset Failure Lockout Interval

This attribute defines (in minutes) the amount of time in which the number of password reset attempts (as defined in Password Reset Failure Lockout Count) can be completed, before being locked out.

Email Address to Send Lockout Notification

This attribute specifies an email address that will receive notification if a user is locked out from the Password Reset service. Specify multiple email address in a space-separated list.

Warn User After N Failures

This attribute specifies the number of password reset failures that can occur before OpenSSO Enterprise sends a warning message that user will be locked out.

Password Reset Failure Lockout Duration

This attribute defines (in minutes) the duration that user will not be able to attempt a password reset if a lockout has occurred.

Password Reset Lockout Attribute Name

This attribute contains the *inetuserstatus* value that is set in Password Reset Lockout Attribute Value. If a user is locked out from Password Reset, and the Password Reset Failure Lockout Duration (minutes) variable is set to 0, *inetuserstatus* will be set to inactive, prohibiting the user from attempting to reset his or her password.

Password Reset Lockout Attribute Value

This attribute specifies the *inetuserstatus* value (contained in Password Reset Lockout Attribute Name) of the user status, as either active or inactive. If a user is locked out from Password Reset, and the Password Reset Failure Lockout Duration (minutes) variable is set to 0, *inetuserstatus* will be set to inactive, prohibiting the user from attempting to reset his or her password.

Policy Configuration

The Policy Configuration attributes enable the administrator to set configuration global and realm properties used by the Policy service.

Global Properties

The Global Properties are:

Resource Comparator

Specifies the resource comparator information used to compare resources specified in a Policy rule definition. Resource comparison is used for both policy creation and evaluation.

Click the Add button and define the following attributes:

Service Type	Specifies the service to which the comparator should be used.
Class	Defines the Java class that implements the resource comparison algorithm.
Delimiter	Specifies the delimiter to be used in the resource name.
Wildcard	Specifies the wildcard that can be defined in resource names.
One Level Wildcard	Matches zero or more characters, at the same delimiter boundary.
Case Sensitive	Specifies if the comparison of the two resources should consider or ignore case. False ignores case, True considers case.

Continue Evaluation on Deny Decision

Specifies whether or not the policy framework should continue evaluating subsequent policies, even if a DENY policy decision exists. If it is not selected (default), policy evaluation would skip subsequent policies once the DENY decision is recognized.

Advices Handleable by OpenSSO

Defines the names of policy advice keys for which the Policy Enforcement Point (Policy Agent) would redirect the user agent to OpenSSO Enterprise. If the agent receives a policy decision that does not allow access to a resource, but does posses advices, the agent checks to see whether it has a advice key listed in this attribute.

If such an advice is found, the user agent is redirected to OpenSSO Enterprise, potentially allowing the access to the resource.

Realm Alias Referrals

When set to Yes, this attribute allows you to create policies in sub-realms without having to create referral policies from the top-level or parent realm. You can only create policies to protect HTTP or HTTPS resources whose fully qualified hostname matches the DNSAlias of the realm. By default, this attribute is defined as No.

Realm Attributes

The LDAP Properties are:

Primary LDAP Server

Specifies the host name and port number of the primary LDAP server specified during OpenSSO Enterprise installation that will be used to search for Policy subjects, such as LDAP users, LDAP roles, LDAP groups, and so forth.

The format is *hostname:port*. For example: `machine1.example.com:389`

For failover configuration to multiple LDAP server hosts, this value can be a space-delimited list of hosts. The format is *hostname1:port1 hostname2:port2...*

For example: `machine1.example1.com:389 machine2.example1.com:389`

Multiple entries must be prefixed by the local server name. This is to allow specific OpenSSO Enterprise instances to be configured to talk to specific Directory Servers.

The format is *servername*|*hostname:port* For example:

```
machine1.example1.com|machine1.example1.com:389
```

```
machine1.example2.com|machine1.example2.com:389
```

For failover configuration:

```
AM_Server1.example1.com|machine1.example1.com:389 machine2.example.com1:389
```

```
AM_Server2.example2.com|machine1.example2.com:389 machine2.example2.com:389
```

LDAP Base DN

Specifies the base DN in the LDAP server from which to begin the search. By default, it is the top-level realm of the OpenSSO Enterprise installation.

LDAP Users Base DN

This attribute specifies the base DN used by the LDAP Users subject in the LDAP server from which to begin the search. By default, it is the top-level realm of the OpenSSO Enterprise installation base.

OpenSSO Enterprise Roles Base DN

Defines the DN of the realm or organization which is used as a base while searching for the values of OpenSSO Enterprise Roles. This attribute is used by the *AccessManagerRoles* policy subject.

LDAP Bind DN

Specifies the bind DN in the LDAP server.

LDAP Bind Password

Defines the password to be used for binding to the LDAP server. By default, the `amldapuser` password that was entered during installation is used as the bind user.

LDAP Bind Password Confirm

Confirm the password.

LDAP Organizations Search Filter

Specifies the search filter to be used to find organization entries. The default is `(objectclass=sunMangagedOrganization)`.

LDAP Organizations Search Scope

Defines the scope to be used to find organization entries. The scope must be one of the following:

- SCOPE_BASE
- SCOPE_ONE

- SCOPE_SUB (default)

LDAP Groups Search Scope

Defines the scope to be used to find group entries. The scope must be one of the following:

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (default)

LDAP Groups Search Filter

Specifies the search filter to be used to find group entries. The default is `(objectclass=groupOfUniqueNames)`.

LDAP Users Search Filter

Specifies the search filter to be used to find user entries. The default is `(objectclass=inetorgperson)`.

LDAP Users Search Scope

Defines the scope to be used to find user entries. The scope must be one of the following:

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (default)

LDAP Roles Search Filter

Specifies the search filter to be used to find entries for roles. The default is `(&(objectclass=ldapsubentry)(objectclass=nsroledefinitions))`.

LDAP Roles Search Scope

This attribute defines the scope to be used to find entries for roles. The scope must be one of the following:

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (default)

OpenSSO Roles Search Scope

Defines the scope to be used to find entries for OpenSSO Enterprise Roles subject.

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (default)

LDAP Organization Search Attribute

Defines the attribute type for which to conduct a search on an organization. The default is `o`.

LDAP Groups Search Attribute

Defines the attribute type for which to conduct a search on a group. The default is `cn`.

LDAP Users Search Attribute

Defines the attribute type for which to conduct a search on a user. The default is `uid`.

LDAP Roles Search Attribute

This field defines the attribute type for which to conduct a search on a role. The default is `cn`.

Maximum Results Returned from Search

This field defines the maximum number of results returned from a search. The default value is 100. If the search limit exceeds the amount specified, the entries that have been found to that point will be returned.

Search Timeout

Specifies the amount of time before a timeout on a search occurs. If the search exceeds the specified time, the entries that have been found to that point will be returned

LDAP SSL

Specifies whether or not the LDAP server is running SSL. Selecting enables SSL, deselecting (default) disables SSL.

If the LDAP Server is running with SSL enabled (LDAPS), you must make sure that OpenSSO Enterprise is configured with proper SSL-trusted certificates so that OpenSSO Enterprise can connect to Directory server over LDAPS protocol.

LDAP Connection Pool Minimum Size

Specifies the minimal size of connection pools to be used for connecting to the Directory Server, as specified in the LDAP server attribute. The default is 1.

Connection Pool Maximum Size

This attribute specifies the maximum size of connection pools to be used for connecting to the Directory Server, as specified in the LDAP server attribute. The default is 10.

Selected Policy Subjects

Allows you to select a set of subject types available to be used for policy definition in the realm.

Selected Policy Conditions

Allows you to select a set of conditions types available to be used for policy definition in the realm.

Selected Policy Referrals

Allows you to select a set of referral types available to be used for policy definition in the realm.

Subject Results Time To Live

This attribute specifies the amount of time (in minutes) that a cached subject result can be used to evaluate the same policy request based on the single sign-on token.

When a policy is initially evaluated for an SSO token, the subject instances in the policy are evaluated to determine whether the policy is applicable to a given user. The subject result, which is keyed by the SSO token ID, is cached in the policy. If another evaluation occurs for the same policy for the same SSO token ID within the time specified in the Subject Result Time To Live attribute, the policy framework retrieves the cached subjects result, instead of evaluating the subject instances. This significantly reduces the time for policy evaluation.

User Alias

This attribute must be enabled if you create a policy to protect a resource whose subject's member in a remote Directory Server aliases a local user. This attribute must be enabled, for example, if you create `uid=rmuser` in the remote Directory Server and then add `rmuser` as an alias to a local user (such as `uid=luser`) in OpenSSO Enterprise. When you login as `rmuser`, a session is created with the local user (`luser`) and policy enforcement is successful.

Selected Response Providers

Defines the policy response provider plug-ins that are enabled for the realm. Only the response provider plug-ins selected in this attribute can be added to policies defined in the realm.

Selected Dynamic Response Attributes

Defines the dynamic response attributes that are enabled for the realm. Only a subset of names selected in this attribute can be defined in the dynamic attributes list in *IDResponseProvider* to be added to policies defined in the realm.

SAMLv2 Service Configuration

Cache Cleanup Interval

This attribute specifies the duration (in seconds) between each cache cleanup.

Attribute Name for Name ID Information

Specifies the attribute name used to store name identifier information on a user's entry. If nothing is specified, the default attribute (`sun-fm-saml2-nameid-info`) will be used. The corresponding datastore bind user must have read/write/search/compare permission to this attribute.

Attribute Name for Name ID Information Key

Specifies the attribute name used to store name identifier key on a user's entry. If not specified, the default attribute (`sun-fm-saml2-nameid-infokey`) will be used. The corresponding datastore bind user must have read/write/search/compare permission to this attribute. You must also must make sure that the `equality` type index is added.

Cookie Domain for IDP Discovery Service

Specifies the cookie domain for the SAMLv2 IDP discovery cookie.

Cookie Type for IDP Discovery Service

Specifies cookie type used in SAMLv2 IDP Discovery Service, either Persistent or Session. Default is Session.

URL Scheme for IDP Discovery Service

Specifies URL scheme used in SAMLv2 IDP Discovery Service.

XML Encryption SPI Implementation Class

Specifies implementation class name for the SAMLv2 Encryption Provider interface. The class is used to perform XML encryption and decryption in SAMLv2 profiles.

Include Encrypted Key Inside KeyInfo Element

This is used in the `com.sun.identity.saml2.xmlenc.FMEncProvider` class. If enabled, it will include `EncryptedKey` inside a `KeyInfo` in the `EncryptedData` element when performing XML encryption operation. If it is not enabled, `EncryptedKey` is paralleled to the `EncryptedData` element. Default is enabled.

XML Signing Implementation Class

If enabled, the signing certificate used by identity provider and service provider will be validated against certificate revocation list (CRL) configured in the Security settings under the Sites and Servers tab. If the certificate is not validated and accepted, it will stop and return a validation error without doing further XML signature validation.

XML Signing Certificate Validation

If enabled, the SAML identity provider or service provider will validate the certificate that is used in signing . If the certificate is validated and accepted, the provider will validate the signature. If not, it will stop and return a validation error.

CA Certificate Validation

If enabled, the signing certificate used by identity provider and service provider will be validated against the trusted CA list. If the certificate is not validated and accepted, it will stop and return a validation error without doing further XML signature validation.

SAMLv2 SOAP Binding

The SAMLv2 SOAP Binding service provides SOAP-based exchange of SAMLv2 Request and Response message between a OpenSSO Enterprise Client and the OpenSSO Enterprise Server. The requests received are delegated to the request handler for further processing. The key to the Request Handler and the meta alias is in the SOAP Binding service URL. A mapping of the meta alias and the RequestHandler is stored in the SAMLv2 SOAP Binding service which can be read from the OpenSSO Enterprise configuration store.

Request Handler List

The RequestHandlerList is a list of key/value pair entries containing the mapping of the meta alias to the RequestHandler implementation. This attribute must be set if a OpenSSO Enterprise 8.0 server is being configured to act as Policy Decision Point (PDP).

The *Key* is the Policy Decision Point meta alias and the *Class* is the Java class name, which is the implementation of RequestHandler Interface which can process XACML Requests.

For example, If the meta Alias of the XACML Policy Decision Point is `/pdp` and the implementation of the interface is `com.sun.identity.xacml.plugins.XACMLAuthzDecisionQueryHandler`, then the key should be set to `/pdp` and the class should be set to `com.sun.identity.xacml.plugins.XACMLAuthzDecisionQueryHandler`.

▼ To Configure a Request Handler

The `RequestHandler` interface must be implemented on the server side by each SAMLv2 service that uses the SOAP Binding Service. The Request Handler List attribute stores information about the implementation classes that implement the Request Handler. The Request Handler List displays entries that contain key/value pairs.

1. **Click New to display the New Request Handler attributes or click on a configured key value to modify existing attributes.**

2. **Provide values for the attributes based on the following information:**

   key — The *Key* is the Policy Decision Point meta alias.

   class — The *Class* is the Java class name, which is the implementation of RequestHandler Interface which can process XACML Requests.

3. **Click OK to complete the Request Handler configuration.**

4. **Click Save on the SAMLv2 SOAP Binding page to complete the service configuration.**

Security Token Service

The attributes contained in this service define the dynamic configuration for the OpenSSO Enterprise Security Token Service (STS). These attributes define the following configuration:

- Issuing and creating security tokens

- Web services security for the STS itself for securing STS service endpoints. The Signing and Encryption attributes configures the server provider validation of incoming WS-Trust requests and secures outgoing WS-Trust responses. The Security Mechanism attribute defines the security credential of the security tokens.
- SAML configuration to request SAML attribute mapping in the security token (through a SAML assertion) when the configured STS is specified as a web service provider and receives a SAML token (assertion) generated by a remote STS.
- Security token validation received from a web service provider when the token was generated by a remote STS.

  You can create dynamic configuration profiles for different OpenSSO Enterprise web services security providers in the Centralized Agent Configuration under the Realms tab.

Issuer

The name of the Security Token service that issues the security tokens.

End Point

This field takes a value equal to:

```
%protocol://%host:%port%uri/sts
```

This syntax allows for dynamic substitution of the Security Token Service Endpoint URL based on the specific session parameters.

Encryption Issued Key

When enabled, this attribute encrypts the key issued by the Security Token service.

Encryption Issued Token

When enabled, this attribute encrypts the security token issued by the Security Token service.

Lifetime for Security Token

Defines the amount of time for which the issued token is valid.

Token Implementation Class

This attribute specifies the implementation class for the security token provider/issuer.

Certificate Alias Name

Defines the alias name for the certificate used to sign the security token issues by the Security Token service.

STS End User Token Plug-in Class

Defines the implementation class for the end user token conversion.

Security Mechanism

Defines the type of security credential that is used to secure the security token itself, or the security credential accepted by the Security Token service from the incoming WS-Trust request sent the by the client. You can choose from the following security types:

- Anonymous — The anonymous security mechanism contains no security credentials.
- KerberosToken — Uses Kerberos tokens.
- LibertyBearerToken – Uses the Liberty-defined bearer token.
- LibertySAMLToken – Uses the Liberty-defined SAML token.
- LibertyX509Token – Uses the Liberty-defined X509 certificate.
- SAML-HolderOfKey — Uses the SAML 1.1 assertion type Holder-Of-Key.
- SAML-SenderVouches — Uses the SAML 1.1 assertion type Sender Vouches.
- SAML2–HolderOfKey — Uses the SAML 2.0 assertion token type Holder-Of-Key.
- SAML2–SenderVouches — Uses the SAML 2.0 assertion token type Sender Vouches.
- UserNameToken — Uses a user name token to secure the Security Token service requests.
- UserNameToken-Plain — Uses a user name token with a clear text password for securing Security Token service requests.
- X509Token — Uses the X509 certificate to secure the Security token.

Authentication Chain

Defines the authentication chain or service name that can be used to authenticate to the OpenSSO Enterprise authentication service using the credentials from an incoming issuer request's security token to generate OpenSSO Enterprise's authenticated security token.

User Credential

The attribute represents the username/password shared secrets that are used by the Security Token service to validate a UserName token sent by the client as part of the incoming WS-Trust request.

Is Request Signature Verified

Specifies that the Security Token service must verify the signature of the incoming WS-Trust request.

Is Request Header Decrypted

Specifies that all request headers received by the Security Token Service must be decrypted.

Is Request Decrypted

Specifies that all requests received by the Security Token Service must be decrypted.

Is Response Signed

Specifies that all responses received by the Security Token Service must be signed.

Is Response Encrypted

Specifies that all responses sent by the Security Token service must be encrypted.

Signing Reference Type

Defines the reference types used when the Security Token service signs the WS-Trust response. The possible reference types are `DircectReference`, `KeyIdentifier`, and `X509`.

Encryption Algorithm

Defines the encryption algorithm used by the Security Token service to encrypt the WS-Trust response.

Encryption Strength

Sets the encryption strength used by he Security Token service to encrypt the WS-Trust response. Select a greater value for greater encryption strength.

Private Key Alias

This attribute defines the private certificate key alias that is used to sign the WS-Trust response or to decrypt the incoming WS-Trust request.

Private Key Type

This attribute defines the certificate private key type used for signing WS-Trust responses or decrypting WS-Trust requests. The possible types are `PublicKey`, `SymmetricKey`, or `NoProofKey`.

Public Key Alias of Web Service (WS-Trust) Client

Defines the public certificate key alias used to verify the signature of the incoming WS-Trust request or to encrypt the WS-Trust response.

Kerberos Domain Server

This attribute specifies the Kerberos Distribution Center (the domain controller) hostname. You must enter the fully qualified domain name (FQDN) of the domain controller.

Kerberos Domain

This attribute specifies the Kerberos Distribution Center (domain controller) domain name. Depending up on your configuration, the domain name of the domain controller may be different than the OpenSSO Enterprise domain name.

Kerberos Service Principal

Specifies the Kerberos principal as the owner of the generated Security token.

Use the following format:

```
HTTP/hostname.domainname@dc_domain_name
```

`hostname` and `domainame` represent the hostname and domain name of the OpenSSO Enterprise instance. `dc_domain_name` is the Kerberos domain in which the Windows Kerberos server (domain controller) resides. It is possible that the Kerberos server is different from the domain name of the OpenSSO Enterprise instance.

Kerberos Key Tab File

This attribute specifies the Kerberos keytab file that is used for issuing the token. Use the following format, although the format is not required:

```
hostname.HTTP.keytab
```

`hostname` is the hostname of the OpenSSO Enterprise instance.

Verify Kerberos Signature

If enabled, this attribute specifies that the Kerberos token is signed.

SAML Attribute Mapping

Note – All of the following SAML-related attributes are to be used in the configuration where the current instance of the Security Token service haves as the web service provider and receives a SAML Token generated from another Security Token service instance.

This configuration represents a SAML attribute that needs to be generated as an Attribute Statement during SAML assertion creation by the Security Token Service for a web service provider. The format is *SAML_attr_name=Real_attr_name*.

SAML_attr_name is the SAML attribute name from a SAML assertion from an incoming web service request. *Real_attr_name* is the attribute name that is fetched from either the authenticated SSOToken or the identity repository.

NameID Mapper

The SAML NameID Mapper for an assertion that is generated for the Security Token service.

Should Include Memberships

When enabled, the generated assertion contains user memberships as SAML attributes.

Attribute Namespace

Defines the SAML Attribute Namespace for an assertion that is generated for the Security Token service.

Trusted Issuers

Defines a list of trusted issuers that can be trusted to send security tokens to OpenSSO Enterprise. OpenSSO Enterprise must verify whether the security token was sent from one of these issuers.

Trusted IP Addresses

Defines a list of IP addresses that can be trusted to send security tokens to OpenSSO Enterprise. OpenSSO Enterprise must verify whether the security token was sent from one of these hosts.

Session

The Session service defines values for an authenticated user session such as maximum session time and maximum idle time. The Session attributes are global, dynamic, or user attributes. The attributes are:

Secondary Configuration Instance

Provides the connection information for the session repository used for the session failover functionality in OpenSSO Enterprise. The URL of the load balancer should be given as the identifier to this secondary configuration. If the secondary configuration is defined in this case, the session failover feature will be automatically enabled and become effective after the server restart.

▼ To Add a Sub Configuration

1. **Click New in the Secondary Configuration Instance list.**
2. **Enter a name for the new Sub Configuration.**
3. **Enter data for the following fields:**

Session Store User	Defines the database user who is used to retrieve and store the session data.
Session Store Password	Defines the password for the database user defined in Session Store.
Session Store Password (Confirm)	Confirm the password.

Maximum Wait Time	Defines the total time a thread is willing to wait for acquiring a database connection object. The value is in milliseconds.
Database URL	Specifies the URL of the database.

4 **Click Add.**

Maximum Number of Search Results

This attribute specifies the maximum number of results returned by a session search. The default value is 120.

Timeout for Search

This attributed defines the maximum amount of time before a session search terminates. The default value is 5 seconds.

Enable Property Change Notifications

Enables or disables the feature session property change notification. In a single sign-on environment, one OpenSSO Enterprise session can be shared by multiple applications. If this feature is set to ON, if one application changes any of the session properties specified in the Notification Properties list (defined as a separate session service attribute), the notification will be sent to other applications participating in the same single sign-on environment.

Enable Quota Constraints

Enables or disables session quota constraints. The enforcement of session quota constraints enables administrators to limit a user to have a specific number of active/concurrent sessions based on the constraint settings at the global level, or the configurations associated with the entities (realm/role/user) to which this particular user belongs.

The default setting for this attribute is OFF. You must restart the server if the settings are changed.

Read Timeout for Quota Constraint

Defines the amount of time (in number of milliseconds) that an inquiry to the session repository for the live user session counts will continue before timing out.

After the maximum read time is reached, an error is returned. This attribute will take effect only when the session quota constraint is enabled in the session failover deployment. The default value is 6000 milliseconds. You must restart the server if the settings are changed.

Exempt Top-Level Admins From Constraint Checking

Specifies whether the users with the Top-level Admin Role should be exempt from the session constraint checking. If YES, even though the session constraint is enabled, there will be no session quota checking for these administrators.

The default setting for this attribute is NO. You must restart the server if the settings are changed. This attribute will take effect only when the session quota constraint is enabled.

Resulting Behavior If Session Quota Exhausted

Specifies the resulting behavior when the user session quota is exhausted. There are two selectable options for this attribute:

DESTROY_OLD_SESSION	The next expiring session will be destroyed.
DENY_ACCESS	The new session creation request will be denied.

This attribute will take effect only when the session quota constraint is enabled and the default setting is DESTROY_OLD_SESSION .

Deny User Login When Session Repository is Down

If set to YES, this attribute will enforce user lockout to the server when the session repository is down. This attribute takes effect only when the session Enable Quota Constrain is selected.

Notification Properties

When a change occurs on a session property defined in the list, the notification will be sent to the registered listeners. The attribute will take effect when the feature of Session Property Change Notification is enabled.

Enable Session Trimming

When set to YES, a minimum set of session properties are stored by the server between the session timeout and purge delay states. This is used to improve memory performance. The following properties are stored:

- loginURL
- SessionTimedOut
- SAML2IDPSessionIndex
- SAML2IDPSessionIndex

If set to OFF, then all session-related attributes are stored by OpenSSO Enterprise after a session timeout.

Maximum Session Time

This attribute accepts a value in minutes to express the maximum time before the session expires and the user must reauthenticate to regain access. A value of 1 or higher will be accepted. The default value is 120. (To balance the requirements of security and convenience, consider setting the Max Session Time interval to a higher value and setting the Max Idle Time interval to a relatively low value.) Max Session Time limits the validity of the session. It does not get extended beyond the configured value.

Maximum Idle Time

This attribute accepts a value (in minutes) equal to the maximum amount of time without activity before a session expires and the user must reauthenticate to regain access. A value of 1 or higher will be accepted. The default value is 30. (To balance the requirements of security and convenience, consider setting the Max Session Time interval to a higher value and setting the Max Idle Time interval to a relatively low value.)

Maximum Caching Time

This attribute accepts a value (in minutes) equal to the maximum interval before the client contacts OpenSSO Enterprise to refresh cached session information. A value of 0 or higher will be accepted. The default value is 3. It is recommended that the maximum caching time should always be less than the maximum idle time.

Active User Sessions

Specifies the maximum number of concurrent sessions allowed for a user.

User

The default user preferences are defined through the user service. These include time zone, locale and DN starting view. The User service attributes are dynamic attributes.

User Preferred Language

This field specifies the user's choice for the text language displayed in the OpenSSO Enterprise console. The default value is en. This value maps a set of localization keys to the user session so that the on-screen text appears in a language appropriate for the user.

User Preferred Timezone

This field specifies the time zone in which the user accesses the OpenSSO Enterprise console. There is no default value.

Administrator Starting View

If this user is a OpenSSO Enterprise administrator, this field specifies the node that would be the starting point displayed in the OpenSSO Enterprise console when this user logs in. There is no default value. A valid DN for which the user has, at the least, read access can be used.

Default User Status

This option indicates the default status for any newly created user. This status is superseded by the User Entry status. Only active users can authenticate through OpenSSO Enterprise. The default value is Active. Either of the following can be selected from the pull-down menu:

Active — The user can authenticate through OpenSSO Enterprise.

Inactive — The user cannot authenticate through OpenSSO Enterprise, but the user profile remains stored in the directory.

The individual user status is set by registering the User service, choosing the value, applying it to a role and adding the role to the user's profile.

System Properties

System Properties contain the following default services that you can configure:

Client Detection

An initial step in the authentication process is to identify the type of client making the HTTP(S) request. This OpenSSO Enterprise feature is known as client detection. The URL information is used to retrieve the client's characteristics. Based on these characteristics, the appropriate authentication pages are returned. For example, when a Netscape browser is used to request a web page, OpenSSO Enterprise 8.0 displays an HTML login page. Once the user is validated, the client type (Netscape browser) is added to the session token. The attributes defined in the Client Detection service are global attributes.

Default Client Type

This attribute defines the default client type derived from the list of client types in the Client Types attribute. The default is genericHTML.

Client Detection Class

This attribute defines the client detection class for which all client detection requests are routed. The string returned by this attribute should match one of the client types listed in the Client Types attribute. The default client detection class is `com.sun.mobile.cdm.FEDIClientDetector`. OpenSSO Enterprise also contains `com.iplanet.services.cdm.ClientDetectionDefaultImpl`.

Enable Client Detection

Enables client detection. If client detection is enabled (default), every request is routed thought the class specified in the Client Detection Class attribute. By default, the client detection capability is enabled. If this attribute is not selected, OpenSSO Enterprise assumes that the client is genericHTML and will be accessed from a HTML browser.

Logging

The Logging service provides status and error messages related to OpenSSO Enterprise administration. An administrator can configures values such as log file size and log file location. OpenSSO Enterprise can record events in flat text files or in a relational database. The Logging service attributes are global attributes. The attributes are:

Maximum Log Size

This attribute accepts a value for the maximum size (in bytes) of a OpenSSO Enterprise log file. The default value is 100000000.

The files only apply to the FILE logging type. When the logging type is set to DB, there are no history files and limit explicitly set by OpenSSO Enterprise to the size of the files.

Number of History Files

This attribute has a value equal to the number of backup log files that will be retained for historical analysis. Any integer can be entered depending on the partition size and available disk space of the local system. The default value is 1.

The files only apply to the FILE logging type. When the logging type is set to DB, there are no history files and limit explicitly set by OpenSSO Enterprise to the size of the files.

Note – Entering a value of 0 is interpreted to be the same as a value of 1, meaning that if you specify 0, a history log file will be created.

Log File Location

The file-based logging function needs a location where log files can be stored. . The default location is:

OpenSSO-deploy-base/*uri*/`log`

OpenSSO-deploy-base/*uri*/`log`are tags representing the base configuration directory and the OpenSSO Enterprise deployment URI. each specified during post-installation configuration. At runtime, the logging service determines the instance's proper directory for logging. This attribute's value can be set to an explicit path , but the base path should be its configuration directory (the value of *OpenSSO-deploy-base*) to avoid permissions problems.

If a non-default directory is specified, OpenSSO Enterprise will create the directory if it does not exist. You should then set the appropriate permissions for that directory (for example, 0700).

When configuring the log location for DB (database) logging (such as, Oracle or MySQL), part of the log location is case sensitive. For example, if you are logging to an Oracle database, the log location should be (note case sensitivity):

```
jdbc:oracle:thin:@machine.domain:port:DBName
```

To configure logging to DB, add the JDBC driver files to the web container's JVM classpath. You need to manually add JDBC driver files to the classpath of the `ssoadm` script, otherwise `ssoadm` logging can not load the JDBC driver.

Changes to logging attributes usually take effect after you save them. This does not require you to restart the server. If you are changing to secure logging, however, you should restart the server.

Log Status

Specifies whether logging is turned on (ACTIVE) or off (INACTIVE). Value is set to ACTIVE during installation.

Log Record Resolve Host Name

If set to false, host lookups will not be performed to populate the LogRecord's HostName field.

Logging Type

Enables you to specify either File, for flat file logging, or DB for database logging.

If the Database User Name or Database User Password is invalid, it will seriously affect OpenSSO Enterprise processing. If OpenSSO Enterprise or the console becomes unstable, you set the Log Status attribute to Inactive.

After you have set the property, restart the server. You can then log in to the console and reset the logging attribute. Then, change the Log Status property to *ACTIVE* and restart the server.

Database User Name

This attribute accepts the name of the user that will connect to the database when the Logging Type attribute is set to DB.

Database User Password

This attribute accepts the database user password when the Logging Type attribute is set to DB.

Database User Password (confirm)

Confirm the database password.

Database Driver Name

This attribute enables you to specify the driver used for the logging implementation class.

Configurable Log Fields

Represents the list of fields that are to be logged. By default, all of the fields are logged. The fields are:

- CONTEXTID
- DOMAIN
- HOSTNAME
- IPADDRESS
- LOGGED BY
- LOGINID
- LOGLEVEL
- MESSAGEID
- MODULENAME
- NAMEID

At minimum you should log CONTEXTID, DOMAIN, HOSTNAME, LOGINID and MESSAGEID.

Log Verification Frequency

This attribute sets the frequency (in seconds) that the server should verify the logs to detect tampering. The default time is 3600 seconds. This parameter applies to secure logging only.

Log Signature Time

This parameter sets the frequency (in seconds) that the log will be signed. The default time is 900 seconds. This parameter applies to secure logging only.

Secure Logging

This attribute enables or disables secure logging. By default, secure logging is off. Secure Logging enables detection of unauthorized changes or tampering of security logs.

Note – Secure logging can only be used for flat files. This option does not work for Database (DB) logging.

Secure Logging Signing Algorithm

This attribute defines RSA and DSA (Digital Signature Algorithm), which have private keys for signing and a public key for verification. You can select from the following:

- MD2 w/RSA
- MD5 w/RSA
- SHA1 w/DSA
- SHA1 w/RSA

MD2, MD5 and RSA are one-way hashes. For example, if you select the signing algorithm MD2 w/RSA, the secure logging feature generates a group of messages with MD2 and encrypts the value with the RSA private key. This encrypted value is the signature of the original logged records and will be appended to the last record of the most recent signature. For validation, it well decrypt the signature with the RSA public key and compare the decrypted value to the group of logged records. The secure logging feature will then will detect any modifications to any logged record.

Logging Certificate Store Location

When secure logging is enabled, the logging service looks for its certificate at the location specified by this attribute. The actual directory path is determined at runtime. The value can be set to an explicit path, but the base path should be accessible by the OpenSSO Enterprise instance.

The default value is *OpenSSO-deploy-base*/*uri*/`Logger.jks`.

Maximum Number of Records

This attribute sets the maximum number of records that the Java LogReader interfaces return, regardless of how many records match the read query. By default, it is set to 500. This attribute can be overridden by the caller of the Logging API through the *LogQuery* class.

Number of Files per Archive

This attribute is only applicable to secure logging. It specifies when the log files and keystore need to be archived, and the secure keystore regenerated, for subsequent secure logging. The default is five files per logger.

Buffer Size

This attribute specifies the maximum number of log records to be buffered in memory before the logging service attempts to write them to the logging repository. The default is one record.

DB Failure Memory Buffer Size

This attribute defines the maximum number of log records held in memory if database (DB) logging fails. This attribute is only applicable when DB logging is specified. When the OpenSSO Enterprise logging service loses connection to the DB, it will buffer up to the number of records specified. This attribute defaults to two times of the value defined in the Buffer Size attribute.

Buffer Time

This attribute defines the amount of time that the log records will be buffered in memory before they are sent to the logging service to be written. This attribute applies if Time Buffering is ON. The default is 3600 seconds.

Time Buffering

When selected as ON, OpenSSO Enterprise will set a time limit for log records to be buffered in memory before they are written. The amount of time is set in the Buffer Time attribute.

Logging Level

Use this attribute to configure the degree of detail for all OpenSSO Enterprise log files. the default is the INFO level. FINE, FINER, FINEST provide more detail and more log records. In addition there is a level OFF that can be used to turn off logging, which is essentially the same as setting the Log Status attribute to INACTIVE..

Naming

The Naming service is used to get and set URLs, plug-ins and configurations as well as request notifications for various other OpenSSO Enterprise services such as session, authentication, logging, SAML and Federation.

This service enables clients to find the correct service URL if the platform is running more than one OpenSSO Enterprise. When a naming URL is found, the naming service will decode the session of the user and dynamically replace the protocol, host, and port with the parameters from the session. This ensures that the URL returned for the service is for the host that the user session was created on. The Naming attributes are:

- "Profile Service URL" on page 254
- "Session Service URL" on page 254
- "Logging Service URL" on page 254
- "Policy Service URL" on page 254
- "Authentication Service URL" on page 255
- "SAML Web Profile/Artifact Service URL" on page 255
- "SAML SOAP Service URL" on page 255

Profile Service URL

This field takes a value equal to :

```
%protocol://%host:%port/Server_DEPLOY_URI/profileservice
```

This syntax allows for dynamic substitution of the profile URL based on the specific session parameters.

Session Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/sessionservice
```

This syntax allows for dynamic substitution of the session URL based on the specific session parameters.

Logging Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/loggingservice
```

This syntax allows for dynamic substitution of the logging URL based on the specific session parameters.

Policy Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/policyservice
```

This syntax allows for dynamic substitution of the policy URL based on the specific session parameters.

Authentication Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/authservice
```

This syntax allows for dynamic substitution of the authentication URL based on the specific session parameters.

SAML Web Profile/Artifact Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/SAMLAwareServlet
```

This syntax allows for dynamic substitution of the SAML web profile/artifact URL based on the specific session parameters.

SAML SOAP Service URL

This field takes a value equal to

```
%protocol://%host:%port/Server_DEPLOY_URI/SAMLSOAPReceiver
```

This syntax allows for dynamic substitution of the SAML SOAP URL based on the specific session parameters.

SAML Web Profile/POST Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/SAMLPOSTProfileServlet
```

This syntax allows for dynamic substitution of the SAML web profile/POST URL based on the specific session parameters.

SAML Assertion Manager Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/AssertionManagerServlet/AssertionM
anagerIF
```

This syntax allows for dynamic substitution of the SAML Assertion Manager Service URL based on the specific session parameters.

Federation Assertion Manager Service URL

This field takes a value equal to:

```
%protocol://%host:%port/amserver/FSAssertionManagerServlet/FSAssertionMana
gerIF
```

This syntax allows for dynamic substitution of the Federation Assertion Manager Service URL based on the specific session parameters.

Security Token Manager URL

This field takes a value equal to:

```
%protocol://%host:%port/amserver/SecurityTokenManagerServlet/SecurityToken
ManagerIF/
```

This syntax allows for dynamic substitution of the Security Token Manager URL based on the specific session parameters.

JAXRPC Endpoint URL

This field takes a value equal to:

```
%protocol://%host:%port/amserver/jaxrpc/
```

This syntax allows for dynamic substitution of the JAXRPC Endpoint URL based on the specific session parameters.

Identity Web Services Endpoint URL

This field takes a value equal to:

```
%protocol://%host:%port%uri/identityservices/
```

This syntax allows for dynamic substitution of the Identity Web Services Endpoint URL based on the specific session parameters.

Identity REST Services Endpoint URL

This field takes a value equal to:

```
%protocol://%host:%port%uri/identity//
```

This syntax allows for dynamic substitution of the Identity REST Services Endpoint URL based on the specific session parameters.

Security Token Service Endpoint URL

This field takes a value equal to:

```
%protocol://%host:%port%uri/sts
```

This syntax allows for dynamic substitution of the Security Token Service Endpoint URL based on the specific session parameters.

Security Token Service MEX Endpoint URL

This field takes a value equal to:

```
%protocol://%host:%port%uri/sts/mex
```

This syntax allows for dynamic substitution of the Security Token Service MEX Endpoint URL based on the specific session parameters.

Platform

The Platform service is where additional servers can be added to the OpenSSO Enterprise configuration as well as other options applied at the top level of the OpenSSO Enterprise application. The Platform service attributes are global attributes. The attributes are:

Platform Locale

The platform locale value is the default language subtype that OpenSSO Enterprise was installed with. The authentication, logging and administration services are administered in the language of this value. The default is en_US. See "Supported Language Locales" on page 218for a listing of supported language subtypes.

Cookie Domains

The list of domains that will be returned in the cookie header when setting a cookie to the user's browser during authentication. If empty, no cookie domain will be set. In other words, the OpenSSO Enterprise session cookie will only be forwarded to the OpenSSO Enterprise itself and to no other servers in the domain.

If SSO is required with other servers in the domain, this attribute must be set with the cookie domain. If you had two interfaces in different domains on one OpenSSO Enterprise then you

would need to set both cookie domains in this attribute. If a load balancer is used, the cookie domain must be that of the load balancer's domain, not the servers behind the load balancer. The default value for this field is the domain of the installed OpenSSO Enterprise.

Hex Encode Cookies

If set to yes, this attribute enable hex encoding for cookies. The default is No.

Client Character Sets

This attribute specifies the character set for different clients at the platform level. It contains a list of client types and the corresponding character sets.

▼ To Specify a New Character Set

1. **Click New from the Client Character Sets list.**
2. **Enter a value for the Client Type.**
3. **Enter a value for the Character Set. See "Supported Language Locales" on page 218 for the character sets available.**
4. **Click OK.**
5. **Click Save in the Platform Service main page.**

Servers and Sites

The Servers and Sites configuration attributes allow for centralized configuration management of sites and servers for the entire deployment.

Multiple (two or more) OpenSSO Enterprise instances can be deployed on at least two different host servers. For example, you might deploy two instances on one server and a third instance on another server. Or you might deploy all instances on different servers. You can also configure the OpenSSO Enterprise instances in session failover mode, if required for your deployment.

One or more load balancers route client requests to the various OpenSSO Enterprise instances. You configure each load balancer according to your deployment requirements (for example, to use round-robin or load average) to distribute the load between the OpenSSO Enterprise instances. A load balancer simplifies the deployment, as well as resolves issues such as a firewall

between the client and the back-end OpenSSO Enterprise servers. You can use a hardware or software load balancer with your OpenSSO Enterprise deployment. All OpenSSO Enterprise instances access the same Directory Server.

Caution – If you make any changes to the configuration attributes for Servers and Sites, either through the console or the command line interface, you must restart the web container on which OpenSSO Enterprise is deployed for the changes to take effect.

▼ To Create a New Server Instance

An entry for each server is automatically created in the server list when the OpenSSO Enterprise Configurator is run for server configuration. Under normal circumstances, these steps should not be required.

1. **Log into the OpenSSO Enterprise console as the top-level administrator.**
2. **Click the Configuration tab and then click Sites and Servers.**
3. **Click New in the Servers list.**
4. **Enter the FQDN of the server that you wish to add and click OK.**

   The FQDN should be in the format of `http`*(s)*`://`*host.domain*`:`*port*`/`*uri*.
5. **The newly created server instance appears in the list.**
6. **To edit the server, click on the name of the server. The configuration attributes for the server are available for you to customize.**

   The Default Server Settings are the set of default values for server instances. Each server instance needs to have a minimum set of properties values and most of the properties values, depending on your deployment, can be the same for all server instance. This setting allows you to enter the basic properties in one place, without having to change hem for each additional server instance.

   These default values can be overwritten. This done by clicking on the Inheritance Settings button, located at the top of the server instance profile page. After this button is clicked, the console displays a page where you can select and deselect which values to inherit or overwrite.

Inheritance Settings

The Inheritance Settings allow you to select which default values can be overwritten for each server instance. Make sure that the attributes that you wish to define for the server instance are unchecked, and then click Save.

General

The General attributes configure basic configuration data for your centralized server management.

Site Attributes

The site attribute is:

Parent Site

This attribute maps the load balancer Site Name (site ID) to the OpenSSO Enterprise server. Note that the site must be created before you can add the site.

System Attributes

The system attributes list location information for the server instance:

Base Installation Directory

Specifies the base directory where product's data resides.

Default Locale

The locale value is the default language subtype that OpenSSO Enterprise was installed with. The default is `en_us`.

Notification URL

The location of notification service end point. This value is set during installation.

XML Validation

Default value is no. Determines if validation is required when parsing XML documents using the OpenSSO Enterprise `XMLUtils` class. This property is in effect only when value for the

Debug Level attribute is set to warning or message. Allowable values are yes and no. The XML document validation is turned on only if the value for this property yes, and if value for Debug Level attribute is set to warning or message.

Debugging Attributes

The Debugging attributes list basic error checking information:

Debug Level

Specifies debug level. Default value is error. Possible values are:

- off — No debug file is created.
- error — Only error messages are logged.
- warning — Only warning messages are logged.
- message — Error, warning, and informational messages are logged.

Merge Debug Files

If set to on, the server directs all debug data to a single file (`debug.out`). If set to OFF, the server creates separate per-component debug files.

Debug Directory

Specifies the output directory where debug files will be created. Value is set during installation. Example: *OpenSSO-deploy-base*`/`*uri*`/debug`.

Mail Server

The Mail Server attributes list the host name and port for the mail server:

Mail Server Host Name

Default value is `localhost`. Specifies the mail server host.

Mail Server Port Number

Default value is 25. Specifies the mail server port.

Security

The Security attributes define encryption, validation and cookie information to control the level of security for the server instance.

Encryption

The encryption attributes are:

Password Encryption Key

Specifies the key used to encrypt and decrypt passwords and is stored in the Service Management System configuration. Value is set during installation. Example: `dSB9LkwPCSoXfIKHVMhIt3bKgibtsggd`

Authentication Service Shared Secret

The shared secret for application authentication module. Value is set during installation. Example: `AQICPX9e1cxSxB2RSy1WG1+O4msWpt/6djZl`

Encryption Class

Default value is `com.iplanet.services.util.JCEEncryption`. Specifies the encrypting class implementation. Available classes are: `com.iplanet.services.util.JCEEncryption` and `com.iplanet.services.util.JSSEncryption`.

Secure Random Factory Class

Default value is `com.iplanet.am.util.JSSSecureRandomFactoryImpl`. Specifies the factory class name for `SecureRandomFactory`. Available implementation classes are: `com.iplanet.am.util.JSSSecureRandomFactoryImpl` which uses JSS, and `com.iplanet.am.util.SecureRandomFactoryImpl` which uses pure Java.

Validation

The validation attributes are:

Platform Low Level Comm. Max. Content Length

Default value is 16384 or 16k. Specifies the maximum content-length for an `HttpRequest` that OpenSSO Enterprise will accept.

Client IP Address Check

Default value is NO. Specifies whether or not the IP address of the client is checked in all `SSOToken` creations or validations.

Cookie

The cookie attributes are:

Cookie Name

Default value is `iPlanetDirectoryPro`. Cookie name used by Authentication Service to set the valid session handler ID. The value of this cookie name is used to retrieve the valid session information.

Secure Cookie

Allows the OpenSSO Enterprise cookie to be set in a secure mode in which the browser will only return the cookie when a secure protocol such as `HTTP(s)` is used. Default value is false.

Encode Cookie Value

This property allows OpenSSO Enterprise to `URLencode` the cookie value which converts characters to ones that are understandable by HTTP.

Keystore

The following attributes allow you to configure keystore information for additional sites and servers that you create:

Keystore File

Value is set during installation. Example: *OpenSSO-deploy-base*/*URI*/`keystore.jks`. Specifies the path to the SAML XML keystore password file.

Keystore Password File

Value is set during installation. Example: *OpenSSO-deply-base*/*URI*/`.storepass`. Specifies the path to the SAML XML key storepass file.

Private Key Password File

Value is set during installation. Example: *OpenSSO-deploy-base*/*URI*/`.keypass` Specifies the path to the SAML XML key password file.

Certificate Alias

Default value is test.

Certificate Revocation List Caching

These attributes define the local Certificate Revocation List (CRL) caching repository that is used for keeping the CRL from certificate authorities. Any service that needs to obtain a CRL for certificate validation will receive the CRL based on this information.

LDAP Server Host Name

Specifies the name of the LDAP server where the certificates are stored. The default value is the host name specified when OpenSSO Enterprise was installed. The host name of any LDAP Server where the certificates are stored can be used.

LDAP Server Port Number

Specifies the port number of the LDAP server where the certificates are stored. The default value is the port specified when OpenSSO Enterprise was installed. The port of any LDAP Server where the certificates are stored can be used.

SSL Enabled

Specifies whether to use SSL to access the LDAP server. The default is that the Certificate Authentication service does not use SSL for LDAP access.

LDAP Server Bind User Name

Specifies the bind DN in the LDAP server.

LDAP Server Bind Password

Defines the password to be used for binding to the LDAP server. By default, the amldapuser password that was entered during installation is used as the bind user.

LDAP Search Base DN

This attribute specifies the base DN used by the LDAP Users subject in the LDAP server from which to begin the search. By default, it is the top-level realm of the OpenSSO Enterprise installation base.

Search Attributes

Any DN component of issuer's `subjectDN` can be used to retrieve a CRL from a local LDAP server. It is a single value string, like, "cn". All Root CAs need to use the same search attribute.

Online Certificate Status Protocol Check

The Online Certificate Status Protocol (OCSP) enables OpenSSO Enterprise services to determine the (revocation) state of a specified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.

Check Enabled

This attribute enables OCSP checking. It is enabled by default.

Responder URL

This attribute defines is a URL that identifies the location of the OCSP responder. For example, `http://ocsp.example.net:80`.

By default, the location of the OCSP responder is determined implicitly from the certificate being validated. The property is used when the Authority Information Access extension (defined in RFC 3280) is absent from the certificate or when it requires overriding.

Certificate Nickname

The OCSP responder nickname is the CA certificate nick name for that responder, for example `Certificate Manager - sun`. If set, the CA certificate must be presented in the web server's certificate database. If the OCSP URL is set, the OCSP responder nickname must be set also. Otherwise, both will be ignored. If they are not set, the OCSP responder URL presented in user's certificate will be used for OCSP validation. If the OCSP responder URL is not presented in user's certificate, no OCSP validation will be performed.

Federal Information Processing Standards

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

FIPS Mode

This property can be true or false. All the cryptography operations will be running FIPS compliant mode only if it is true.

Session

The session attributes allow you to configure session information for a additional site and server instances.

Session Limits

The following attributes set server session limits:

Maximum Sessions

Default value is 5000. Specify the maximum number of allowable concurrent sessions. Login sends a Maximum Sessions error if the maximum concurrent sessions value exceeds this number.

Invalidate Session Max Time

Default value is 3. Specifies the number of minutes after which the invalid session will be removed from the session table if it is created and the user does not login. This value should always be greater than the timeout value in the Authentication module properties file.

Session Purge Delay

Default value is 0. Specifies the number of minutes to delay the purge session operation. After a session times out, this is an extended time period during which the session continues to reside in the session server. This property is used by the client application to check if the session has timed out through SSO APIs. At the end of this extended time period, the session is destroyed. The session is not sustained during the extended time period if the user logs out or if the session is explicitly destroyed by an OpenSSO Enterprise component. The session is in the INVALID state during this extended period.

Statistics

The following attributes set statistical configuration:

Logging Interval

Default value is 60. Specifies number of minutes to elapse between statistics logging. Minimum is 5 seconds to avoid CPU saturation. OpenSSO Enterprise assumes any value less than 5 seconds to be 5 seconds.

State

Default value is file. Specifies location of statistics log. Possible values are:

- off — No statistics are logged.
- file — Statistics are written to a file under the specified directory.
- console — Statistics are written into Web Server log files.

Directory

Value is set during installation. Example: *OpenSSO Enterprise-base*`/`*server-URI*`/stats`. Specifies directory where debug files are created.

Enable Host Lookup

Default value is false. Enables or disables host lookup during session logging.

Notification

The following attributes set notification configuration:

Notification Pool Size

Default value is 10. Defines the size of the pool by specifying the total number of threads.

Notification Thread Pool Threshold

Default value is 100. Specifies the maximum task queue length. When a notification task comes in, it is sent to the task queue for processing. If the queue reaches the maximum length, further incoming requests will be rejected along with a `ThreadPoolException`, until the queue has a vacancy.

Validation

The following attribute sets validation configuration:

Case Insensitive Client DN Comparison

Default value is true. Compares the Agent DN. If the value is false, the comparison is case-sensitive.

SDK

The SDK attributes set configuration definitions for the back-end data store.

Data Store

The Data Store attributes basic datastore configuration:

Enable Datastore Notification

Specifies if the back-end datastore notification is enabled. If this value is set to 'false', then in-memory notification is enabled.

Enable Directory Proxy

The default is false. The purpose of this flag is to report to Service Management that the Directory Proxy must be used for read, write, and/or modify operations to the Directory Server. This flag also determines if ACIs or delegation privileges are to be used. This flag must be set to "true" when the Access Manager SDK (from version 7 or 7.1) is communicating with Access Manager version 6.3.

For example, in the co-existence/legacy mode this value should be "true". In the legacy DIT, the delegation policies were not supported. Only ACIs were supported, so o to ensure proper delegation check, this flag must be set to 'true' in legacy mode installation to make use of the ACIs for access control. Otherwise the delegation check will fail.

In realm mode, this value should be set to false so only the delegation policies are used for access control. In version 7.0 and later, Access Manager or OpenSSO Enterprise supports data-agnostic feature in realm mode installation. So, in addition to Directory Server, other servers may be used to store service configuration data. Additionally, this flag will report to the Service Management feature that the Directory Proxy does not need to be used for the read, write, and/or modify operations to the back-end storage. This is because some data stores, like Active Directory, may not support proxy.

Notification Pool Size

Default value is 10. Defines the size of the pool by specifying the total number of threads.

Event Service

The following attributes define event service notification for the data store:

Number of Retries for Event Service Connections

Default value is 3. Specifies the number of attempts made to successfully re-establish the Event Service connections.

Delay Between LDAP Connection Tries

Default value is 3000. Specifies the delay in milliseconds between retries to re-establish the Event Service connections.

Error Codes for LDAP Connection Tries

Default values are 80,81,91. Specifies the LDAP exception error codes for which retries to re-establish Event Service connections will trigger.

Idle Timeout

Default value is 0. Specifies the number of minutes after which the persistent searches will be restarted.

This property is used when a load balancer or firewall is between the policy agents and the Directory Server, and the persistent search connections are dropped when TCP idle timeout occurs. The property value should be lower than the load balancer or firewall TCP timeout. This ensures that the persistent searches are restarted before the connections are dropped. A value of 0 indicates that searches will not be restarted. Only the connections that are timed out will be reset.

Disabled Event Service Connection

Specifies which event connection can be disabled. Values (case insensitive) can be:

- aci — Changes to the aci attribute, with the search using the LDAP filter (aci=*).
- sm — Changes in the OpenSSO Enterprise information tree (or service management node), which includes objects with the `sunService` or `sunServiceComponent` marker object class. For example, you might create a policy to define access privileges for a protected resource, or you might modify the rules, subjects, conditions, or response providers for an existing policy.
- um — Changes in the user directory (or user management node). For example, you might change a user's name or address.

For example, to disable persistent searches for changes to the OpenSSO Enterprise information tree (or service management node):

```
com.sun.am.event.connection.disable.list=sm
```

Caution – Persistent searches cause some performance overhead on Directory Server. If you determine that removing some of this performance overhead is absolutely critical in a production environment, you can disable one or more persistent searches using this property.

However, before disabling a persistent search, you should understand the limitations described above. It is strongly recommended that this property not be changed unless absolutely required. This property was introduced primarily to avoid overhead on Directory Server when multiple 2.1 J2EE agents are used, because each of these agents establishes these persistent searches. The 2.2 J2EE agents no longer establish these persistent searches, so you might not need to use this property.

Disabling persistent searches for any of these components is not recommended, because a component with a disabled persistent search does not receive notifications from Directory Server. Consequently, changes made in Directory Server for that particular component will not be notified to the component cache. For example, if you disable persistent searches for changes in the user directory (`um`), OpenSSO Enterprise will not receive notifications from Directory Server. Therefore, an agent would not get notifications from OpenSSO Enterprise to update its local user cache with the new values for the user attribute. Then, if an application queries the agent for the user attributes, it might receive the old value for that attribute.

Use this property only in special circumstances when absolutely required. For example, if you know that Service Configuration changes (related to changing values to any of services such as Session Service and Authentication Services) will not happen in production environment, the persistent search to the Service Management (`sm`) component can be disabled. However, if any changes occur for any of the services, a server restart would be required. The same condition also applies to other persistent searches, specified by the `aci` and `um` values.

LDAP Connection

The following attributes set connection data for the back end data store:

Number of Retries for LDAP Connection

Default is 1000. Specifies the number milliseconds between retries.

Delay Between LDAP Connection Retries

Default value is 3. Specifies the number of attempts made to successfully re-establish the LDAP connection.

Error Codes for LDAP Connection Retries

Default values are 80,81,91. Specifies the `LDAPException` error codes for which retries to re-establish the LDAP connection will trigger.

Caching and Replica

The following attributes define caching and replication configuration:

SDK Caching Max. Size

Default value is 10000. Specifies the size of the SDK cache when caching is enabled. Use an integer greater than 0, or the default size (10000 users) will be used.

SDK Replica Retries

Default value is 0. Specifies the number of times to retry.

Delay Between SDK Replica Tries

Default value is 1000. Specifies the number of milliseconds between retries.

Time To Live Configuration

Cache Entry Expiration Enabled

When enabled, the cache entries will expire based on the time specified in User Entry Expiration Time attribute.

User Entry Expiration Time

This attribute specifies time in minutes for which the user entries remain valid in the cache after their last modification. After this specified period of time elapses (after the last modification/read from the Directory Server), the data for the entry that is cached will expire. At this point, new requests for data for these user entries are read from the Directory Server.

Default Entry Expiration Time

This attribute specifies the time in minutes for which the non-user entries remain valid in the cache after their last modification. After this specified period of time elapses (after the last modification/read from the Directory Server), the data for the entry that is cached will expire. At this point, new requests for data for these non-user entries are read from the Directory Server.

Directory Configuration

The Directory Configuration attributes define basic configuration information for the embedded directory store:

Directory Configuration

The Directory Configuration attributes are:

Minimum Connection Pool

Specifies the minimal size of connection pools to be used for connecting to the Directory Server, as specified in the LDAP server attribute. The default is 1.

Maximum Connection Pool

This attribute specifies the maximum size of connection pools to be used for connecting to the Directory Server, as specified in the LDAP server attribute. The default is 10.

Bind DN

Specifies the bind DN in the LDAP server.

Bind Password

Defines the password to be used for binding to the LDAP server. By default, the amldapuser password that was entered during installation is used as the bind user.

Server

This attribute defines the directory server that will serve as the configuration data store for the OpenSSO Enterprise instance. To add a configuration server, click the Add button, and provide values for the following attributes:

Name	Enter a name for the server.
Host Name	Specifies fully-qualified host name of the Directory Server. For example: *DirectoryServerHost.domainName*`.com`
Port Number	Specifies the Directory Server port number .
Connection Type	Defines the connection type for the Directory Server. By default, SIMPLE is selected. You can also choose SSL.

Legacy Configuration

The following attribute define basic directory-server configurations for Legacy mode instances of OpenSSO Enterprise. These attributes will only appear in a Legacy mode installation.

Minimum Connection Pool

Specifies the minimal size of connection pools to be used for connecting to the Directory Server, as specified in the LDAP server attribute. The default is 1.

Maximum Connection Pool

This attribute specifies the maximum size of connection pools to be used for connecting to the Directory Server, as specified in the LDAP server attribute. The default is 10.

Server

This attribute lists the load balancer protocol, host name, and port. For example: `http://lb.example.com:80`.

Advanced

The advanced properties enable an administrator to select and add values to server configuration properties that are not present in the OpenSSO Enterprise Console. All Server and Sites properties were located in the `AMConfig.properties` file in previous releases.

In addition to the default properties displayed in the Advance table of the console, the following properties can be added.

```
am.encryption.pwd=
am_load_balancer_cookie=
com.iplanet.am.clientIPCheckEnabled=true,false
com.iplanet.am.console.deploymentDescriptor=
com.iplanet.am.console.host=
com.iplanet.am.console.port=integer
com.iplanet.am.console.protocol=https,http
com.iplanet.am.console.remote=true,false
com.iplanet.am.cookie.encode=true,false
com.iplanet.am.cookie.name=
com.iplanet.am.cookie.secure=true,false
com.iplanet.am.directory.host=
com.iplanet.am.directory.port=integer
com.iplanet.am.directory.ssl.enabled=true,false
com.iplanet.am.domaincomponent=
```

```
com.iplanet.am.event.connection.delay.between.retries=integer
com.iplanet.am.event.connection.ldap.error.codes.retries=
com.iplanet.am.event.connection.num.retries=integer
com.iplanet.am.jssproxy.checkSubjectAltName=true,false
com.iplanet.am.jssproxy.resolveIPAddress=true,false
com.iplanet.am.jssproxy.SSLTrustHostList=
com.iplanet.am.jssproxy.trustAllServerCerts=true,false
com.iplanet.am.lbcookie.name=
com.iplanet.am.lbcookie.value=
com.iplanet.am.ldap.connection.delay.between.retries=integer
com.iplanet.am.ldap.connection.ldap.error.codes.retries=
com.iplanet.am.ldap.connection.num.retries=integer
com.iplanet.am.locale=
com.iplanet.am.notification.threadpool.size=integer
com.iplanet.am.notification.threadpool.threshold=integer
com.sun.identity.client.notification.url=
com.iplanet.am.replica.delay.between.retries=integer
com.iplanet.am.replica.num.retries=integer
com.iplanet.am.rootsuffix=
com.iplanet.am.sdk.cache.entry.default.expire.time=integer
com.iplanet.am.sdk.cache.entry.expire.enabled=true,false
com.iplanet.am.sdk.cache.entry.user.expire.time=integer
com.iplanet.am.sdk.cache.maxSize=integer
com.iplanet.am.sdk.caching.enabled=true,false
com.iplanet.am.sdk.ldap.debugFileName=
com.iplanet.am.sdk.package=
com.iplanet.am.sdk.remote.pollingTime=integer
com.iplanet.am.server.host=
com.iplanet.am.server.port=integer
com.iplanet.am.server.protocol=https,http
com.iplanet.am.serverMode=true,false
com.iplanet.am.service.secret=
com.iplanet.am.services.deploymentDescriptor=
com.iplanet.am.session.client.polling.enable=true,false
com.iplanet.am.session.client.polling.period=integer
com.iplanet.am.session.failover.cluster.stateCheck.period=integer
com.iplanet.am.session.failover.cluster.stateCheck.timeout=integer
com.iplanet.am.session.failover.httpSessionTrackingCookieName=
com.iplanet.am.session.failover.sunAppServerLBRoutingCookieName=
com.iplanet.am.session.failover.useInternalRequestRouting=true,false
com.iplanet.am.session.failover.useRemoteSaveMethod=true,false
com.iplanet.am.session.invalidsessionmaxtime=integer
com.iplanet.am.session.maxSessions=integer
com.iplanet.am.session.protectedPropertiesList=
com.iplanet.am.session.purgedelay=integer
com.iplanet.am.smtphost=
com.iplanet.am.smtpport=integer
```

```
com.iplanet.am.stats.interval=integer
com.iplanet.am.util.xml.validating=on,off
com.iplanet.am.version=
com.iplanet.security.SSLSocketFactoryImpl=
com.iplanet.security.SecureRandomFactoryImpl=
com.iplanet.security.encryptor=
com.iplanet.services.cdsso.cookiedomain=
com.iplanet.services.comm.server.pllrequest.maxContentLength=integer
com.iplanet.services.configpath=
com.iplanet.services.debug.directory=
com.sun.identity.configFilePath=
com.iplanet.am.sdk.userEntryProcessingImpl=
com.iplanet.am.profile.host=
com.iplanet.am.profile.port=integer
com.iplanet.am.pcookie.name=
com.iplanet.am.jssproxy.SSLTrustHostList=
com.sun.identity.authentication.ocspCheck=
com.sun.identity.authentication.ocsp.responder.url=
com.sun.identity.authentication.ocsp.responder.nickname=
com.sun.identity.authentication.super.user=
com.sun.identity.password.deploymentDescriptor=
com.iplanet.am.session.httpSession.enabled=
unixHelper.port=integer
com.sun.identity.policy.Policy.policy_evaluation_weights=
unixHelper.ipaddrs=
com.sun.identity.authentication.uniqueCookieDomain=
com.sun.identity.monitoring.local.conn.server.url=
com.sun.identity.monitoring=
com.iplanet.services.debug.level=off,error,warning,message
com.sun.services.debug.mergeall=on,off
com.sun.embedded.sync.servers=on,off
com.sun.embedded.replicationport=integer
com.iplanet.services.stats.directory=
com.iplanet.services.stats.state=off,file,console
com.sun.am.event.connection.disable.list=
com.sun.am.event.connection.idle.timeout=integer
com.sun.am.ldap.connnection.idle.seconds=integer
com.sun.am.ldap.fallback.sleep.minutes=integer
com.sun.am.session.SessionRepositoryImpl=
com.sun.am.session.caseInsensitiveDN=true,false
com.sun.am.session.enableAddListenerOnAllSessions=true,false
com.sun.am.session.enableHostLookUp=true,false
com.sun.am.session.trustedSourceList=
com.sun.identity.agents.true.value=
com.sun.identity.amsdk.cache.enabled=true,false
com.sun.identity.client.encryptionKey=
com.sun.identity.cookieRewritingInPath=true,false
```

```
com.sun.identity.delegation.cache.size=integer
com.sun.identity.enableUniqueSSOTokenCookie=true,false
com.sun.identity.idm.cache.enabled=true,false
com.sun.identity.idm.cache.entry.default.expire.time=integer
com.sun.identity.idm.cache.entry.expire.enabled=true,false
com.sun.identity.idm.cache.entry.user.expire.time=integer
com.sun.identity.jsr196.authenticated.user=
com.sun.identity.jss.donotInstallAtHighestPriority=true,false
com.sun.identity.liberty.ws.util.providerManagerClass=
com.sun.identity.log.logSubdir=
com.sun.identity.loginurl=
com.sun.identity.overrideAMC=true,false
com.sun.identity.plugin.datastore.class.*=
com.sun.identity.security.checkcaller=true,false
com.sun.identity.security.x509.pkg=
com.sun.identity.server.fqdnMap=map
com.sun.identity.session.application.maxCacheTime=integer
com.sun.identity.session.connectionfactory.provider=
com.sun.identity.session.failover.connectionPoolClass=
com.sun.identity.session.httpClientIPHeader=
com.sun.identity.session.polling.threadpool.size=integer
com.sun.identity.session.polling.threadpool.threshold=integer
com.sun.identity.session.repository.cleanupGracePeriod=integer
com.sun.identity.session.repository.cleanupRunPeriod=integer
com.sun.identity.session.repository.dataSourceName=
com.sun.identity.session.repository.enableEncryption=true,false
com.sun.identity.session.repository.healthCheckRunPeriod=integer
com.sun.identity.session.resetLBCookie=true,false
com.sun.identity.session.returnAppSession=true,false
com.sun.identity.sitemonitor.SiteStatusCheck.class=
com.sun.identity.sitemonitor.interval=integer
com.sun.identity.sitemonitor.timeout=integer
com.sun.identity.sm.authservicename.provider=
com.sun.identity.sm.cache.enabled=true,false
com.sun.identity.sm.cacheTime=integer
com.sun.identity.sm.enableDataStoreNotification=true,false
com.sun.identity.sm.flatfile.root_dir=
com.sun.identity.sm.ldap.enableProxy=true,false
com.sun.identity.sm.notification.threadpool.size=integer
com.sun.identity.sm.sms_object_class_name=
com.sun.identity.url.readTimeout=integer
com.sun.identity.url.redirect=
com.sun.identity.urlchecker.invalidate.interval=integer
com.sun.identity.urlchecker.sleep.interval=integer
com.sun.identity.urlchecker.targeturl=
com.sun.identity.util.debug.provider=
com.sun.identity.webcontainer=
```

```
com.sun.identity.wss.discovery.config.plugin=
com.sun.identity.wss.provider.config.plugin=
com.sun.identity.wss.security.authenticator=
com.sun.identity.xmlenc.EncryptionProviderImpl=
s1is.java.util.logging.config.class=
s1is.java.util.logging.config.file=
com.sun.identity.authentication.special.users=
com.sun.identity.auth.cookieName=
com.iplanet.am.naming.failover.url=
com.sun.identity.authentication.uniqueCookieName=
securidHelper.ports=integer
com.iplanet.am.daemons=
bootstrap.file=
com.sun.identity.crl.cache.directory.host=
com.sun.identity.crl.cache.directory.port=integer
com.sun.identity.crl.cache.directory.ssl=true,false
com.sun.identity.crl.cache.directory.user=
com.sun.identity.crl.cache.directory.password=
com.sun.identity.crl.cache.directory.searchlocs=
com.sun.identity.crl.cache.directory.searchattr=
com.sun.identity.authentication.ocspCheck=true,false
com.sun.identity.authentication.ocsp.responder.url=
com.sun.identity.authentication.ocsp.responder.nickname=
com.sun.identity.security.fipsmode=true,false
com.sun.identity.urlconnection.useCache=true,false
com.sun.identity.sm.cache.ttl.enable=true,false
com.sun.identity.sm.cache.ttl=integer
com.sun.identity.common.systemtimerpool.size=integer
com.iplanet.services.cdc.invalidGotoStrings=
```

▼ To Create a New Site Instance

1. **Click New in the Site list.**
2. **Enter the Site Name.**

   This value uniquely identifies the server and allows the possibility of specifying a second entry point (in addition to the primary URL) to the site. This is also used to shorten the cookie length by mapping the server URL to the server ID.
3. **Enter the Primary URL for the site instance, including the site URI.**
4. **Click Save.**

   The created site will appear in the site list in the correct format.

▼ To Edit a Site Instance

1. **Click on the name of the site you wish to edit from the Site list.**
2. **The primary URL for the site is listed in the Primary URL attribute.**
3. **If you wish, add a Secondary URL.**

   The secondary URL provides the connection information for the session repository used for the session failover functionality in OpenSSO Enterprise. The URL of the load balancer should be given as the identifier to this secondary configuration. If the secondary configuration is defined in this case, the session failover feature will be automatically enabled and become effective after the server restart.
4. **Click Save.**

Servers and Sites Console Attribute Maps

The following table lists the Servers and Sites properties that were included in `AMConfig.properties` in previous releases, but are now managed as attributes through the OpenSSO Enterprise console. The properties are listed alphabetically. To search for a particular property, use your browser's Search or Find function.

Property Name	The name of the property located in the `AMConfig.properties` file.
Attribute Name in Console	Is the name of the attribute as it appears in the OpenSSO Enterprise console.
Location in Console	Lists the console location where the attribute is located.

TABLE 7–1 Servers and Sites Attribute Map

Property Name	Attribute Name in Console	Location in Console
am.encryption.pwd	Password Encryption Key	Servers and Sites > Security
com.iplanet.am.clientIPCheckEnabled	Client IP Address Check	Servers and Sites > Security
com.iplanet.am.cookie.encode	Encode Cookie Value	Servers and Sites > Security
com.iplanet.am.cookie.name	Cookie Name	Servers and Sites > Security
com.iplanet.am.cookie.secure	Secure Cookie	Servers and Sites > Security
com.iplanet.am.event.connection.delay.between.retries	Delay Between Event Service Connection Retries	Servers and Sites > SDK

TABLE 7–1 Servers and Sites Attribute Map *(Continued)*

Property Name	Attribute Name in Console	Location in Console
com.iplanet.am.event.connection.ldap.error.codes.retries	Error Codes for Event Service Connection Retries	Servers and Sites > SDK
com.iplanet.am.event.connection.num.retries	Number of retries for Event Service Notification	Servers and Sites > SDK
com.iplanet.am.ldap.connection.delay.between.retries	Number of Retries for LDAP Connection	Servers and Sites > SDK
com.iplanet.am.ldap.connection.ldap.error.codes.retries	Error Codes for LDAP Connection Retries	Servers and Sites > SDK
com.iplanet.am.ldap.connection.num.retries	Delay Between LDAP Connection Retries	Servers and Sites > SDK
com.iplanet.am.locale	Default Locale	Servers and Sites > General
com.iplanet.am.notification.threadpool.size	Notification Pool Size	Servers and Sites > Session
com.iplanet.am.notification.threadpool.threshold	Notification Thread Pool Threshold	Servers and Sites > Session
com.iplanet.am.replica.delay.between.retries	Delay Between SDK Replica Retries	Servers and Sites > SDK
com.iplanet.am.replica.num.retries	SDK Replica Retries	Servers and Sties > SDK
com.iplanet.am.rootsuffix		
com.iplanet.am.sdk.cache.entry.default.expire.time	Default Entry Expiration Time	Servers and Sites > SDK
com.iplanet.am.sdk.cache.entry.expire.enabled	Cached Entry Expiration Enabled	Servers and Sites > SDK
com.iplanet.am.sdk.cache.entry.user.expire.time	User Entry Expiration Time	Servers and Sites > SDK
com.iplanet.am.sdk.cache.maxSize	SDK Caching Max. Size	Servers and Sites > SDK
com.iplanet.am.service.secret	Authentication Service Shared Secret	Servers and Sites > Security
com.iplanet.am.session.invalidsessionmaxtime	Invalid Session Max Time	Servers and Sites > Session
com.iplanet.am.session.maxSessions	Maximum Sessions	Servers and Sites > Session
com.iplanet.am.session.purgedelay	Sessions Purge Delay	Servers and Sites > Session
com.iplanet.am.smtphost	Mail Server Host Name	Servers and Sites > General
com.iplanet.am.smtpport	Mail Server Port Number	Servers and Sites > General
com.iplanet.am.stats.interval	Logging Interval	Servers and Sites > Session
com.iplanet.security.encryptor	Encryption Class	Servers and Sites > Security

TABLE 7–1 Servers and Sites Attribute Map *(Continued)*

Property Name	Attribute Name in Console	Location in Console
com.iplanet.services.comm.server.pll.maxContentLength	Platform Low Level Comm. Max. Content Length	Servers and Sites > Security
com.iplanet.services.configpath	Base Installation Directory	Servers and Sites > General
com.iplanet.services.debug.directory	Debug Directory	Servers and Sites > General
com.iplanet.services.debug.level	Debug Level	Servers and Sites > General
com.iplanet.services.stats.directory	Directory	Servers and Sites > General
com.iplanet.services.stats.state	State	Servers and Sites > Session
com.sun.am.event.connection.disableList	Disabled Even Service Connection	Servers and Sites > SDK
com.sun.am.session.caseInsensitiveDN	Case Insensitive Client DN Comparison	Servers and Sites > Session
com.sun.am.session.enableHostLookUp	Enable Host Lookup	Servers and Sites > Session
com.sun.identity.saml.xmlsig.certalias	Certificate Alias	Servers and Sites > Security
com.sun.identity.saml.xmlsig.keypass	Private Key Password File	Servers and Sites > Security
com.sun.identity.saml.xmlsig.keystore	Keystore File	Servers and Sites > Security
com.sun.identity.saml.xmlsig.storepass	Keystore Password File	Servers and Sites > Security
com.sun.identity.sm.ldap.enableProxy	Enable Directory Proxy	Servers and Sites > SDK

◆ ◆ ◆ CHAPTER 8

Data Store Attributes

This chapter contains definitions of the attributes for configuring the OpenSSO Enterprise data store types. The Active Directory, Generic LDAPv3, and Sun Directory Server with OpenSSO Enterprise Schema data store types share the same underlying plug-in, so the configuration attributes are the same. (The default values for some of the attributes are different for each datastore type and are displayed accordingly in the OpenSSO Enterprise console.) This chapter contains the following sections:

Active Directory Attributes

When configuring Microsoft Active Directory to work with OpenSSO Enterprise, you have to map the predefined properties to properties defined in your instance of Active Directory; this is called attribute mapping. Following are the attributes that need to be defined when adding Active Directory as a data store to a realm.

LDAP Server

Enter the name of the LDAP server to which OpenSSO will be connected in the format *host*.*domain*:*portnumber*. If more than one entry is entered, an attempt is made to connect to the first host in the list. The next entry in the list is tried only if the attempt to connect to the current host fails.

Optionally, a server identifier and site identifier can be appended to the value of the LDAP Server attribute for redundancy. In this case, the format is *host*.*domain*:*portnumber*|*serverID*|*siteID*. These identifiers are assigned to the server when they are configured globally.

- *serverID* specifies a particular server as the primary LDAP server and others as secondary and tertiary (as defined) fallback servers. (If no number is specified, the LDAP server is primary.) The identifier is displayed in the OpenSSO console.
  1. Click the Configuration tab, click the Servers and Sites tab.
  2. Click the appropriate Server Name.
  3. Under the Advanced tab, see the value of the `com.iplanet.am.lbcookie.value` property — for example, `01`.
  4. Click the Configuration tab, click the Servers and Sites tab.
- *siteID* is not currently displayed in the OpenSSO console. It is a two digit number generated internally by OpenSSO — for example, `02`. To find this value, use an LDAP browser to find **`ou=accesspoint,ou=`***site_name*`,ou=com-sun-identity sites,ou=default,ou=GlobalConfig,ou=iPlanetAMPlatformService,ou=services,`***root-suffix*. Under this DN, see **`sunkeyvalue:primary-siteid=`***site-id* for the site identifier.

Caution – This configuration should not be changed for the OpenSSO embedded data store as it may cause inconsistent behavior.

LDAP Bind DN

Specifies the DN name that OpenSSO Enterprise will use to authenticate to the LDAP server to which you are currently connected. The user with the DN name used to bind should have the correct add/modification/delete privileges that you configured in the "LDAPv3 Plugin Supported Types and Operations" on page 299 attribute.

LDAP Bind Password

Specifies the DN password that OpenSSO Enterprise will use to authenticate to the LDAP server to which you are currently connected.

LDAP Bind Password (confirm)

Confirm the password.

LDAP Organization DN

The DN to which this data store repository will map. This will be the base DN of all operations performed in this data store.

LDAP SSL

When enabled, OpenSSO Enterprise will connect to the primary server using the HTTPS protocol.

LDAP Connection Pool Minimum Size

Specifies the initial number of connections in the connection pool. The use of connection pool avoids having to create a new connection each time.

LDAP Connection Pool Maximum Size

Specifies the maximum number of connections to allowed.

Maximum Results Returned from Search

Specifies the maximum number of entries returned from a search operation. If this limit is reached, Active Directory returns any entries that match the search request.

Search Timeout

Specifies the maximum number of seconds allocated for a search request. If this limit is reached, Active Directory returns any search entries that match the search request.

LDAP Follows Referral

If enabled, this option specifies that referrals to other LDAP servers are followed automatically.

LDAPv3 Repository Plugin Class Name

Specifies the location of the class file which implements the LDAPv3 repository.

Attribute Name Mapping

Enables common attributes known to the framework to be mapped to the native data store. For example, if the framework uses `inetUserStatus` to determine user status, it is possible that the native data store actually uses `userStatus`. The attribute definitions are case-sensitive. The defaults are:

- `employeeNumber=distinguishedName`
- `iplanet-am-user-alias-list=objectGUID`
- `mail=userPrincipalName`
- `portalAddress=sAMAccountName`
- `telephonenumber=displayName`
- `uid=sAMAccountName`

LDAPv3 Plugin Supported Types and Operations

Specifies the operations that are permitted to or can be performed on this LDAP server. The default operations that are the only operations that are supported by this LDAPv3 repository plug-in. The following are operations supported by LDAPv3 Repository Plugin:

- Agent: read, create, edit, delete
- Group: read, create, edit, delete
- Realm: read, create, edit, delete, service
- User: read, create, edit, delete, service
- Role: read, create, edit, delete

You can remove permissions from the above list (except role) based on your LDAP server settings and the tasks, but you can not add more permissions. If the configured LDAPv3 Repository plug-in is pointing to an instance of Sun Directory Server, permissions for the type `role` can be added. Otherwise, this permission may not be added because other data stores may not support roles.

If you have `user` as a supported type for the LDAPv3 repository, the read, create, edit, and delete service operations are possible for that user. In other words, if `user` is a supported type, then the read, edit, create, and delete operations allow you to read, edit, create, and delete user entries from the identity repository. The `user=service` operation lets OpenSSO Enterprise services access attributes in user entries. Additionally, the user is allowed to access the dynamic service attributes if the service is assigned to the realm or role to which the user belongs.

The user is also allowed to manage the user attributes for any assigned service. If the user has `service` as the operation (`user=service`), then it specifies that all service-related operations are supported. These operations are `assignService`, `unassignService`, `getAssignedServices`, `getServiceAttributes`, `removeServiceAttributes` and `modifyService`.

LDAPv3 Plug-in Search Scope

Defines the scope to be used to find LDAPv3 plug-in entries. The scope must be one of the following:

- SCOPE_BASE: searches only the base DN.
- SCOPE_ONE: searches only the entries under the base DN.

- SCOPE_SUB (default): searched the base DN and all entries within its subtree.

LDAP Users Search Attribute

This field defines the attribute type to conduct a search for a user. For example, if the user's DN is `uid=user1, ou=people, dc=example, dc=com`, then you would specify `uid` in this field.

LDAP Users Search Filter

Specifies the search filter to be used to find user entries.

LDAP User Object Class

Specifies the object classes for a user. When a user is created, this list of user object classes will be added to the user's attributes list.

LDAP User Attributes

Defines the list of attributes associated with a user. Any attempt to read/write user attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined before you define the object classes and attribute schema here.

Create User Attribute Mapping

Specifies which attributes are required when a user is created. This attribute uses the following syntax:

```
DestinationAttributeName=SourceAttributeName
```

If the source attribute name is missing, the default is the user ID (`uid`). For example:

cn
sn=givenName

Both `cn` and `sn` are required in order to create a user profile. `cn` gets the value of the attribute named `uid`, and `sn` gets the value of the attribute named `givenName`.

Attribute Name of User Status

Specifies the attribute name to indicate if the user is active or inactive.

User Status Active Value

This attribute value is assigned to the user when the user is created. For a user to be active, the Active Directory value is 544. For a user to be inactive, the Active Directory value is 546.

User Status Inactive Value

For Active Directory, this field is not used.

LDAP Groups Search Attribute

This field defines the attribute type for which to conduct a search on a group. The default is `cn`.

LDAP Group Search Filter

Specifies the search filter to be used to find group entries. The default is `(objectclass=groupOfUniqueNames)`.

LDAP Groups Container Naming Attribute

Specifies the naming attribute for a group container, if groups resides in a container. Otherwise, this attribute is left empty. For example, if a group DN of `cn=group1,ou=groups,dc=iplanet,dc=com`resides in `ou=groups`, then the group container naming attribute is `ou`.

LDAP Groups Container Value

Specifies the value for the group container. For example, a group DN of `cn=group1,ou=groups,dc=iplanet,dc=com` resides in a container name `ou=groups`, then the group container value would be `groups`.

LDAP Groups Object Classes

Specifies the object classes for groups. When a group is created, this list of group object classes will be added to the group's attributes list.

LDAP Groups Attributes

Defines the list of attributes associated with a group. Any attempt to read/write group attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined before you define the object classes and attribute schema here.

Attribute Name for Group Membership

Specifies the name of the attribute whose values are the names of all the groups to which DN belongs. The default is `memberOf`.

Attribute Name of Unique Member

Specifies the attribute name whose values is a DN belonging to this group. The default is `uniqueMember`.

Attribute Name of Group Member URL

Specifies the name of the attribute whose value is an LDAP URL which resolves to members belonging to this group. The default is `memberUrl`.

LDAP People Container Naming Attribute

Specifies the naming attribute of the people container if a user resides in a people container. This field is left blank if the user does not reside in a people container.

LDAP People Container Value

Specifies the value of the people container. The default is `people`.

Caution – The entire tree under the `baseDN` will be searched if the value of this attribute is set to null (empty).

Identity Types That Can be Authenticated

Specifies that this data store can authenticate user and/or agent identity types when the authentication module mode for the realm is set to Data Store.

Authentication Naming Attribute

This value is currently not used.

Persistent Search Base DN

Defines the base DN to use for persistent search. Some LDAPv3 servers only support persistent search at the root suffix level.

Persistent Search Filter

Defines the filter that will return the specific changes to directory server entries. The data store will only receive the changes that match the defined filter.

Persistent Search Scope

Defines the scope to be used in a persistent search. The scope must be one of the following:

- SCOPE_BASE – searches only the base DN.
- SCOPE_ONE – searches only the entries under the base DN.
- SCOPE_SUB (default) – searched the base DN and all entries within its subtree.

Persistent Search Maximum Idle Time Before Restart

Defines the maximum idle time before restarting the persistence search. The value must be great than 1. Values less than or equal to 1 will restart the search irrespective of the idle time of the connection.

If OpenSSO Enterprise is deployed with a load balancer, some load balancers will time out if it has been idle for a specified amount of time. In this case, you should set the Persistent Search Maximum Idle Time Before Restart to a value less than the specified time for the load balancer.

Maximum Number of Retries After Error Code

Defines the maximum number of retries for the persistent search operation if it encounters the error codes specified in LDAPException Error Codes to Retry On.

The Delay Time Between Retries

Specifies the time to wait before each retry. This only applies to persistent search connection.

LDAPException Error Codes to Retry

Specifies the error codes to initiate a retry for the persistent search operation. This attribute is only applicable for the persistent search, and not for all LDAP operations.

Caching

If enabled, this allows OpenSSO Enterprise to cache data retrieved from the data store.

Maximum Age of Cached Items

Specifies the maximum time data is stored in the cache before it is removed. The values are defined in seconds.

Maximum Size of the Cache

Specifies the maximum size of the cache. The larger the value, the more data can be stored, but it will require more memory. The values are defined in bytes.

Generic LDAPv3 Attributes

The following attributes are used to configure a LDAPv3 repository plug-in:

LDAP Server

Enter the name of the LDAP server to which OpenSSO will be connected in the format *host*.*domain*:*portnumber*. If more than one entry is entered, an attempt is made to connect to the first host in the list. The next entry in the list is tried only if the attempt to connect to the current host fails.

Optionally, a server identifier and site identifier can be appended to the value of the LDAP Server attribute for redundancy. In this case, the format is *host*.*domain*:*portnumber*|*serverID*|*siteID*. These identifiers are assigned to the server when they are configured globally.

- *serverID* specifies a particular server as the primary LDAP server and others as secondary and tertiary (as defined) fallback servers. (If no number is specified, the LDAP server is primary.) The identifier is displayed in the OpenSSO console.
  1. Click the Configuration tab, click the Servers and Sites tab.

2. Click the appropriate Server Name.
3. Under the Advanced tab, see the value of the `com.iplanet.am.lbcookie.value` property — for example, `01`.
4. Click the Configuration tab, click the Servers and Sites tab.

- *siteID* is not currently displayed in the OpenSSO console. It is a two digit number generated internally by OpenSSO — for example, `02`. To find this value, use an LDAP browser to find **`ou=accesspoint,ou=`***site_name*`,ou=com-sun-identity sites,ou=default,ou=GlobalConfig,ou=iPlanetAMPlatformService,ou=services,`***root-suffix*. Under this DN, see **`sunkeyvalue:primary-siteid=`***site-id* for the site identifier.

Caution – This configuration should not be changed for the OpenSSO embedded configuration data store as it may cause inconsistent behavior.

LDAP Bind DN

Specifies the DN name that OpenSSO Enterprise will use to authenticate to the LDAP server to which you are currently connected. The user with the DN name used to bind should have the correct add/modification/delete privileges that you configured in the "LDAPv3 Plugin Supported Types and Operations" on page 299 attribute.

LDAP Bind Password

Specifies the DN password that OpenSSO Enterprise will use to authenticate to the LDAP server to which you are currently connected

LDAP Bind Password (confirm)

Confirm the password.

LDAP Organization DN

The DN to which this data store repository will map. This will be the base DN of all operations performed in this data store.

LDAP SSL

When enabled, OpenSSO Enterprise will connect to the primary server using the HTTPS protocol.

LDAP Connection Pool Minimum Size

Specifies the initial number of connections in the connection pool. The use of connection pool avoids having to create a new connection each time.

LDAP Connection Pool Maximum Size

Specifies the maximum number of connections to allowed.

Maximum Results Returned from Search

Specifies the maximum number of entries returned from a search operation. If this limit is reached, the data store returns any entries that match the search request.

Search Timeout

Specifies the maximum number of seconds allocated for a search request. If this limit is reached, the data store returns any search entries that match the search request.

LDAP Follows Referral

If enabled, this option specifies that referrals to other LDAP servers are followed automatically.

LDAPv3 Repository Plugin Class Name

Specifies the location of the class file which implements the LDAPv3 repository.

Attribute Name Mapping

Enables common attributes known to the framework to be mapped to the native data store. For example, if the framework uses `inetUserStatus` to determine user status, it is possible that the native data store actually uses `userStatus`. The attribute definitions are case-sensitive.

LDAPv3 Plugin Supported Types and Operations

Specifies the operations that are permitted to or can be performed on this LDAP server. The default operations that are the only operations that are supported by this LDAPv3 repository plug-in. The following are operations supported by LDAPv3 Repository Plugin:

- agent: read, create, edit, delete
- group: read, create, edit, delete
- realm: read, create, edit, delete, service
- user: read, create, edit, delete, service
- role: read, create, edit, delete

You can remove permissions from the above list based on your LDAP server settings and the tasks, but you can not add more permissions.

If you have `user` as a supported type for the LDAPv3 repository, the read, create, edit, and delete service operations are possible for that user. In other words, if `user` is a supported type, then the read, edit, create, and delete operations allow you to read, edit, create, and delete user entries from the identity repository. The `user=service` operation lets OpenSSO Enterprise services access attributes in user entries. Additionally, the user is allowed to access the dynamic service attributes if the service is assigned to the realm or role to which the user belongs.

The user is also allowed to manage the user attributes for any assigned service. If the user has `service` as the operation (`user=service`), then it specifies that all service-related operations are supported. These operations are `assignService`, `unassignService`, `getAssignedServices`, `getServiceAttributes`, `removeServiceAttributes` and `modifyService`.

LDAPv3 Plug-in Search Scope

Defines the scope to be used to find LDAPv3 plug-in entries. The scope must be one of the following:

- SCOPE_BASE: searches only the base DN.
- SCOPE_ONE: searches only the entries under the base DN.
- SCOPE_SUB (default): searched the base DN and all entries within its subtree.

LDAP Users Search Attribute

This field defines the attribute type to conduct a search for a user. For example, if the user's DN is `uid=user1, ou=people, dc=example, dc=com`, then you would specify `uid` in this field.

LDAP Users Search Filter

Specifies the search filter to be used to find user entries.

LDAP User Object Class

Specifies the object classes for a user. When a user is created, this list of user object classes will be added to the user's attributes list.

LDAP User Attributes

Defines the list of attributes associated with a user. Any attempt to read/write user attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined before you define the object classes and attribute schema here.

Create user Attribute Mapping

Specifies which attributes are required when a user is created. This attribute uses the following syntax:

```
DestinationAttributeName=SourceAttributeName
```

If the source attribute name is missing, the default is the user ID (`uid`). For example:

cn
sn=givenName

Both `cn` and `sn` are required in order to create a user profile. `cn` gets the value of the attribute named `uid`, and `sn` gets the value of the attribute named `givenName`.

Attribute Name of User Status

Specifies the attribute name to indicate the user's status.

User Status Active Value

Specifies the attribute name for an active user status. The default is `active`.

User Status Inactive Value

Specifies the attribute name for an inactive user status. The default is `inactive`.

LDAP Groups Search Attribute

This field defines the attribute type for which to conduct a search on a group. The default is `cn`.

LDAP Group Search Filter

Specifies the search filter to be used to find group entries. The default is `(objectclass=groupOfUniqueNames)`.

LDAP Groups Container Naming Attribute

Specifies the naming attribute for a group container, if groups resides in a container. Otherwise, this attribute is left empty. For example, if a group DN of `cn=group1,ou=groups,dc=iplanet,dc=com`resides in `ou=groups`, then the group container naming attribute is `ou`.

LDAP Groups Container Value

Specifies the value for the group container. For example, a group DN of `cn=group1,ou=groups,dc=iplanet,dc=com` resides in a container name `ou=groups`, then the group container value would be `groups`.

LDAP Groups Object Classes

Specifies the object classes for groups. When a group is created, this list of group object classes will be added to the group's attributes list.

LDAP Groups Attributes

Defines the list of attributes associated with a group. Any attempt to read/write group attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined before you define the object classes and attribute schema here.

Attribute Name for Group Membership

Specifies the name of the attribute whose values are the names of all the groups to which DN belongs. The default is `memberOf`.

Attribute Name of Unique Member

Specifies the attribute name whose values is a DN belonging to this group. The default is `uniqueMember`.

Attribute Name of Group Member URL

Specifies the name of the attribute whose value is an LDAP URL which resolves to members belonging to this group. The default is `memberUrl`.

Default Group Member's User DN

The DN value specified in this attribute automatically adds users to the group when it is created.

LDAP People Container Naming Attribute

Specifies the naming attribute of the people container if a user resides in a people container. This field is left blank if the user does not reside in a people container.

LDAP People Container Value

Specifies the value of the people container. The default is `people`.

Caution – The entire tree under the `baseDN` will be searched if the value of this attribute is set to null (empty).

Identity Types That Can Be Authenticated

Specifies that this data store can authenticate user and/or agent identity types when the authentication module mode for the realm is set to Data Store.

Persistent Search Base DN

Defines the base DN to use for persistent search. Some LDAPv3 servers only support persistent search at the root suffix level.

Persistent Search Filter

Defines the filter that will return the specific changes to directory server entries. The data store will only receive the changes that match the defined filter.

Persistent Search Scope

Defines the scope to be used in a persistent search. The scope must be one of the following:

- SCOPE_BASE – searches only the base DN.
- SCOPE_ONE – searches only the entries under the base DN.
- SCOPE_SUB (default) – searched the base DN and all entries within its subtree.

Persistent Search Maximum Idle Time Before Restart

Defines the maximum idle time before restarting the persistence search. The value must be great than 1. Values less than or equal to 1 will restart the search irrespective of the idle time of the connection.

If OpenSSO Enterprise is deployed with a load balancer, some load balancers will time out if it has been idle for a specified amount of time. In this case, you should set the Persistent Search Maximum Idle Time Before Restart to a value less than the specified time for the load balancer.

Maximum Number of Retries After Error Code

Defines the maximum number of retries for the persistent search operation if it encounters the error codes specified in LDAPException Error Codes to Retry On.

The Delay Time Between Retries

Specifies the time to wait before each retry. This only applies to persistent search connection.

LDAPException Error Codes to Retry

Specifies the error codes to initiate a retry for the persistent search operation. This attribute is only applicable for the persistent search, and not for all LDAP operations.

Caching

If enabled, this allows OpenSSO Enterprise to cache data retrieved from the data store.

Maximum Age of Cached Items

Specifies the maximum time data is stored in the cache before it is removed. The values are defined in seconds.

Maximum Size of the Cache

Specifies the maximum size of the cache. The larger the value, the more data can be stored, but it will require more memory. The values are defined in bytes.

Sun Directory Server with OpenSSO Enterprise Schema Attributes

The following attributes are used to configure Directory Server with OpenSSO Enterprise schema:

LDAP Server

Enter the name of the LDAP server to which OpenSSO will be connected in the format *host*.*domain*:*portnumber*. If more than one entry is entered, an attempt is made to connect to the first host in the list. The next entry in the list is tried only if the attempt to connect to the current host fails.

Optionally, a server identifier and site identifier can be appended to the value of the LDAP Server attribute for redundancy. In this case, the format is *host*.*domain*:*portnumber*|*serverID*|*siteID*. These identifiers are assigned to the server when they are configured globally.

- *serverID* specifies a particular server as the primary LDAP server and others as secondary and tertiary (as defined) fallback servers. (If no number is specified, the LDAP server is primary.) The identifier is displayed in the OpenSSO console.
  1. Click the Configuration tab, click the Servers and Sites tab.
  2. Click the appropriate Server Name.
  3. Under the Advanced tab, see the value of the `com.iplanet.am.lbcookie.value` property — for example, `01`.
  4. Click the Configuration tab, click the Servers and Sites tab.
- *siteID* is not currently displayed in the OpenSSO console. It is a two digit number generated internally by OpenSSO — for example, `02`. To find this value, use an LDAP browser to find **`ou=accesspoint,ou=`***site_name*`,ou=com-sun-identity sites,ou=default,ou=GlobalConfig,ou=iPlanetAMPlatformService,ou=services,`***root-suffix*. Under this DN, see **`sunkeyvalue:primary-siteid=`***site-id* for the site identifier.

Caution – This configuration should not be changed for the embedded data store as it may cause inconsistent behavior.

LDAP Bind DN

Specifies the DN name that OpenSSO Enterprise will use to authenticate to the LDAP server to which you are currently connected. The user with the DN name used to bind should have the correct add/modification/delete privileges that you configured in the "LDAPv3 Plugin Supported Types and Operations" on page 299 attribute.

LDAP Bind Password

Specifies the DN password that OpenSSO Enterprise will use to authenticate to the LDAP server to which you are currently connected

LDAP Bind Password (confirm)

Confirm the password.

LDAP Organization DN

The DN to which this data store repository will map. This will be the base DN of all operations performed in this data store.

LDAP SSL

When enabled, OpenSSO Enterprise will connect to the primary server using the HTTPS protocol.

LDAP Connection Pool Minimum Size

Specifies the initial number of connections in the connection pool. The use of connection pool avoids having to create a new connection each time.

LDAP Connection Pool Maximum Size

Specifies the maximum number of connections to allowed.

Maximum Results Returned from Search

Specifies the maximum number of entries returned from a search operation. If this limit is reached, Directory Server returns any entries that match the search request.

Search Timeout

Specifies the maximum number of seconds allocated for a search request. If this limit is reached, Directory Server returns any search entries that match the search request.

LDAP Follows Referral

If enabled, this option specifies that referrals to other LDAP servers are followed automatically.

LDAPv3 Repository Plugin Class Name

Specifies the location of the class file which implements the LDAPv3 repository.

Attribute Name Mapping

Enables common attributes known to the framework to be mapped to the native data store. For example, if the framework uses `inetUserStatus` to determine user status, it is possible that the native data store actually uses `userStatus`. The attribute definitions are case-sensitive.

LDAPv3 Plugin Supported Types and Operations

Specifies the operations that are permitted to or can be performed on this LDAP server. The default operations that are the only operations that are supported by this LDAPv3 repository plug-in. The following are operations supported by LDAPv3 Repository Plugin:

- Filtered role: read, create, edit, delete
- Group: read, create, edit, delete
- Realm: read, create, edit, delete, service
- User: read, create, edit, delete, service
- Role: read, create, edit, delete

You can remove permissions from the above list (except role) based on your LDAP server settings and the tasks, but you can not add more permissions. If the configured LDAPv3 Repository plug-in is pointing to an instance of Sun Directory Server, then permissions for the type `role` can be added. Otherwise, this permission may not be added because other data stores may not support roles.

If you have `user` as a supported type for the LDAPv3 repository, the read, create, edit, and delete service operations are possible for that user. In other words, if `user` is a supported type, then the read, edit, create, and delete operations allow you to read, edit, create, and delete user entries from the identity repository. The `user=service` operation lets OpenSSO Enterprise services access attributes in user entries. Additionally, the user is allowed to access the dynamic service attributes if the service is assigned to the realm or role to which the user belongs.

The user is also allowed to manage the user attributes for any assigned service. If the user has `service` as the operation (`user=service`), then it specifies that all service-related operations are supported. These operations are `assignService, unassignService, getAssignedServices, getServiceAttributes, removeServiceAttributes` and `modifyService.`

LDAPv3 Plug-in Search Scope

Defines the scope to be used to find LDAPv3 plug-in entries. The scope must be one of the following:

- SCOPE_BASE – searches only the base DN.
- SCOPE_ONE – searches only the entries under the base DN.
- SCOPE_SUB (default) – searched the base DN and all entries within its subtree.

LDAP Users Search Attribute

This field defines the attribute type to conduct a search for a user. For example, if the user's DN is `uid=user1, ou=people, dc=example, dc=com`, then you would specify `uid` in this field.

LDAP Users Search Filter

Specifies the search filter to be used to find user entries.

LDAP User Object Class

Specifies the object classes for a user. When a user is created, this list of user object classes will be added to the user's attributes list.

LDAP User Attributes

Defines the list of attributes associated with a user. Any attempt to read/write user attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined in Directory Server before you define the object classes and attribute schema here.

Create User Attribute Mappings

Specifies which attributes are required when a user is created. This attribute uses the following syntax:

```
DestinationAttributeName=SourceAttributeName
```

If the source attribute name is missing, the default is the user ID (`uid`). For example:

cn
sn=givenName

Both cn and sn are required in order to create a user profile. cn gets the value of the attribute named uid, and sn gets the value of the attribute named givenName.

Attribute Name of User Status

Specifies the attribute name to indicate the user's status.

LDAP Groups Search Attribute

This field defines the attribute type for which to conduct a search on a group. The default is cn.

LDAP Group Search Filter

Specifies the search filter to be used to find group entries. The default is (objectclass=groupOfUniqueNames).

LDAP Groups Container Naming Attribute

Specifies the naming attribute for a group container, if groups resides in a container. Otherwise, this attribute is left empty. For example, if a group DN of cn=group1,ou=groups,dc=iplanet,dc=comresides in ou=groups, then the group container naming attribute is ou.

LDAP Groups Container Value

Specifies the value for the group container. For example, a group DN of cn=group1,ou=groups,dc=iplanet,dc=com resides in a container name ou=groups, then the group container value would be groups.

LDAP Groups Object Classes

Specifies the object classes for groups. When a group is created, this list of group object classes will be added to the group's attributes list.

LDAP Groups Attributes

Defines the list of attributes associated with a group. Any attempt to read/write group attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined in Directory Server before you define the object classes and attribute schema here.

Attribute Name for Group Memberships

Specifies the name of the attribute whose values are the names of all the groups to which DN belongs. The default is `memberOf`.

Attribute Name of Unique Member

Specifies the attribute name whose values is a DN belonging to this group. The default is `uniqueMember`.

Attribute Name of Group Member URL

Specifies the name of the attribute whose value is an LDAP URL which resolves to members belonging to this group. The default is `memberUrl`.

LDAP Roles Search Attribute

This field defines the attribute type for which to conduct a search on a role. The default is `cn`.

LDAP Role Search Filter

Defines the filter used to search for an role. The LDAP Role Search attribute is prepended to this field to form the actual role search filter.

For example, if the LDAP Role Search Attribute is `CN` and LDAP Role Search Filter is `(objectClass=sunIdentityServerDevice)` , then the actual user search filter will be: `(&(cn=*)(objectClass=sunIdentityServ erDevice))`

LDAP Role Object Class

Defines the object classes for roles. When a role is created, the list of user object classes will be added to the role's attributes list

LDAP Roles Attributes

Defines the list of attributes associated with a role. Any attempt to read/write agent attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined in Directory Server before you define the object classes and attribute schema here.

LDAP Filter Roles Search Attribute

This field defines the attribute type for which to conduct a search on a filter role. The default is `cn`.

LDAP Filter Role Search Filter

Defines the filter used to search for an filtered role. The LDAP Filter Role Search attribute is prepended to this field to form the actual filtered role search filter.

For example, if the LDAP Filter Role Search Attribute is `CN` and LDAP Filter Role Search Filter is `(objectClass=sunIdentityServerDevice)` , then the actual user search filter will be: `(&(cn=*)(objectClass=sunIdentityServ erDevice))`

LDAP Filter Role Object Class

Defines the object classes for filtered roles. When a filtered role is created, the list of user object classes will be added to the filtered role's attributes list

LDAP Filter Roles Attributes

Defines the list of attributes associated with a filtered role. Any attempt to read/write agent attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined in Directory Server before you define the object classes and attribute schema here.

LDAP People Container Naming Attribute

Specifies the naming attribute of the people container if a user resides in a people container. This field is left blank if the user does not reside in a people container.

LDAP People Container Value

Specifies the value of the people container. The default is `people`.

Caution – The entire tree under the `baseDN` will be searched if the value of this attribute is set to null (empty).

Identity Types that can be Authenticated

Specifies that this data store can authenticate user and/or agent identity types when the authentication module mode for the realm is set to Data Store.

Persistent Search Base DN

Defines the base DN to use for persistent search. Some LDAPv3 servers only support persistent search at the root suffix level.

Persistent Search Filter

Defines the filter that will return the specific changes to directory server entries. The data store will only receive the changes that match the defined filter.

Persistent Search Scope

Defines the scope to be used in a persistent search. The scope must be one of the following:

- SCOPE_BASE – searches only the base DN.
- SCOPE_ONE – searches only the entries under the base DN.
- SCOPE_SUB (default) – searched the base DN and all entries within its subtree.

Persistent Search Maximum Idle Time Before Restart

Defines the maximum idle time before restarting the persistence search. The value must be great than 1. Values less than or equal to 1 will restart the search irrespective of the idle time of the connection.

If OpenSSO Enterprise is deployed with a load balancer, some load balancers will time out if it has been idle for a specified amount of time. In this case, you should set the Persistent Search Maximum Idle Time Before Restart to a value less than the specified time for the load balancer.

Maximum Number of Retries After Error Code

Defines the maximum number of retries for the persistent search operation if it encounters the error codes specified in LDAPException Error Codes to Retry On.

The Delay Time Between Retries

Specifies the time to wait before each retry. This only applies to persistent search connection.

LDAPException Error Codes to Retry

Specifies the error codes to initiate a retry for the persistent search operation. This attribute is only applicable for the persistent search, and not for all LDAP operations.

Caching

If enabled, this allows OpenSSO Enterprise to cache data retrieved from the data store.

Maximum Age of Cached Items

Specifies the maximum time data is stored in the cache before it is removed. The values are defined in seconds.

Maximum Size of the Cache

Specifies the maximum size of the cache. The larger the value, the more data can be stored, but it will require more memory. The values are defined in bytes.

PART III

Error Codes and Log File Reference

◆ ◆ ◆ CHAPTER 9

OpenSSO Enterprise Component Error Codes

This appendix provides a list of the error messages generated by OpenSSO Enterprise. While this list is not exhaustive, the information presented in this chapter will serve as a good starting point for common problems. The tables listed in this appendix provide the error code itself, a description and/or probable cause of the error, and describes the actions that can be taken to fix the encountered problem.

This appendix lists error codes for the following functional areas:

If you require further assistance in diagnosing errors, please contact Sun Technical Support:

http://www.sun.com/service/sunone/software/index.html

OpenSSO Enterprise Console Errors

The following table describes the error codes generated and displayed by the OpenSSO Enterprise Console.

TABLE 9–1 OpenSSO Enterprise Console Errors

Error Message	Description/Probable Cause	Action
Unable to get attribute from data store.	The object may have been removed by another user prior to being removed by the current user.	Redisplay the objects that you are trying to delete and try the operation again.

TABLE 9–1 OpenSSO Enterprise Console Errors *(Continued)*

Error Message	Description/Probable Cause	Action
Invalid URL	This occurs if the URL for an OpenSSO Enterprise console window is entered incorrectly.	
There are no entities.	The parameters entered in the search window, or in the Filter fields, did not match any objects in the directory.	Run the search again with a different set of parameters
There are no attributes to display.	The selected object does not contain any editable attributes defined in its schema.	
There is no information to display for this service.	The services viewed from the Service Configuration module do not have global or organization based attributes	
Size limit Exceeded. Refine your search to locate more entries.	The parameters specified in the search have returned more entries than are allowed to be returned	Modify the Maximum Results Returned from a Search attribute in the Administration service to a larger value. You can also modify the search parameters to be more restrictive.
Time limit Exceeded. Refine your search to locate more entries.	The search for the specified parameters has taken longer than the allowed search time.	Modify the Timeout for Search attribute in the Administration service to a larger value. You can also modify the search parameters, so they are less restrictive, to return more values.
Invalid user's start location. Please contact your administrator.	The start location DN in the users entry is no longer valid	Edit the properties of the User service and change the value for Administrator DN to a valid DN value.
Could not create identity object. User does not have sufficient access.	An operation was executed by a user with insufficient permissions. The permissions a user has defined determines what operations they can perform.	

ssoadm Command Line Interface Error Codes

The following table describes the error codes generated by the `ssoadm` command line utility.

TABLE 9–2 Authentication Error Codes

Error Message	Description/Probable Cause	Action
Missing Resource Bundle		Make sure the `ssoadmTools.zip` is setup correctly. For information, see "Installing the OpenSSO Enterprise Utilities and Scripts in the ssoAdminTools.zip File" in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*
Missing CLI Definition Files		Make sure the `ssoadmTools.zip` is setup correctly. For information, see "Installing the OpenSSO Enterprise Utilities and Scripts in the ssoAdminTools.zip File" in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*
Missing Command Name		Make sure the `ssoadmTools.zip` is setup correctly. For information, see "Installing the OpenSSO Enterprise Utilities and Scripts in the ssoAdminTools.zip File" in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*
Missing Definition Classes		Make sure the `ssoadmTools.zip` is setup correctly. For information, see "Installing the OpenSSO Enterprise Utilities and Scripts in the ssoAdminTools.zip File" in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*

TABLE 9–2 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
Incorrect Definition Classes		Make sure the `ssoadmTools.zip` is setup correctly. For information, see "Installing the OpenSSO Enterprise Utilities and Scripts in the ssoAdminTools.zip File" in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*
Unable to instantiate Definition Classes		Make sure the `ssoadmTools.zip` is setup correctly. For information, see "Installing the OpenSSO Enterprise Utilities and Scripts in the ssoAdminTools.zip File" in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*
Unable to access Definition Classes		Make sure the `ssoadmTools.zip` is setup correctly. For information, see "Installing the OpenSSO Enterprise Utilities and Scripts in the ssoAdminTools.zip File" in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*
Reserved option is used		If you are extending the ssoadm CLI, check that the new sub command does not use reserved option names.
Incorrect Usage format		If you are extending the ssoadm CLI, check that the new sub command does not use reserved option names.
Incorrect Option	You have entered invalid options.	
Incorrect Sub Command	You have entered invalid sub command.	

TABLE 9–2 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
Sub Command implementation is not found		If you are extending the ssoadm CLI, check that the implementation class is in the class path.
Sub Command implementation cannot be instantiated		If you are extending the ssoadm CLI, check that the implementation class is in the class path.
Sub Command implementation is not accessed		If you are extending the ssoadm CLI, check that the implementation class is accessible.
Output Writer Class cannot be instantiated		If you are extending the ssoadm CLI, check that the output writer class is in the class path
Debug Class cannot be instantiated		If you are extending the ssoadm CLI, check that the debug class is in the class path
Cannot read the input file		Check the file name that is provided to ssoadm
Cannot authenticate (LDAP based).		Check user name and password are valid
Cannot authenticate (session		Check user name and password are valid
Duplicated options are defined		If you are extending the ssoadm CLI, check that the new sub command does not have duplicate option names.
Cannot logout	The server may be down.	Restart the server and logout again.
Incorrect Option values	You have entered invalid option values.	
Input/Output Exception	This usually happens if the input file is not readable	Check the structure of the input file to ensure its validity.
Cannot write to log file	Log directory permissions may be set incorrectly.	Check if the log directory is writable.

TABLE 9–2 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
Incorrect data format	The data in input file needs to have a key and value. e.g. `example.key=value1`	
Session expired	The session has expired. Usually happens if ssoadm runs for a long period of time.	
Request cannot be serviced		Read the output printed by ssoadm. It will provide information on why ssoadm fails. For a list of messages, see Chapter 10, "OpenSSO Enterprise Log File Reference"

Authentication Error Codes

The following table describes the error codes generated by the Authentication service. These errors are displayed to the user/administrator in the Authentication module.

TABLE 9–3 Authentication Error Codes

Error Message	Description/Probable Cause	Action
You are already logged in	The user has already logged in and has a valid session, but there is no Success URL redirect defined.	Either logout, or set up some login success redirect URL(s) through the OpenSSO Enterprise Console. Use the "goto' query parameter with the value as Admin Console URL.
Logout Failure	A user is unable to logout of OpenSSO Enterprise.	Restart the server.
Authentication exception	An authentication Exception is thrown due to an incorrect handler	Check the Login URL for any invalid or special characters.
Can non redirect to default page.	OpenSSO Enterprise cannot redirect to Success or Failure redirect URL.	Check the web container's error log to see if there are any errors.
gotoLoginAfterFail link	This link is generated when most errors occur. The link will send the user to the original Login URL page.	

TABLE 9–3 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
Invalid password	The password entered is invalid.	Passwords must contain at least 8 characters. Check that the password contains the appropriate amount of characters and ensure that it has not expired.
Authentication failed	. This is the generic error message displayed in the default login failed template. The most common cause is invalid/incorrect credentials.	Enter valid and correct user name/password (the credentials required by the invoked authentication module.)
No user profile was found matching the entered user name in the given organization.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Enter your login information again. If this is your first login attempt, select New User in the login screen.
The password entered does not contain enough characters.	This error is displayed while logging in to the Membership/Self-registration authentication module.	The login password must contain at least 8 characters by default (this number is configurable through the Membership Authentication module).
A user already exists with this name in the given organization.	This error is displayed while logging in to the Membership/Self-registration authentication module.	User IDs must be unique within the organization.
The User Name and Password fields cannot have the same value.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure that the username and password are different.
No user name was entered	.This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure to enter the user name.
No password was entered.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure to enter the password.
Missing the confirmation password field.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure to enter the password in the Confirm Password field.

TABLE 9–3 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
The password and the confirm password do not match.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure that the password and confirmation password match.
An error occurred while storing the user profile.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure that the attributes and elements are valid and correct for Self Registration in the `Membership.xml` file.
This organization is not active	The organization is not active.	Activate the organization through the OpenSSO Enterprise console by changing the organization status from `inactive` to `active`.
Internal Authentication Error.	This is a generic Authentication error which may be caused by different and multiple environmental and/or configuration issues.	
User is not active	The user no longer has an active status.	Activate the user through the Admin Console by changing the user status from `inactive` to `active`. if the user is locked out by Memory Locking, restart the server.
User does not belong to the specified role.	This error is displayed during role-based authentication.	Make sure that the login user belongs to the role specified for the role-based authentication.
User session has timed out.	The user session has timed out.	Log in again.
Specified authentication module is denied.	The specified authentication module is denied.	Make sure that the required authentication module is registered under the required organization, that the template is created and saved for the module, and that the module is selected in the Organization Authentication Modules list in the Core Authentication module.

TABLE 9–3 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
No configuration found	The configuration for the authentication module was not found.	Check the Authentication Configuration service for the required authentication method.
Persistent Cookie Username does not exist	Persistent Cookie Username does not exist in the Persistent Cookie Domain.	
No organization found.	The organization was not found.	Make sure that the requested organization is valid and correct.
User has no profile in the specified organization.	User has no profile in the specified organization.	Make sure that the user exists and is valid in the specified organization in the local Directory Server.
One of the required fields was not completed.	One of the required fields was not completed.	Make sure that all required fields are entered.
Maximum Session Limit was reached	The maximum sessions limit was reached.	Logout and login again.

Policy Error Codes

The following table describes the error codes generated by the Policy framework and displayed in the OpenSSO Enterprise Console.

TABLE 9–4 Policy Error Codes

Error Message	Description/Probable Cause	Action
Illegal character "/" in the policy name	There was an illegal character "/" in the policy name.	Make sure that the policy name does not contain the "/' character.
A rule with the same name already exists	A rule with the same name already exists within the realm.	Use a different name for policy creation.
Another rule with the given name already exists	Another rule with the given name already exists	Use a different rule name for policy creation.
A rule with the same rule value already exists	A rule with the same rule value already exists within the policy.	Use a different rule value.

TABLE 9–4 Policy Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
No referral exists to the realm.	No referral exists to the realm.	In order to create policies under a sub realm, you must create a referral policy at its parent realm to indicate what resources can be referred to this sub realm
LDAP search size limit exceeded.	An error occurred because the search found more than the maximum number of results.	Change the search pattern or policy configuration of the organization for the search control parameters.T he Search Size Limit is located in the Policy Configuration service.
LDAP search time limit exceeded.	An error occurred because the search found more than the maximum number of results.	Change the search pattern or policy configuration of the organization for the search control parameters. The Search Time Limit is located in the Policy Configuration service.
Invalid LDAP Bind password.	Invalid LDAP Bind password.	The password for LDAP Bind user defined in Policy Configuration is incorrect. This leads to the inability to get an authenticated LDAP connection to perform policy operations.
Application SSO token is invalid	The server could not validate the Application SSO token. Most likely the SSO token is expired.	Enter the authentication credentials again.
User SSO token is invalid.	The server could not validate the User SSO token. Most likely the SSO token is expired.	User must reauthenticate..
Property value not an integer	The property value not an integer.	The value for this plugin's property should be an integer.
Property Value not defined	Property value should be defined.	Provide a value for the given property.
Start IP is larger than End IP	Start IP is larger than End IP for the policy's condition.	An attempt was made to set end IP Address to be larger than start IP Address in IP Address condition. The Start IP cannot be larger than the End IP.

TABLE 9–4 Policy Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
Start Date is larger than End Date	Start date is larger than end date for the policy's condition.	An attempt was made to set end Date to be larger than start Date in the policy's Time Condition. The Start Date cannot be larger than the End Date.
Policy not found in realm.	An error occurred trying to locate a non-existing policy in a realm	Make sure that the policy exists under the specified realm.
User does not have sufficient access.	The user does not have sufficient right to perform policy operations.	Perform policy operations with the user who has appropriate access rights.
Invalid LDAP Server host.	The LDAP Server Host attribute value is invalid.	Change the invalid LDAP Server host that was entered in the Policy Configuration service.

amadmin Error Codes

The following table describes the error codes generated by the `amadmin` command line tool to OpenSSO Enterprise's debug file.

TABLE 9–5 amadmin error codes

Code	Description/Probable Cause	Action
1	Too few arguments.	Make sure that the mandatory arguments (`--runasdn`, `--password`, `--passwordfile`, `--schema`, `--data`, and `--addattributes`) and their values are supplied in the command line.
2	The input XML file was not found.	Check the syntax and make sure that the input XML is valid.
3	The user DN for the `--runasdn` value is missing.	Provide the user DN as the value for `--runasdn`.
4	The service name for the `--deleteservice` value is missing.	Provide the service name as the value for `--deleteservice`.
5	The password for the `--password` value is missing.	Provide the password as the value for `--password`.
6	The locale name was not provided. The locale will default to en_US.	See the Online Help for a list of locales.
7	Missing XML input file.	Provide at least one input XML filename to process.

TABLE 9–5 amadmin error codes *(Continued)*

Code	Description/Probable Cause	Action
8	One or more arguments are incorrect.	Check that all arguments are valid. For a set of valid arguments, type `amadmin --help`.
9	Operation failed.	When `amadmin` fails, it produces more precise error codes to indicate the specific error. Refer to those error codes to evaluate the problem.
10	Cannot process requests.	When `amadmin` fails, it produces more precise error codes to indicate the specific error. Refer to those error codes to evaluate the problem.
12	Policy cannot be created.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
13	Policy cannot be deleted.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
14	Service cannot be deleted.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
15	Cannot authenticate user.	Make sure the user DN and password are correct.
16	Cannot parse the input XML file.	Make sure that the XML is formatted correctly and adheres to the `amAdmin.dtd`.
17	Cannot parse due to an application error or a parser initialization error.	Make sure that the XML is formatted correctly and adheres to the `amAdmin.dtd`.
18	Cannot parse because a parser with specified options cannot be built.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
19	Cannot read the input XML file.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
20	Cannot parse because the XML file is not a valid file.	Check the syntax and make sure that the input XML is valid.
21	Cannot parse because the XML file is not a valid file.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
22	XML file validation warnings for the file.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.

TABLE 9–5 amadmin error codes *(Continued)*

Code	Description/Probable Cause	Action
23	Cannot process the XML file.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
24	Neither `--data` or `--schema` options are in the command.	Check that all arguments are valid. For a set of valid arguments, type `amadmin --help`.
25	The XML file does not follow the correct DTD.	Check the XML file for the `DOCTYPE` element.
26	LDAP Authentication failed due to invalid DN, password, hostname, or portnumber.	Make sure the user DN and password are correct.
28	Service Manager exception (SSO exception).	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
29	Service Manager exception.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
30	Schema file inputstream exception.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
31	Policy Manager exception (SSO exception).	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
32	Policy Manager exception.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
33	More than one debug option is specified.	Only one debug option should be specified.
34	Login failed.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
36	Invalid attribute value.	Check the level set for the LDAP search. It should be either `SCOPE_SUB` or `SCOPE_ONE`.
37	Error in getting object type.	Make sure that the DN in the XML file is value and contains the correct object type.
38	Invalid organization DN.	Make sure that the DN in the XML file is valid and is an organization object.
39	Invalid role DN.	Make sure that the DN in the XML file is valid and is a role object.

TABLE 9–5 amadmin error codes *(Continued)*

Code	Description/Probable Cause	Action
40	Invalid static group DN.	Make sure that the DN in the XML file is valid and is a static group object.
41	Invalid people container DN.	Make sure the DN in the XML file is valid and is a people container object.
42	Invalid organizational unit DN.	Make sure that the DN in the XML file is valid and is a container object.
43	Invalid service host name.	Make sure that the hostname for retrieving valid sessions is correct.
44	Subschema error.	Subcschema is only supported for global and organization attributes.
45	Cannot locate service schema for service.	Make sure that the sub schema in the XML file is valid.
46	The role template can be true only if the schema type is dynamic.	Make sure that the role template in the XML file is valid.
47	Cannot add users to a filtered role.	Made sure that the role DN in the XML file is not a filtered role.
48	Template does not exist.	Make sure that the service template in the XML file is valid.
49	Cannot add users to a dynamic group.	Made sure that the group DN in the XML file is not a dynamic group.
50	Policies can not be created in an organization that is a child organization of a container.	Make sure that the organization in which the policy is to be created is not a child of a container.
51	The group container was not found.	Create a group container for the parent organization or container.
52	Cannot remove a user from a filtered role.	Make sure that the role DN in the XML file is not filtered role.
53	Cannot remove users from a dynamic group.	Make sure that the group DN in the XML file is not a dynamic group.
54	The subschema string does not exist.	Make sure that the subschema string exists in the XML file.
59	You are trying to add user to an organization or container. And default people container does not exists in an organization or container.	Make sure the default people container exists.

TABLE 9–5 amadmin error codes *(Continued)*

Code	Description/Probable Cause	Action
60	Default URL prefix is not found following --defaultURLPrefix argument	provide the default URL prefix accordingly.
61	Meta Alias is not found following --metaalias argument	provide the Meta Alias accordingly.
62	Entity Name is not specified.	provide the entity name.
63	File name for importing meta data is missing.	provide the file name that contains meta data.
64	File name for storing exported meta data is missing.	provide the file name for storing meta data.
65	Unable to get a handler to Meta attribute. Specified user name and password may be incorrect.	ensure that user name and password are correct.
66	Missing resource bundle name when adding, viewing or deleting resource bundle that is store in directory server.	provide the resource bundle name
67	Missing file name of file that contains the resource strings when adding resource bundle to directory server.	Please provide a valid file name.
68	Failed to load liberty meta to Directory Server.	Please check the meta data again before loading it again

◆ ◆ ◆ CHAPTER 10

OpenSSO Enterprise Log File Reference

This section lists the possible log files for each area of OpenSSO Enterprise functionality. The tables in this appendix document the following log file items:

- Id — The log identification number.
- Log Level — The Log Level attribute for the message.
- Description — A description of the logging message.
- Data — The data type to which the message pertains.
- Triggers — Reason for the log file message.
- Actions — Actions for you to take to gain more information.

Definitions and locations and of the log files are described in "Log File Formats and Log File Types" in *Sun OpenSSO Enterprise 8.0 Technical Overview*.

Log file reference is provided for thee following areas:

amadmin Command Line Utility

Note – The amadmin command line utility has been replaced in this release by the `ssoadm` command line utility. This section is provided for purposes of backward compatibility.

TABLE 10–1 Log Reference Document for Amadmin_CLI

Id	Log Level	Description	Data	Triggers	Actions
1	INFO	Unsuccessful login for user.	user id	Unsuccessful login for user.	
2	INFO	ADMINEXCEPTION Received	Element name error message	Received ADMINEXCEPTION while processing Admin request(s).	Look in amAdmin debug file for more information.
3	INFO	Session destroyed	name of user	Session destroyed.	
11	INFO	Service Schema Loaded	schema name	Successfully loaded service schema.	
12	INFO	Service deleted	service name	Successfully deleted service.	
13	INFO	Attributes Added	attribute name	Attributes successfully added.	
21	INFO	There are no policies for this service	service name	Delete Policy Rule Flag specified, but service has no policies.	
22	INFO	Policy Schema for Service not found	service name	Delete Policy Rule Flag specified, but could not find the policy schema for the service	
23	INFO	Deleting Policies For Service	service name	Deleting Service with Delete Policy Rule Flag specified.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
24	INFO	Done Deleting Policies For Service	service name	Deleting Service with Delete Policy Rule Flag specified.	
25	INFO	Created Policy in Organization	policy name organization DN	Created Policy in Organization DN.	
26	INFO	Deleted Policy from Organization	policy name organization DN	Deleted Policy from Organization DN.	
31	INFO	Add Resource Bundle of Locale to Directory Server	resource bundle name resource locale	Resource Bundle of Locale successfully stored in Directory Server.	
32	INFO	Add Default Resource Bundle to Directory Server	resource bundle name	Default Resource Bundle successfully stored in Directory Server.	
33	INFO	Deleted Resource Bundle of Locale from Directory Server	resource bundle name resource locale	Successfully deleted Resource Bundle of Locale from Directory Server.	
34	INFO	Deleted Default Resource Bundle of Locale from Directory Server	resource bundle name	Successfully deleted default Resource Bundle from Directory Server.	
41	INFO	Modified Service Schema of service	name of service	Successfully modified Service Schema of service.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
42	INFO	Deleted Service Sub Schema of service	name of sub schema name of service	Successfully deleted service sub schema of service.	
43	INFO	Added Service Sub Schema to service.	name of service	Successfully added service sub schema to service.	
44	INFO	Added Sub Configuration to service.	name of sub configuration name of service	Successfully added sub configuration to service.	
45	INFO	Modified Sub Configuration of service	name of sub configuration name of service	Successfully modified sub configuration of service.	
46	INFO	Deleted Sub Configuration of service	name of sub configuration name of service	Successfully deleted sub configuration of service.	
47	INFO	Deleted all Service Configurations of service.	name of service	Successfully deleted all service configurations of service.	
91	INFO	Modify Service SubConfiguration in Organization	subconfiguration name service name organization DN	Successfully Modified Service SubConfiguration in Organization.	
92	INFO	Added Service SubConfiguration in Organization	subconfiguration name service name organization DN	Successfully Added Service SubConfiguration in Organization.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
93	INFO	Deleted Service SubConfiguration in Organization	subconfiguration name service name organization DN	Successfully Deleted Service SubConfiguration in Organization.	
94	INFO	Created remote provider in organization	provider name organization DN	Successfully created remote provider in organization.	
95	INFO	Modified remote provider in organization	provider name organization DN	Successfully modified remote provider in organization.	
96	INFO	Modified hosted provider in organization	provider name organization DN	Successfully modified hosted provider in organization.	
97	INFO	Created hosted provider in organization	provider name organization DN	Successfully created hosted provider in organization.	Look under identity repository log for more information.
98	INFO	Deleted Remote Provider in organization	provider name organization DN	Successfully Deleted Remote Provider in organization.	
99	INFO	Created circle of trust in organization	name of circle of trust organization DN	Successfully Created circle of trust in organization.	
100	INFO	Deleted circle of trust in organization.	name of circle of trust organization DN	Successfully Deleted circle of trust in 0rganization.	
101	INFO	Modified circle of trust in organization.	name of circle of trust organization DN	Successfully Modified circle of trust in 0rganization.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
102	INFO	Attempt to modify service template	DN of service template	Attempted to modify service template.	
103	INFO	Modified service template	DN of service template	Successfully modified service template.	
104	INFO	Attempt to remove service template	DN of service template	Attempted to remove service template.	
105	INFO	Removed service template	DN of service template	Successfully removed service template.	
106	INFO	Attempt to add service template	DN of service template	Attempted to add service template.	
107	INFO	Added service template	DN of service template	Successfully added service template.	
108	INFO	Attempt to add nested groups to group	name of group to add DN of containing group	Attempted to add nested groups to group.	
109	INFO	Added nested groups to group	name of group to add DN of containing group	Successfully added nested groups to group.	
110	INFO	Attempt to add user to group or role	name of user target group or role	Attempted to add user to group or role.	
111	INFO	Added user to group or role	name of user target group or role	Successfully added user to group or role.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
112	INFO	Attempt to create entity.	localized name of entity DN of entity container where entity is to be created	Attempted to Create entity.	
113	INFO	Created entity.	localized name of entity DN of entity	Created entity.	
114	INFO	Attempt to create role	role DN container where role is to be created	Attempted to create role.	
115	INFO	Created role	name of role	Created role.	
116	INFO	Attempt to create group container	name of group container container where group container is to be created.	Attempted to create group container.	
117	INFO	Create group container	name of group container	Created group container.	
118	INFO	Attempt to create group.	name of group type of group container where group is to be created.	Attempted to create group.	
119	INFO	Create group.	name of group	Created group.	
120	INFO	Attempt to create people container.	DN of people container container where people container is to be created.	Attempted to create people container.	
121	INFO	Create people container.	DN of people container	Created people container.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
122	INFO	Attempt to create service template in organization or role	name of service template name of organization or role	Attempted to create service template in organization or role.	
123	INFO	Create service template in organization or role	name of service template name of organization or role	Created service template in organization or role.	
124	INFO	Attempt to create container	name of container container where container is to be created.	Attempted to create container.	
125	INFO	Create container	name of container	Created container.	
126	INFO	Attempt to create user.	name of user organization, organizational unit or people container where user is to be created in.	Attempted to create user.	
127	INFO	Create user.	name of user	Created user.	
128	INFO	Attempt to delete entity.	DN of entity	Attempted to delete entity.	
129	INFO	Delete entity.	localized name of entity DN of entity	Deleted entity.	
130	INFO	Attempt to delete people container	DN of people container	Attempted to delete people container.	
131	INFO	Delete people container	DN of people container	Deleted people container.	
132	INFO	Attempt to delete role	name of role	Attempted to delete role.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
133	INFO	Delete role	name of role	Deleted role.	
134	INFO	Attempt to delete service template in organization	name of service template name of organization	Attempted to delete service template in organization.	
135	INFO	Delete service template in organization	name of service template name of organization	Deleted service template in organization.	
136	INFO	Attempt to delete container.	name of container	Attempted to delete container.	
137	INFO	Delete container.	name of container	Deleted container.	
138	INFO	Attempt to modify entity	localized name of entity DN of entity	Attempted to modify entity.	
139	INFO	Modify entity	localized name of entity DN of entity	Modified entity.	
140	INFO	Attempt to modify people container.	DN of people container	Attempted to modify people container.	
141	INFO	Modify people container.	DN of people container	Modified people container.	
142	INFO	Attempt to modify container.	name of container	Attempted to modify container.	
143	INFO	Modify container.	name of container	Modified container.	
144	INFO	Attempt to register service under organization.	name of service name of organization	Attempted to register service under organization	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
145	INFO	Register service under organization.	name of service name of organization	Registered service under organization	
146	INFO	Attempt to unregister service under organization.	name of service name of organization	Attempted to unregister service under organization	
147	INFO	Unregister service under organization.	name of service name of organization	Unregistered service under organization	
148	INFO	Attempt to modify group.	name of group	Attempted to modify group	
149	INFO	Modify group.	name of group	Modified group	
150	INFO	Attempt to remove nested group from group.	name of nested group name of group	Attempted to remove nested group from group.	
151	INFO	Remove nested group from group.	name of nested group name of group	Removed nested group from group.	
152	INFO	Attempt to delete group	name of group	Attempted to delete group.	
153	INFO	Delete group	name of group	Deleted group.	
154	INFO	Attempt to remove a user from a Role	name of user name of role	Attempted to remove a user from a Role.	
155	INFO	Remove a user from a Role	name of user name of role	Removed a user from a Role.	
156	INFO	Attempt to remove a user from a Group	name of user name of group	Attempted to remove a user from a Group.	
157	INFO	Remove a user from a Group	name of user name of group	Removed a user from a Group.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
201	INFO	Attempt to add an Identity to an Identity in a Realm	name of identity to add type of identity to add name of identity to add to type of identity to add to name of realm	Attempted to add an Identity to an Identity in a Realm.	
202	INFO	Add an Identity to an Identity in a Realm	name of identity to add type of identity to add name of identity to add to type of identity to add to name of realm	Added an Identity to an Identity in a Realm.	
203	INFO	Attempt to assign service to an identity in a realm.	name of service name of identity type of identity name of realm	Attempted to assign service to an identity in a realm.	
204	INFO	Assign service to an identity in a realm.	name of service name of identity type of identity name of realm	Assigned service to an identity in a realm.	
205	INFO	Attempt to create identities of a type in a realm.	type of identity name of realm	Attempted to create identities of a type in a realm.	
206	INFO	Create identities of a type in a realm.	type of identity name of realm	Created identities of a type in a realm.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
207	INFO	Attempt to create identity of a type in a realm.	name of identity type of identity name of realm	Attempted to create identity of a type in a realm.	
208	INFO	Create identity of a type in a realm.	name of identity type of identity name of realm	Created identity of a type in a realm.	
209	INFO	Attempt to delete identity of a type in a realm	name of identity type of identity name of realm	Attempted to delete identity of a type in a realm.	
210	INFO	Delete identity of a type in a realm	name of identity type of identity name of realm	Deleted identity of a type in a realm.	
211	INFO	Attempt to modify a service for an Identity in a Realm	name of service type of identity name of identity name of realm	Attempted to modify a service for an Identity in a Realm.	
212	INFO	Modify a service for an Identity in a Realm	name of service type of identity name of identity name of realm	Modified a service for an Identity in a Realm.	
213	INFO	Attempt to remove an Identity from an Identity in a Realm	name of identity to remove type of identity to remove name of identity to remove from type of identity to remove from name of realm	Attempted to remove an Identity from an Identity in a Realm.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
214	INFO	Remove an Identity from an Identity in a Realm	name of identity to remove type of identity to remove name of identity to remove from type of identity to remove from name of realm	Removed an Identity from an Identity in a Realm.	
215	INFO	Attempt to set Service Attributes for an Identity in a Realm	name of service type of identity name of identity name of realm	Attempted to set Service Attributes for an Identity in a Realm.	
216	INFO	Set Service Attributes for an Identity in a Realm	name of service type of identity name of identity name of realm	Set Service Attributes for an Identity in a Realm.	
217	INFO	Attempt to unassign a service from an Identity in a Realm	name of service type of identity name of identity name of realm	Attempted to unassign a service from an Identity in a Realm.	
218	INFO	Unassign a service from an Identity in a Realm	name of service type of identity name of identity name of realm	Unassigned a service from an Identity in a Realm.	
219	INFO	Attempt to create organization	name of organization container where sub organization is to be created	Attempted to create an organization.	
220	INFO	Create organization	name of organization	Created an organization.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
221	INFO	Attempt to delete suborganization.	name of suborganization	Attempted to delete suborganization.	
222	INFO	Delete suborganization.	name of suborganization	Deleted suborganization.	
223	INFO	Attempt to modify role	name of role	Attempted to modify role.	
224	INFO	Modify role	name of role	Modified role.	
225	INFO	Attempt to modify suborganization.	name of suborganization	Attempted to modify suborganization.	
226	INFO	Modify suborganization.	name of suborganization	Modified suborganization.	
227	INFO	Attempt to delete user.	name of user	Attempted to delete user.	
228	INFO	Delete user.	name of user	Deleted user.	
229	INFO	Attempt to modify user.	name of user	Attempted to modify user.	
230	INFO	Modify user.	name of user	Modified user.	
231	INFO	Attempt to add values to a Service Attribute in a Realm.	name of attribute name of service name of realm	Attempted to add values to a Service Attribute in a Realm.	
232	INFO	Add values to a Service Attribute in a Realm.	name of attribute name of service name of realm	Added values to a Service Attribute in a Realm.	
233	INFO	Attempt to assign a Service to a Realm	name of service name of realm	Attempted to assign a Service to a Realm.	
234	INFO	Assign a Service to a Realm	name of service name of realm	Assigned a Service to a Realm.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
235	INFO	Attempt to create a Realm	name of realm created name of parent realm	Attempted to create a Realm.	
236	INFO	Create a Realm	name of realm created name of parent realm	Created a Realm.	
237	INFO	Delete Realm.	recursive or not name of realm deleted	Deleted Realm.	
238	INFO	Delete Realm.	recursive or not name of realm deleted	Deleted Realm.	
239	INFO	Attempt to modify a service in a Realm.	name of service name of realm	Attempted to modify a service in a Realm.	
240	INFO	Modify a service in a Realm.	name of service name of realm	Modified a service in a Realm.	
241	INFO	Attempt to remove an attribute from a service in a Realm	name of attribute name of service name of realm	Attempted to remove an attribute from a service in a Realm.	
242	INFO	Remove an attribute from a service in a Realm	name of attribute name of service name of realm	Removed an attribute from a service in a Realm.	
243	INFO	Attempt to remove values from a service's attribute in a Realm	name of attribute name of service name of realm	Attempted to remove values from a service's attribute in a Realm.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
244	INFO	Remove values from a service's attribute in a Realm	name of attribute name of service name of realm	Removed values from a service's attribute in a Realm.	
245	INFO	Attempt to set attributes for a service in a Realm.	name of service name of realm	Attempted to set attributes for a service in a Realm.	
246	INFO	Set attributes for a service in a Realm.	name of service name of realm	Set attributes for a service in a Realm.	
247	INFO	Attempt to unassign a service from a Realm.	name of service name of realm	Attempted to unassign a service from a Realm.	
248	INFO	Unassign a service from a Realm.	name of service name of realm	Unassigned a service from a Realm.	
249	INFO	Attempt to assign a Service to an Organization Configuration	name of service name of realm	Attempted to assign a Service to an Organization Configuration.	
250	INFO	Assign a Service to an Organization Configuration	name of service name of realm	Assigned a Service to an Organization Configuration.	
251	INFO	Assign a Service to an Organization Configuration Not Done	name of service name of realm	Assigned a Service to an Organization Configuration, but the service is not one of the org config's assignable services.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
252	INFO	Assign a Service to a Realm Not Done	name of service name of realm	Assigned a Service to a Realm, but the service is not one of the realm's assignable services.	
253	INFO	Attempt to unassign a service from an Organization Configuration.	name of service name of realm	Attempted to unassign a service from an Organization Configuration.	
254	INFO	Unassign a service from an Organization Configuration.	name of service name of realm	Unassigned a service from an Organization Configuration.	
255	INFO	Unassign a service not in the Organization Configuration or Realm.	name of service name of realm	Requested to unassign a service not in the Organization Configuration or Realm.	
256	INFO	Attempt to modify a service in an Organization Configuration.	name of service name of realm	Attempted to modify a service in an Organization Configuration.	
257	INFO	Modify a service in an Organization Configuration.	name of service name of realm	Modified a service in an Organization Configuration.	
258	INFO	Modify a service not in the Organization Configuration or Realm.	name of service name of realm	Attempted to modify a service not in the Organization Configuration or Realm.	

TABLE 10–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
259	INFO	Attempt to get privileges of an Identity.	name of realm name of identity type of identity	Attempted to get privileges of an Identity.	
260	INFO	Get privileges of an Identity.	name of realm name of identity type of identity	Gotten privileges of an Identity.	
261	INFO	Attempt to add privileges to an Identity.	name of realm name of identity type of identity	Attempted to add privileges to an Identity.	
262	INFO	Added privileges to an Identity.	name of realm name of identity type of identity	Added privileges to an Identity.	
263	INFO	Attempt to remove privileges from an Identity.	name of realm name of identity type of identity	Attempted to remove privileges from an Identity.	
264	INFO	Removed privileges to an Identity.	name of realm name of identity type of identity	Removed privileges from an Identity.	

Authentication

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-100	INFO	Authentication is Successful	message	User authenticated with valid credentials	
AUTHENTICATION-101	INFO	User based authentication is successful	message authentication type user name	User authenticated with valid credentials	

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-102	INFO	Role based authentication is successful	message authentication type role name	User belonging to role authenticated with valid credentials	
AUTHENTICATION-103	INFO	Service based authentication is successful	message authentication type service name	User authenticated with valid credentials to a configured service under realm	
AUTHENTICATION-104	INFO	Authentication level based authentication is successful	message authentication type authentication level value	User authenticated with valid credentials to one or more authentication modules having authentication level value greater than or equal to specified authentication level	
AUTHENTICATION-105	INFO	Module based authentication is successful	message authentication type module name	User authenticated with valid credentials to authentication module under realm	
AUTHENTICATION-200	INFO	Authentication Failed	error message	Incorrect/invalid credentials presented User locked out/not active	Enter correct/valid credentials to required authentication module
AUTHENTICATION-201	INFO	Authentication Failed	error message	Invalid credentials entered.	Enter the correct password.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-202	INFO	Authentication Failed	error message	Named Configuration (Auth Chain) does not exist.	Create and configure a named config for this org.
AUTHENTICATION-203	INFO	Authentication Failed	error message	No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.
AUTHENTICATION-204	INFO	Authentication Failed	error message	This user is not active.	Activate the user.
AUTHENTICATION-205	INFO	Authentication Failed	error message	Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
AUTHENTICATION-206	INFO	Authentication Failed	error message	User account has expired.	Contact system administrator.
AUTHENTICATION-207	INFO	Authentication Failed	error message	Login timed out.	Try to login again.
AUTHENTICATION-208	INFO	Authentication Failed	error message	Authentication module is denied.	Configure this module or use some other module.
AUTHENTICATION-209	INFO	Authentication Failed	error message	Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
AUTHENTICATION-210	INFO	Authentication Failed	error message	Org/Realm does not exists.	Use a valid Org/Realm.
AUTHENTICATION-211	INFO	Authentication Failed	error message	Org/Realm is not active.	Activate the Org/Realm.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-012	INFO	Authentication Failed	error message	Cannot create a session.	Ensure that session service is configured and maxsession is not reached.
AUTHENTICATION-013	INFO	User based authentication failed	error message authentication type user name	No authentication configuration (chain of one or more authentication modules) configured for user Incorrect/invalid credentials presented User locked out/not active	Configure authentication configuration (chain of one or more authentication modules) for user Enter correct/valid credentials to required authentication module
AUTHENTICATION-014	INFO	Authentication Failed	error message authentication type user name	User based Auth. Invalid credentials entered.	Enter the correct password.
AUTHENTICATION-015	INFO	Authentication Failed	error message authentication type user name	Named Configuration (Auth Chain) does not exist for this user	Create and configure a named config for this user
AUTHENTICATION-016	INFO	Authentication Failed	error message authentication type user name	User based Auth. No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-217	INFO	Authentication Failed	error message authentication type user name	User based Auth. This user is not active.	Activate the user.
AUTHENTICATION-218	INFO	Authentication Failed	error message authentication type user name	User based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
AUTHENTICATION-219	INFO	Authentication Failed	error message authentication type user name	User based Auth. User account has expired.	Contact system administrator.
AUTHENTICATION-220	INFO	Authentication Failed	error message authentication type user name	User based Auth. Login timed out.	Try to login again.
AUTHENTICATION-221	INFO	Authentication Failed	error message authentication type user name	User based Auth. Authentication module is denied.	Configure this module or use some other module.
AUTHENTICATION-222	INFO	Authentication Failed	error message authentication type user name	User based auth. Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
AUTHENTICATION-223	INFO	Authentication Failed	error message authentication type user name	User based auth. Org/Realm does not exists.	Use a valid Org/Realm.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-224	INFO	Authentication Failed	error message authentication type user name	User based auth. Org/Realm is not active.	Activate the Org/Realm.
AUTHENTICATION-225	INFO	Authentication Failed	error message authentication type user name	User based auth. Cannot create a session.	Ensure that session service is configured and maxsession is not reached.
AUTHENTICATION-226	INFO	Role based authentication failed	error message authentication type role name	No authentication configuration (chain of one or more authentication modules) configured for role Incorrect/invalid credentials presented User does not belong to this role User locked out/not active	Configure authentication configuration (chain of one or more authentication modules) for role Enter correct/valid credentials to required authentication module Assign this role to the authenticating user
AUTHENTICATION-227	INFO	Authentication Failed	error message authentication type role name	Role based Auth. Invalid credentials entered.	Enter the correct password.
AUTHENTICATION-228	INFO	Authentication Failed	error message authentication type role name	Named Configuration (Auth Chain) does not exist for this role.	Create and configure a named config for this role.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-229	INFO	Authentication Failed	error message authentication type role name	Role based Auth. No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.
AUTHENTICATION-230	INFO	Authentication Failed	error message authentication type role name	Role based Auth. This user is not active.	Activate the user.
AUTHENTICATION-231	INFO	Authentication Failed	error message authentication type role name	Role based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
AUTHENTICATION-232	INFO	Authentication Failed	error message authentication type role name	Role based Auth. User account has expired.	Contact system administrator.
AUTHENTICATION-233	INFO	Authentication Failed	error message authentication type role name	Role based Auth. Login timed out.	Try to login again.
AUTHENTICATION-234	INFO	Authentication Failed	error message authentication type role name	Role based Auth. Authentication module is denied.	Configure this module or use some other module.
AUTHENTICATION-235	INFO	Authentication Failed	error message authentication type role name	Role based auth. Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-236	INFO	Authentication Failed	error message authentication type role name	Role based auth. Org/Realm does not exists.	Use a valid Org/Realm.
AUTHENTICATION-237	INFO	Authentication Failed	error message authentication type role name	Role based auth. Org/Realm is not active.	Activate the Org/Realm.
AUTHENTICATION-238	INFO	Authentication Failed	error message authentication type role name	Role based auth. Cannot create a session.	Ensure that session service is configured and maxsession is not reached.
AUTHENTICATION-239	INFO	Authentication Failed	error message authentication type role name	Role based auth. User does not belong to this role.	Add the user to this role.
AUTHENTICATION-240	INFO	Service based authentication failed	error message authentication type service name	No authentication configuration (chain of one or more authentication modules) configured for service Incorrect/invalid credentials presented User locked out/not active	Configure authentication configuration (chain of one or more authentication modules) for service Enter correct/valid credentials to required authentication module
AUTHENTICATION-241	INFO	Authentication Failed	error message authentication type service name	Service based Auth. Invalid credentials entered.	Enter the correct password.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-242	INFO	Authentication Failed	error message authentication type service name	Named Configuration (Auth Chain) does not exist with this service name.	Create and configure a named config.
AUTHENTICATION-243	INFO	Authentication Failed	error message authentication type service name	Service based Auth. No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.
AUTHENTICATION-244	INFO	Authentication Failed	error message authentication type service name	Service based Auth. This user is not active.	Activate the user.
AUTHENTICATION-245	INFO	Authentication Failed	error message authentication type service name	Service based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
AUTHENTICATION-246	INFO	Authentication Failed	error message authentication type service name	Service based Auth. User account has expired.	Contact system administrator.
AUTHENTICATION-247	INFO	Authentication Failed	error message authentication type service name	Service based Auth. Login timed out.	Try to login again.
AUTHENTICATION-248	INFO	Authentication Failed	error message authentication type service name	Service based Auth. Authentication module is denied.	Configure this module or use some other module.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-249	INFO	Authentication Failed	error message authentication type service name	Service based Auth. Service does not exist.	Please use only valid Service.
AUTHENTICATION-250	INFO	Authentication Failed	error message authentication type service name	Service based auth. Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
AUTHENTICATION-251	INFO	Authentication Failed	error message authentication type service name	Service based auth. Org/Realm does not exists.	Use a valid Org/Realm.
AUTHENTICATION-252	INFO	Authentication Failed	error message authentication type service name	Service based auth. Org/Realm is not active.	Activate the Org/Realm.
AUTHENTICATION-253	INFO	Authentication Failed	error message authentication type service name	Service based auth. Cannot create a session.	Ensure that session service is configured and maxsession is not reached.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-254	INFO	Authentication level based authentication failed	error message authentication type authentication level value	There are no authentication module(s) having authentication level value greater than or equal to specified authentication level Incorrect/invalid credentials presented to one or more authentication modules having authentication level greater than or equal to specified authentication level User locked out/not active	Configure one or more authentication modules having authentication level value greater than or equal to required authentication level Enter correct/valid credentials to one or more authentication modules having authentication level greater than or equal to specified authentication level
AUTHENTICATION-255	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. Invalid credentials entered.	Enter the correct password.
AUTHENTICATION-256	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. No Auth Configuration available.	Create an auth configuration.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-257	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.
AUTHENTICATION-258	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. This user is not active.	Activate the user.
AUTHENTICATION-259	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
AUTHENTICATION-260	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. User account has expired.	Contact system administrator.
AUTHENTICATION-261	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. Login timed out.	Try to login again.
AUTHENTICATION-262	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. Authentication module is denied.	Configure this module or use some other module.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-263	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. Invalid Authg Level.	Please specify valid auth level.
AUTHENTICATION-264	INFO	Authentication Failed	error message authentication type authentication level value	Level based auth. Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
AUTHENTICATION-265	INFO	Authentication Failed	error message authentication type authentication level value	Level based auth. Org/Realm does not exists.	Use a valid Org/Realm.
AUTHENTICATION-266	INFO	Authentication Failed	error message authentication type authentication level value	Level based auth. Org/Realm is not active.	Activate the Org/Realm.
AUTHENTICATION-267	INFO	Authentication Failed	error message authentication type authentication level value	Level based auth. Cannot create a session.	Ensure that session service is configured and maxsession is not reached.
AUTHENTICATION-268	INFO	Module based authentication failed	error message authentication type module name	Module is not registered/configured under realm Incorrect/invalid credentials presented User locked out/not active	Register/configure authentication module under realm Enter correct/valid credentials to authentication module

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-269	INFO	Authentication Failed	error message authentication type module name	Module based Auth. Invalid credentials entered.	Enter the correct password.
AUTHENTICATION-270	INFO	Authentication Failed	error message authentication type module name	Module based Auth. No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.
AUTHENTICATION-271	INFO	Authentication Failed	error message authentication type module name	Module based Auth. This user is not active.	Activate the user.
AUTHENTICATION-272	INFO	Authentication Failed	error message authentication type module name	Module based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
AUTHENTICATION-273	INFO	Authentication Failed	error message authentication type module name	Module based Auth. User account has expired.	Contact system administrator.
AUTHENTICATION-274	INFO	Authentication Failed	error message authentication type module name	Module based Auth. Login timed out.	Try to login again.
AUTHENTICATION-275	INFO	Authentication Failed	error message authentication type module name	Module based Auth. Authentication module is denied.	Configure this module or use some other module.

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-276	INFO	Authentication Failed	error message authentication type module name	Module based auth. Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
AUTHENTICATION-277	INFO	Authentication Failed	error message authentication type module name	Module based auth. Org/Realm does not exists.	Use a valid Org/Realm.
AUTHENTICATION-278	INFO	Authentication Failed	error message authentication type module name	Module based auth. Org/Realm is not active.	Activate the Org/Realm.
AUTHENTICATION-279	INFO	Authentication Failed	error message authentication type module name	Module based auth. Cannot create a session.	Ensure that session service is configured and maxsession is not reached.
AUTHENTICATION-300	INFO	User logout is Successful	message	User logged out	
AUTHENTICATION-301	INFO	User logout is successful from user based authentication	message authentication type user name	User logged out	
AUTHENTICATION-302	INFO	User logout is successful from role based authentication	message authentication type role name	User belonging to this role logged out	
AUTHENTICATION-303	INFO	User logout is successful from service based authentication	message authentication type service name	User logged out of a configured service under realm	

TABLE 10–2 Log Reference Document for AuthenticationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AUTHENTICATION-304	INFO	User logout is successful from authentication level based authentication	message authentication type authentication level value	User logged out of one or more authentication modules having authentication level value greater than or equal to specified authentication level	
AUTHENTICATION-305	INFO	User logout is successful from module based authentication	message authentication type module name	User logged out of authentication module under realm	

Command Line Interface – ssoadm

TABLE 10–3 Log Reference Document for CLILogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-1	INFO	Attempt to login to execute the commandline.	user ID	Run the Commandline tool.	
AMCLI-2	INFO	Login to execute the commandline.	user ID	Run the Commandline tool.	
AMCLI-3	INFO	Failed to login.	user ID error message	Run the Commandline tool.	Check your user ID and password. Look under debug file for more information.
AMCLI-20	INFO	Attempt to load schema to data store.	XML file name	Load Schema through Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-21	INFO	Schema is loaded to data store.	XML file name	Load Schema through Commandline interface.	
AMCLI-22	SEVERE	Schema is not loaded to data store.	XML file name error message	Load Schema through Commandline interface.	Look under debug file for more information.
AMCLI-30	INFO	Attempt to delete service from data store.	service name	Delete Service through Commandline interface.	
AMCLI-31	INFO	Deleted service from data store.	service name	Delete Service through Commandline interface.	
AMCLI-32	SEVERE	Schema is not loaded to data store.	service name error message	Delete Service Schema through Commandline interface.	Look under debug file for more information.
AMCLI-40	INFO	Attempt to attribute schema to an existing service.	service name schema type XML file name	Add attribute schema through Commandline interface.	
AMCLI-41	INFO	Added attribute schema to existing service.	service name schema type XML file name	Add attribute schema through Commandline interface.	
AMCLI-42	SEVERE	Attribute schema is not added to existing service.	service name schema type XML file name error message	Add attribute schema through Commandline interface.	Check the service name, schema type and XML file. Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-50	INFO	Attempt to add resource bundle to data store.	resource bundle name file name locale	Add Resource Bundle through Commandline interface.	
AMCLI-51	INFO	Resource bundle is added to data store.	resource bundle name file name locale	Add Resource Bundle through Commandline interface.	
AMCLI-52	SEVERE	Failed to add resource bundle to data store.	resource bundle name file name locale error message	SDK for adding resource bundle failed.	Look under debug file for more information.
AMCLI-60	INFO	Attempt to get resource bundle from data store.	resource bundle name locale	Get Resource Bundle through Commandline interface.	
AMCLI-61	INFO	Resource bundle retrieved from data store.	resource bundle name locale	Get Resource Bundle through Commandline interface.	
AMCLI-62	SEVERE	Failed to get resource bundle from data store.	resource bundle name locale error message	SDK for getting resource bundle failed.	Look under debug file for more information.
AMCLI-70	INFO	Attempt to delete resource bundle from data store.	resource bundle name locale	Delete Resource Bundle through Commandline interface.	
AMCLI-71	INFO	Resource bundle deleted from data store.	resource bundle name locale	Delete Resource Bundle through Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-72	SEVERE	Failed to delete resource bundle from data store.	resource bundle name locale error message	SDK for deleting resource bundle failed.	Look under debug file for more information.
AMCLI-100	INFO	Attempt to destroy Session destroyed	name of user	Administrator invalidates session via Commandline interface.	
AMCLI-101	INFO	Session destroyed	name of user	Administrator invalidates session via Commandline interface.	
AMCLI-102	SEVERE	Failed to destroy session	name of user error message	Session cannot be destroyed.	Look under debug file for more information.
AMCLI-1000	INFO	Attempt to migration organization to realm/	distinguished name of organization	Migration Commandline interface.	
AMCLI-1001	INFO	Migration completed.	distinguished name of organization	Migration Commandline interface.	
AMCLI-2000	INFO	Attempt to delete realm/	name of realm recursive	Delete realm command through Commandline interface.	
AMCLI-2001	INFO	Realm deleted.	name of realm recursive	Delete realm command through Commandline interface.	
AMCLI-2002	INFO	Failed to delete realm.	name of realm recursive error message	Delete realm command through Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2010	INFO	Attempt to create realm/	name of realm	Create realm command through Commandline interface.	
AMCLI-2011	INFO	Realm created.	name of realm	Create realm command through Commandline interface.	
AMCLI-2012	INFO	Failed to create realm.	name of realm error message	Create realm command through Commandline interface.	Look under debug file for more information.
AMCLI-3020	INFO	Attempt to search for realms by name.	name of realm search pattern recursive	Search realms command through Commandline interface.	
AMCLI-3021	INFO	Completed searching for realms.	name of realm search pattern recursive	Search realms command through Commandline interface.	
AMCLI-3022	INFO	Search for realms failed.	name of realm search pattern recursive error message	Search realms command through Commandline interface.	Look under debug file for more information.
AMCLI-2020	INFO	Attempt to get assignable services of realm.	name of realm	Execute get assignable services of realm Commandline interface.	
AMCLI-2021	INFO	Assignable services command is serviced.	name of realm	Execute get assignable services of realm Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2022	INFO	Unable to get assignable services of realm.	name of realm error message	Execute get assignable services of realm Commandline interface.	Look under debug file for more information.
AMCLI-2030	INFO	Attempt to get services assigned to a realm.	name of realm include mandatory services	Execute get services assigned to realm Commandline interface.	
AMCLI-2031	INFO	Assignable services command is serviced.	name of realm include mandatory services	Execute get services assigned to realm Commandline interface.	
AMCLI-2032	INFO	Unable to get services assigned to realm.	name of realm include mandatory services error message	Execute get services assigned to realm Commandline interface.	Look under debug file for more information.
AMCLI-2040	INFO	Attempt to assign service to a realm.	name of realm name of service	Execute assign service to realm Commandline interface.	
AMCLI-2041	INFO	Service is assigned to realm.	name of realm name of service	Execute assign service to realm Commandline interface.	
AMCLI-2042	INFO	Unable to assign service to realm.	name of realm name of service error message	Execute assign service to realm Commandline interface.	Look under debug file for more information.
AMCLI-2050	INFO	Attempt to unassign service from a realm.	name of realm name of service	Execute unassign service from realm Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2051	INFO	Service is unassigned from realm.	name of realm name of service	Execute unassign service from realm Commandline interface.	
AMCLI-2052	INFO	Unable to unassign service from realm.	name of realm name of service error message	Execute unassign service from realm Commandline interface.	Look under debug file for more information.
AMCLI-2060	INFO	Attempt to get service attribute values from a realm.	name of realm name of service	Execute get service attribute values from realm Commandline interface.	
AMCLI-2061	INFO	Service attribute values of realm is returneed.	name of realm name of service	Execute get service attribute values from realm Commandline interface.	
AMCLI-2062	INFO	Unable to get service attribute values of realm.	name of realm name of service error message	Execute get service attribute values from realm Commandline interface.	Look under debug file for more information.
AMCLI-2070	INFO	Attempt to remove attribute from a realm.	name of realm name of service name of attribute	Execute remove attribute from realm Commandline interface.	
AMCLI-2071	INFO	Attribute of realm is removed.	name of realm name of service name of attribute	Execute remove attribute from realm Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2072	INFO	Unable to remove attribute from realm.	name of realm name of service name of attribute error message	Execute remove attribute from realm Commandline interface.	Look under debug file for more information.
AMCLI-2080	INFO	Attempt to modify service of realm.	name of realm name of service	Execute modify service of realm Commandline interface.	
AMCLI-2081	INFO	Attribute of realm is modified.	name of realm name of service	Execute modify service of realm Commandline interface.	
AMCLI-2082	INFO	Unable to modify service of realm.	name of realm name of service error message	Execute modify service of realm Commandline interface.	Look under debug file for more information.
AMCLI-2090	INFO	Attempt to add attribute value to realm.	name of realm name of service name of attribute	Execute add attribute values to realm Commandline interface.	
AMCLI-2091	INFO	Attribute values is added to realm.	name of realm name of service name of attribute	Execute add attribute values to realm Commandline interface.	
AMCLI-2092	INFO	Unable to add attribute values to realm.	name of realm name of service name of attribute error message	Execute add attribute values to realm Commandline interface.	Look under debug file for more information.
AMCLI-2100	INFO	Attempt to set attribute value to realm.	name of realm name of service	Execute set attribute values to realm Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2101	INFO	Attribute values is set to realm.	name of realm name of service	Execute set attribute values to realm Commandline interface.	
AMCLI-2102	INFO	Unable to set attribute values to realm.	name of realm name of service error message	Execute set attribute values to realm Commandline interface.	Look under debug file for more information.
AMCLI-2110	INFO	Attempt to remove schema attribute defaults.	name of service schema type name of sub schema name of attribute	Execute remove schema attribute defaults Commandline interface.	
AMCLI-2111	INFO	Schema attribute defaults is removed.	name of service schema type name of sub schema name of attribute	Execute remove schema attribute defaults Commandline interface.	
AMCLI-2112	INFO	Unable to remove schema attribute defaults.	name of service schema type name of sub schema name of attribute error message	Execute remove schema attribute defaults Commandline interface.	Look under debug file for more information.
AMCLI-2120	INFO	Attempt to add schema attribute defaults.	name of service schema type name of sub schema name of attribute	Execute add schema attribute defaults Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2121	INFO	Schema attribute defaults is added.	name of service schema type name of sub schema name of attribute	Execute add schema attribute defaults Commandline interface.	
AMCLI-2122	INFO	Unable to add schema attribute defaults.	name of service schema type name of sub schema name of attribute error message	Execute add schema attribute defaults Commandline interface.	Look under debug file for more information.
AMCLI-2130	INFO	Attempt to get schema attribute defaults.	name of service schema type name of sub schema	Execute get schema attribute defaults Commandline interface.	
AMCLI-2131	INFO	Schema attribute defaults is returned.	name of service schema type name of sub schema	Execute get schema attribute defaults Commandline interface.	
AMCLI-2132	INFO	Unable to get schema attribute defaults.	name of service schema type name of sub schema error message	Execute get schema attribute defaults Commandline interface.	Look under debug file for more information.
AMCLI-2140	INFO	Attempt to set schema attribute defaults.	name of service schema type name of sub schema	Execute set schema attribute defaults Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2141	INFO	Schema attribute defaults is set.	name of service schema type name of sub schema	Execute set schema attribute defaults Commandline interface.	
AMCLI-2142	INFO	Unable to set schema attribute defaults.	name of service schema type name of sub schema error message	Execute set schema attribute defaults Commandline interface.	Look under debug file for more information.
AMCLI-2150	INFO	Attempt to add choice value to attribute schema.	name of service schema type name of sub schema name of attribute schema	Execute add attribute schema choice values Commandline interface.	
AMCLI-2151	INFO	Choice values are added.	name of service schema type name of sub schema name of attribute schema	Execute add attribute schema choice values Commandline interface.	
AMCLI-2152	INFO	Unable to add choice value to attribute schema.	name of service schema type name of sub schema name of attribute schema error message	Execute add attribute schema choice values Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2160	INFO	Attempt to remove choice value from attribute schema.	name of service schema type name of sub schema name of attribute schema	Execute remove attribute schema choice values Commandline interface.	
AMCLI-2161	INFO	Choice value is removed.	name of service schema type name of sub schema name of attribute schema	Execute remove attribute schema choice values Commandline interface.	
AMCLI-2162	INFO	Unable to remove choice value to attribute schema.	name of service schema type name of sub schema name of attribute schema error message	Execute remove attribute schema choice values Commandline interface.	Look under debug file for more information.
AMCLI-2170	INFO	Attempt to modify attribute schema type.	name of service schema type name of sub schema name of attribute schema attribute schema type	Execute modify attribute schema type Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2171	INFO	Attribute schema type is modified.	name of service schema type name of sub schema name of attribute schema attribute schema type	Execute modify attribute schema type Commandline interface.	
AMCLI-2172	INFO	Unable to modify attribute schema type.	name of service schema type name of sub schema name of attribute schema attribute schema type error message	Execute modify attribute schema type Commandline interface.	Look under debug file for more information.
AMCLI-2180	INFO	Attempt to modify attribute schema UI type.	name of service schema type name of sub schema name of attribute schema attribute schema UI type	Execute modify attribute schema UI type Commandline interface.	
AMCLI-2181	INFO	Attribute schema UI type is modified.	name of service schema type name of sub schema name of attribute schema attribute schema UI type	Execute modify attribute schema UI type Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2182	INFO	Unable to modify attribute schema UI type.	name of service schema type name of sub schema name of attribute schema attribute schema UI type error message	Execute modify attribute schema UI type Commandline interface.	Look under debug file for more information.
AMCLI-2190	INFO	Attempt to modify attribute schema syntax.	name of service schema type name of sub schema name of attribute schema attribute schema syntax	Execute modify attribute schema syntax Commandline interface.	
AMCLI-2191	INFO	Attribute schema syntax is modified.	name of service schema type name of sub schema name of attribute schema attribute schema syntax	Execute modify attribute schema syntax Commandline interface.	
AMCLI-2192	INFO	Unable to modify attribute schema syntax.	name of service schema type name of sub schema name of attribute schema attribute schema syntax error message	Execute modify attribute schema syntax Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2200	INFO	Attempt to modify attribute schema i18n Key.	name of service schema type name of sub schema name of attribute schema attribute schema i18n Key	Execute modify attribute schema i18n Key Commandline interface.	
AMCLI-2201	INFO	Attribute schema i18n Key is modified.	name of service schema type name of sub schema name of attribute schema attribute schema i18n Key	Execute modify attribute schema i18n Key Commandline interface.	
AMCLI-2202	INFO	Unable to modify attribute schema i18n Key.	name of service schema type name of sub schema name of attribute schema attribute schema i18n Key error message	Execute modify attribute schema i18n Key Commandline interface.	Look under debug file for more information.
AMCLI-2210	INFO	Attempt to modify attribute schema properties view bean URL.	name of service schema type name of sub schema name of attribute schema attribute schema properties view bean URL	Execute modify attribute schema properties view bean URL Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2211	INFO	Attribute schema properties view bean URL is modified.	name of service schema type name of sub schema name of attribute schema attribute schema properties view bean URL	Execute modify attribute schema properties view bean URL Commandline interface.	
AMCLI-2212	INFO	Unable to modify attribute schema properties view bean URL.	name of service schema type name of sub schema name of attribute schema attribute schema properties view bean URL error message	Execute modify attribute schema properties view bean URL Commandline interface.	Look under debug file for more information.
AMCLI-2220	INFO	Attempt to modify attribute schema any value.	name of service schema type name of sub schema name of attribute schema attribute schema any	Execute modify attribute schema any Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2221	INFO	Attribute schema any value is modified.	name of service schema type name of sub schema name of attribute schema attribute schema any	Execute modify attribute schema any Commandline interface.	
AMCLI-2222	INFO	Unable to modify attribute schema any value.	name of service schema type name of sub schema name of attribute schema attribute schema any error message	Execute modify attribute schema any Commandline interface.	Look under debug file for more information.
AMCLI-2230	INFO	Attempt to remove attribute schema default value.	name of service schema type name of sub schema name of attribute schema default value to be removed	Execute remove attribute schema default values Commandline interface.	
AMCLI-2231	INFO	Attribute schema default value is removed.	name of service schema type name of sub schema name of attribute schema default value to be removed	Execute remove attribute schema default values Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2232	INFO	Unable to remove attribute schema default value.	name of service schema type name of sub schema name of attribute schema default value to be removed error message	Execute remove attribute schema default values Commandline interface.	Look under debug file for more information.
AMCLI-2240	INFO	Attempt to set attribute schema validator.	name of service schema type name of sub schema name of attribute schema validator	Execute set attribute schema validator Commandline interface.	
AMCLI-2241	INFO	Attribute schema validator is set.	name of service schema type name of sub schema name of attribute schema validator	Execute set attribute schema validator Commandline interface.	
AMCLI-2242	INFO	Unable to set attribute schema validator.	name of service schema type name of sub schema name of attribute schema validator error message	Execute set attribute schema validator Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2250	INFO	Attempt to set attribute schema start range.	name of service schema type name of sub schema name of attribute schema start range	Execute set attribute schema start range Commandline interface.	
AMCLI-2251	INFO	Attribute schema start range is set.	name of service schema type name of sub schema name of attribute schema start range	Execute set attribute schema start range Commandline interface.	
AMCLI-2252	INFO	Unable to set attribute schema start range.	name of service schema type name of sub schema name of attribute schema start range error message	Execute set attribute schema start range Commandline interface.	Look under debug file for more information.
AMCLI-2250	INFO	Attempt to set attribute schema end range.	name of service schema type name of sub schema name of attribute schema end range	Execute set attribute schema end range Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2251	INFO	Attribute schema end range is set.	name of service schema type name of sub schema name of attribute schema end range	Execute set attribute schema end range Commandline interface.	
AMCLI-2252	INFO	Unable to set attribute schema end range.	name of service schema type name of sub schema name of attribute schema end range error message	Execute set attribute schema end range Commandline interface.	Look under debug file for more information.
AMCLI-2260	INFO	Attempt to set service schema i18n key.	name of service i18n key	Execute set service schema i18n key Commandline interface.	
AMCLI-2261	INFO	Service schema i18n key is set.	name of service i18n key	Execute set service schema i18n key Commandline interface.	
AMCLI-2262	INFO	Unable to set service schema i18n key.	name of service i18n key error message	Execute set service schema i18n key Commandline interface.	Look under debug file for more information.
AMCLI-2270	INFO	Attempt to set service schema properties view bean URL.	name of service properties view bean URL	Execute set service schema properties view bean URL Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2271	INFO	Service schema properties view bean URL is set.	name of service properties view bean URL	Execute set service schema properties view bean URL Commandline interface.	
AMCLI-2272	INFO	Unable to set service schema properties view bean URL.	name of service properties view bean URL error message	Execute set service schema properties view bean URL Commandline interface.	Look under debug file for more information.
AMCLI-2280	INFO	Attempt to set service revision number.	name of service revision number	Execute set service revision number Commandline interface.	
AMCLI-2281	INFO	Service revision number is set.	name of service revision number	Execute set service revision number Commandline interface.	
AMCLI-2282	INFO	Unable to set service revision number.	name of service revision number error message	Execute set service revision number Commandline interface.	Look under debug file for more information.
AMCLI-2290	INFO	Attempt to get service revision number.	name of service	Execute get service revision number Commandline interface.	
AMCLI-2291	INFO	Service revision number is returned.	name of service	Execute get service revision number Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2292	INFO	Unable to get service revision number.	name of service error message	Execute get service revision number Commandline interface.	Look under debug file for more information.
AMCLI-2300	INFO	Attempt to remove attribute schema.	name of service schema type name of sub schema name of attribute schema	Execute remove attribute schema Commandline interface.	
AMCLI-2301	INFO	Attribute schema is removed.	name of service schema type name of sub schema name of attribute schema	Execute remove attribute schema Commandline interface.	
AMCLI-2302	INFO	Unable to remove attribute schema.	name of service schema type name of sub schema name of attribute schema error message	Execute remove attribute schema Commandline interface.	Look under debug file for more information.
AMCLI-2310	INFO	Attempt to add sub configuration.	name of sub configuration name of service	Execute add sub configuration Commandline interface.	
AMCLI-2311	INFO	Sub configuration is added.	name of sub configuration name of service	Execute add sub configuration Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2312	INFO	Unable to add sub configuration.	name of sub configuration name of service error message	Execute add sub configuration Commandline interface.	Look under debug file for more information.
AMCLI-2320	INFO	Attempt to add sub configuration to realm.	name of realm name of sub configuration name of service	Execute add sub configuration Commandline interface.	
AMCLI-2321	INFO	Sub configuration is added to realm.	name of realm name of sub configuration name of service	Execute add sub configuration Commandline interface.	
AMCLI-2322	INFO	Unable to add sub configuration.	name of realm name of sub configuration name of service error message	Execute add sub configuration Commandline interface.	Look under debug file for more information.
AMCLI-2330	INFO	Attempt to delete sub configuration.	name of sub configuration name of service	Execute delete sub configuration Commandline interface.	
AMCLI-2331	INFO	Sub configuration is deleted.	name of sub configuration name of service	Execute delete sub configuration Commandline interface.	
AMCLI-2332	INFO	Unable to delete sub configuration.	name of sub configuration name of service error message	Execute delete sub configuration Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2340	INFO	Attempt to delete sub configuration from realm.	name of realm name of sub configuration name of service	Execute delete sub configuration Commandline interface.	
AMCLI-2341	INFO	Sub configuration is deleted from realm.	name of realm name of sub configuration name of service	Execute delete sub configuration Commandline interface.	
AMCLI-2342	INFO	Unable to delete sub configuration.	name of realm name of sub configuration name of service error message	Execute delete sub configuration Commandline interface.	Look under debug file for more information.
AMCLI-2350	INFO	Attempt to add sub schema.	name of service schema type name of sub schema	Execute add sub schema Commandline interface.	
AMCLI-2351	INFO	Sub schema is added.	name of service schema type name of sub schema	Execute add sub schema Commandline interface.	
AMCLI-2352	INFO	Unable to add sub schema.	name of service schema type name of sub schema error message	Execute add sub schema configurations Commandline interface.	Look under debug file for more information.
AMCLI-2360	INFO	Attempt to remove sub schema.	name of service schema type name of parent sub schema name of sub schema	Execute remove sub schema Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2361	INFO	Sub schema is removed.	name of service schema type name of parent sub schema name of sub schema	Execute remove sub schema Commandline interface.	
AMCLI-2362	INFO	Unable to remove sub schema.	name of service schema type name of parent sub schema name of sub schema error message	Execute remove sub schema configurations Commandline interface.	Look under debug file for more information.
AMCLI-2370	INFO	Attempt to modify inheritance of sub schema.	name of service schema type name of sub schema	Execute modify inheritance of sub schema Commandline interface.	
AMCLI-2371	INFO	Sub schema is modified.	name of service schema type name of sub schema	Execute modify inheritance of sub schema Commandline interface.	
AMCLI-2372	INFO	Unable to modify sub schema.	name of service schema type name of sub schema error message	Execute modify inheritance of sub schema configurations Commandline interface.	Look under debug file for more information.
AMCLI-2380	INFO	Attempt to modify sub configuration.	name of sub configuration name of service	Execute modify sub configuration Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2381	INFO	Sub configuration is modified.	name of sub configuration name of service	Execute modify sub configuration Commandline interface.	
AMCLI-2382	INFO	Unable to modify sub configuration.	name of sub configuration name of service error message	Execute modify sub configuration Commandline interface.	Look under debug file for more information.
AMCLI-2390	INFO	Attempt to modify sub configuration in realm.	name of realm name of sub configuration name of service	Execute modify sub configuration Commandline interface.	
AMCLI-2391	INFO	Sub configuration is modified.	name of realm name of sub configuration name of service	Execute modify sub configuration Commandline interface.	
AMCLI-2392	INFO	Unable to modify sub configuration in realm.	name of realm name of sub configuration name of service error message	Execute modify sub configuration Commandline interface.	Look under debug file for more information.
AMCLI-2400	INFO	Attempt to add Plug-in interface to service.	name of service name of plugin	Execute add Plug-in interface Commandline interface.	
AMCLI-2401	INFO	Plug-in interface is added.	name of service name of plugin	Execute add Plug-in interface Commandline interface.	
AMCLI-2402	INFO	Unable to add Plug-in interface to service.	name of service name of plugin error message	Execute add Plug-in interface Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2410	INFO	Attempt to set Plug-in schema's properties view bean.	name of service name of plugin	Execute set Plug-in schema's properties view bean Commandline interface.	
AMCLI-2411	INFO	Plug-in schema's properties view bean is set.	name of service name of plugin	Execute set Plug-in schema's properties view bean Commandline interface.	
AMCLI-2412	INFO	Unable to set Plug-in schema's properties view bean.	name of service name of plugin error message	Execute set Plug-in schema's properties view bean Commandline interface.	Look under debug file for more information.
AMCLI-2420	INFO	Attempt to create policies under realm.	name of realm	Execute create policies under realm Commandline interface.	
AMCLI-2421	INFO	Policies are created.	name of realm	Execute create policies under realm Commandline interface.	
AMCLI-2422	INFO	Unable to create policies under realm.	name of realm error message	Execute create policies under realm Commandline interface.	Look under debug file for more information.
AMCLI-2430	INFO	Attempt to delete policy in realm.	name of realm name of policy	Execute delete policy in realm Commandline interface.	
AMCLI-2431	INFO	Policy is deleted.	name of realm name of policy	Execute delete policy in realm Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2432	INFO	Unable to delete policy under realm.	name of realm name of policy error message	Execute delete policy under realm Commandline interface.	Look under debug file for more information.
AMCLI-2440	INFO	Attempt to get policy definition in realm.	name of realm name of policy	Execute get policy definition in realm Commandline interface.	
AMCLI-2441	INFO	Policy definition is returned.	name of realm name of policy	Execute get policy definition in realm Commandline interface.	
AMCLI-2442	INFO	Unable to get policy definition under realm.	name of realm name of policy error message	Execute get policy definition under realm Commandline interface.	Look under debug file for more information.
AMCLI-2450	INFO	Attempt to create an identity in realm.	name of realm identity type name of identity	Execute create identity in realm Commandline interface.	
AMCLI-2451	INFO	Identity is created.	name of realm identity type name of identity	Execute create identity in realm Commandline interface.	
AMCLI-2452	INFO	Unable to create identity in realm.	name of realm identity type name of identity error message	Execute create identity in realm Commandline interface.	Look under debug file for more information.
AMCLI-2460	INFO	Attempt to delete an identity in realm.	name of realm identity type name of identity	Execute delete identity in realm Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2461	INFO	Identity is deleted.	name of realm identity type name of identity	Execute delete identity in realm Commandline interface.	
AMCLI-2462	INFO	Unable to delete identity in realm.	name of realm identity type name of identity error message	Execute delete identity in realm Commandline interface.	Look under debug file for more information.
AMCLI-2470	INFO	Attempt to search identities in realm.	name of realm identity type search pattern	Execute search identities in realm Commandline interface.	
AMCLI-2471	INFO	Search Result is returned.	name of realm identity type search pattern	Execute search identities in realm Commandline interface.	
AMCLI-2472	INFO	Unable to search identities in realm.	name of realm identity type search pattern error message	Execute search identities in realm Commandline interface.	Look under debug file for more information.
AMCLI-2480	INFO	Attempt to get the allowed operation of an identity type in realm.	name of realm identity type	Execute get the allowed operation of an identity type in realm Commandline interface.	
AMCLI-2481	INFO	Allowed operations are returned.	name of realm identity type	Execute get the allowed operation of an identity type in realm Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2482	INFO	Unable to get the allowed operation of an identity type in realm.	name of realm identity type error message	Execute get the allowed operation of an identity type in realm Commandline interface.	Look under debug file for more information.
AMCLI-2490	INFO	Attempt to get the supported identity type in realm.	name of realm	Execute get the supported identity type in realm Commandline interface.	
AMCLI-2491	INFO	Allowed identity types are returned.	name of realm	Execute get the supported identity type in realm Commandline interface.	
AMCLI-2492	INFO	Unable to get the supported identity type in realm.	name of realm error message	Execute get the supported identity type in realm Commandline interface.	Look under debug file for more information.
AMCLI-2500	INFO	Attempt to get the assignable services of an identity.	name of realm name of identity type name of identity	Execute get the assignable services of an identity Commandline interface.	
AMCLI-2501	INFO	Assignable services are returned.	name of realm name of identity type name of identity	Execute get the assignable services of an identity Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2502	INFO	Unable to get the assignable services of an identity.	name of realm name of identity type name of identity error message	Execute get the assignable services of an identity Commandline interface.	Look under debug file for more information.
AMCLI-2510	INFO	Attempt to get the assigned services of an identity.	name of realm name of identity type name of identity	Execute get the assigned services of an identity Commandline interface.	
AMCLI-2511	INFO	Assigned services are returned.	name of realm name of identity type name of identity	Execute get the assigned services of an identity Commandline interface.	
AMCLI-2512	INFO	Unable to get the assigned services of an identity.	name of realm name of identity type name of identity error message	Execute get the assigned services of an identity Commandline interface.	Look under debug file for more information.
AMCLI-2520	INFO	Attempt to get service attribute values of an identity.	name of realm name of identity type name of identity name of service	Execute get the service attribute values of an identity Commandline interface.	
AMCLI-2521	INFO	Service attribute values are returned.	name of realm name of identity type name of identity name of service	Execute get the service attribute values of an identity Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2522	INFO	Unable to get the service attribute values of an identity.	name of realm name of identity type name of identity name of service error message	Execute get the service attribute values of an identity Commandline interface.	Look under debug file for more information.
AMCLI-2530	INFO	Attempt to get attribute values of an identity.	name of realm name of identity type name of identity	Execute get the attribute values of an identity Commandline interface.	
AMCLI-2531	INFO	Attribute values are returned.	name of realm name of identity type name of identity	Execute get the attribute values of an identity Commandline interface.	
AMCLI-2532	INFO	Unable to get the attribute values of an identity.	name of realm name of identity type name of identity error message	Execute get the attribute values of an identity Commandline interface.	Look under debug file for more information.
AMCLI-2540	INFO	Attempt to get memberships of an identity.	name of realm name of identity type name of identity name of membership identity type	Execute get the memberships of an identity Commandline interface.	
AMCLI-2541	INFO	Memberships are returned.	name of realm name of identity type name of identity name of membership identity type	Execute get the memberships of an identity Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2542	INFO	Unable to get the memberships of an identity.	name of realm name of identity type name of identity name of membership identity type error message	Execute get the memberships of an identity Commandline interface.	Look under debug file for more information.
AMCLI-2550	INFO	Attempt to get members of an identity.	name of realm name of identity type name of identity name of membership identity type	Execute get the members of an identity Commandline interface.	
AMCLI-2551	INFO	Members are returned.	name of realm name of identity type name of identity name of membership identity type	Execute get the members of an identity Commandline interface.	
AMCLI-2552	INFO	Unable to get the members of an identity.	name of realm name of identity type name of identity name of membership identity type error message	Execute get the members of an identity Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2560	INFO	Attempt to determine if an identity is a member of another identity.	name of realm name of identity type name of identity name of member identity type name of member identity	Execute determine if an identity is a member of another identity Commandline interface.	
AMCLI-2561	INFO	Membership is determined.	name of realm name of identity type name of identity name of member identity type name of member identity	Execute determine if an identity is a member of another identity Commandline interface.	
AMCLI-2562	INFO	Unable to determine the membership of an identity of another.	name of realm name of identity type name of identity name of member identity type name of member identity error message	Execute determine if an identity is a member of another identity Commandline interface.	Look under debug file for more information.
AMCLI-2570	INFO	Attempt to determine if an identity is active.	name of realm name of identity type name of identity	Execute determine if an identity is active Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2571	INFO	Active status of identity is determined.	name of realm name of identity type name of identity	Execute determine if an identity is active Commandline interface.	
AMCLI-2572	INFO	Unable to determine if an identity is active.	name of realm name of identity type name of identity error message	Execute determine if an identity is a active Commandline interface.	Look under debug file for more information.
AMCLI-2580	INFO	Attempt to make an identity a member of another identity.	name of realm name of identity type name of identity name of member identity type name of member identity	Execute make an identity a member of another identity Commandline interface.	
AMCLI-2581	INFO	Membership is set.	name of realm name of identity type name of identity name of member identity type name of member identity	Execute make an identity a member of another identity Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2582	INFO	Unable to add member of an identity to another.	name of realm name of identity type name of identity name of member identity type name of member identity error message	Execute make an identity a member of another identity Commandline interface.	Look under debug file for more information.
AMCLI-2590	INFO	Attempt to remove membership an identity from another identity.	name of realm name of identity type name of identity name of member identity type name of member identity	Execute remove membership an identity from another identity Commandline interface.	
AMCLI-2591	INFO	Membership is removed.	name of realm name of identity type name of identity name of member identity type name of member identity	Execute remove membership an identity from another identity Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2592	INFO	Unable to remove membership of an identity.	name of realm name of identity type name of identity name of member identity type name of member identity error message	Execute remove membership an identity from another identity Commandline interface.	Look under debug file for more information.
AMCLI-2600	INFO	Attempt to assign service to an identity.	name of realm identity type name of identity name of service	Execute assign service to an identity Commandline interface.	
AMCLI-2601	INFO	Service is assigned to an identity.	name of realm identity type name of identity name of service	Execute assign service to an identity Commandline interface.	
AMCLI-2602	INFO	Unable to assign service to an identity.	name of realm identity type name of identity name of service error message	Execute assign service to an identity Commandline interface.	Look under debug file for more information.
AMCLI-2610	INFO	Attempt to unassign service from an identity.	name of realm identity type name of identity name of service	Execute unassign service from an identity Commandline interface.	
AMCLI-2611	INFO	Service is unassigned from an identity.	name of realm identity type name of identity name of service	Execute unassign service from an identity Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2612	INFO	Unable to unassign service to an identity.	name of realm identity type name of identity name of service error message	Execute unassign service from an identity Commandline interface.	Look under debug file for more information.
AMCLI-2620	INFO	Attempt to modify service attribute values of an identity.	name of realm identity type name of identity name of service	Execute modify service attribute values of an identity Commandline interface.	
AMCLI-2621	INFO	Service attribute values are modified.	name of realm identity type name of identity name of service	Execute modify service attribute values of an identity Commandline interface.	
AMCLI-2622	INFO	Unable to modify service attribute values of an identity.	name of realm identity type name of identity name of service error message	Execute modify service attribute values of an identity Commandline interface.	Look under debug file for more information.
AMCLI-2630	INFO	Attempt to set attribute values of an identity.	name of realm identity type name of identity	Execute set attribute values of an identity Commandline interface.	
AMCLI-2631	INFO	Attribute values are modified.	name of realm identity type name of identity	Execute set attribute values of an identity Commandline interface.	
AMCLI-2632	INFO	Unable to set attribute values of an identity.	name of realm identity type name of identity error message	Execute set attribute values of an identity Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2640	INFO	Attempt to get privileges of an identity.	name of realm identity type name of identity	Execute get privileges of an identity Commandline interface.	
AMCLI-2641	INFO	Privileges are returned.	name of realm identity type name of identity	Execute get privileges of an identity Commandline interface.	
AMCLI-2642	INFO	Unable to get privileges of an identity.	name of realm identity type name of identity error message	Execute get privileges of an identity Commandline interface.	Look under debug file for more information.
AMCLI-2650	INFO	Attempt to add privileges to an identity.	name of realm identity type name of identity	Execute add privileges to an identity Commandline interface.	
AMCLI-2651	INFO	Privileges are added.	name of realm identity type name of identity	Execute add privileges to an identity Commandline interface.	
AMCLI-2652	INFO	Unable to add privileges to an identity.	name of realm identity type name of identity error message	Execute add privileges to an identity Commandline interface.	Look under debug file for more information.
AMCLI-2660	INFO	Attempt to remove privileges from an identity.	name of realm identity type name of identity	Execute remove privileges from an identity Commandline interface.	
AMCLI-2661	INFO	Privileges are removed.	name of realm identity type name of identity	Execute remove privileges from an identity Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2662	INFO	Unable to remove privileges from an identity.	name of realm identity type name of identity error message	Execute remove privileges from an identity Commandline interface.	Look under debug file for more information.
AMCLI-2670	INFO	Attempt to set boolean values to attribute schema.	name of service schema type name of sub schema name of attribute schema	Execute set attribute schema boolean values Commandline interface.	
AMCLI-2671	INFO	Boolean values are set.	name of service schema type name of sub schema name of attribute schema	Execute set attribute schema boolean values Commandline interface.	
AMCLI-2672	INFO	Unable to set boolean values to attribute schema.	name of service schema type name of sub schema name of attribute schema error message	Execute set attribute schema boolean values Commandline interface.	Look under debug file for more information.
AMCLI-2680	INFO	Attempt to list authentication instances.	name of realm	Execute list authentication instances Commandline interface.	
AMCLI-2681	INFO	List authentication instances succeeded.	name of realm	Execute list authentication instances Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2682	INFO	Failed to list authentication instances.	name of realm	Execute list authentication instances Commandline interface.	Look under debug file for more information.
AMCLI-2690	INFO	Attempt to create authentication instance.	name of realm name of authentication instance type of authentication instance	Execute create authentication instance Commandline interface.	
AMCLI-2691	INFO	Authentication instance created.	name of realm name of authentication instance type of authentication instance	Execute create authentication instance Commandline interface.	
AMCLI-2692	INFO	Failed to create authentication instance.	name of realm name of authentication instance type of authentication instance	Execute create authentication instance Commandline interface.	Look under debug file for more information.
AMCLI-2700	INFO	Attempt to delete authentication instances.	name of realm name of authentication instances	Execute delete authentication instance Commandline interface.	
AMCLI-2701	INFO	Authentication instances are deleted.	name of realm name of authentication instances	Execute delete authentication instances Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2702	INFO	Failed to delete authentication instance.	name of realm name of authentication instances	Execute delete authentication instances Commandline interface.	Look under debug file for more information.
AMCLI-2710	INFO	Attempt to update authentication instance.	name of realm name of authentication instance	Execute update authentication instance Commandline interface.	
AMCLI-2711	INFO	Authentication instance is updated.	name of realm name of authentication instance	Execute update authentication instance Commandline interface.	
AMCLI-2712	INFO	Failed to update authentication instance.	name of realm name of authentication instance	Execute update authentication instance Commandline interface.	Look under debug file for more information.
AMCLI-2710	INFO	Attempt to get authentication instance.	name of realm name of authentication instance	Execute get authentication instance Commandline interface.	
AMCLI-2711	INFO	Authentication instance profile is displayed.	name of realm name of authentication instance	Execute get authentication instance Commandline interface.	
AMCLI-2712	INFO	Failed to get authentication instance.	name of realm name of authentication instance	Execute get authentication instance Commandline interface.	Look under debug file for more information.
AMCLI-2720	INFO	Attempt to list authentication configurations.	name of realm	Execute list authentication configurations Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2721	INFO	List authentication configurations succeeded.	name of realm	Execute list authentication configurations Commandline interface.	
AMCLI-2722	INFO	Failed to list authentication configurations.	name of realm	Execute list authentication configurations Commandline interface.	Look under debug file for more information.
AMCLI-2730	INFO	Attempt to create authentication configuration.	name of realm name of authentication configuration	Execute create authentication configuration Commandline interface.	
AMCLI-2731	INFO	Authentication configuration created.	name of realm name of authentication configuration	Execute create authentication configuration Commandline interface.	
AMCLI-2732	INFO	Failed to create authentication configuration.	name of realm name of authentication configuration	Execute create authentication configuration Commandline interface.	Look under debug file for more information.
AMCLI-2740	INFO	Attempt to delete authentication configurations.	name of realm name of authentication configurations	Execute delete authentication configurations Commandline interface.	
AMCLI-2741	INFO	Authentication configurations are deleted.	name of realm name of authentication configurations	Execute delete authentication configurations Commandline interface.	
AMCLI-2742	INFO	Failed to delete authentication instance.	name of realm name of authentication configurations	Execute delete authentication configurations Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2750	INFO	Attempt to get authentication configuration entries.	name of realm name of authentication configuration	Execute get authentication configuration entries Commandline interface.	
AMCLI-2751	INFO	Authentication instance configuration entries are displayed.	name of realm name of authentication configuration	Execute get authentication configuration entries Commandline interface.	
AMCLI-2752	INFO	Failed to get authentication configuration entries.	name of realm name of authentication configuration	Execute get authentication configuration entries Commandline interface.	Look under debug file for more information.
AMCLI-2760	INFO	Attempt to set authentication configuration entries.	name of realm name of authentication configuration	Execute set authentication configuration entries Commandline interface.	
AMCLI-2761	INFO	Authentication instance configuration entries are displayed.	name of realm name of authentication configuration	Execute set authentication configuration entries Commandline interface.	
AMCLI-2762	INFO	Failed to set authentication configuration entries.	name of realm name of authentication configuration	Execute set authentication configuration entries Commandline interface.	Look under debug file for more information.
AMCLI-2770	INFO	Attempt to list datastores.	name of realm	Execute list datastores Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2771	INFO	List datastores succeeded.	name of realm	Execute list datastores Commandline interface.	
AMCLI-2772	INFO	Failed to list datastores.	name of realm error message	Execute list datastores Commandline interface.	Look under debug file for more information.
AMCLI-2780	INFO	Attemp to create datastore.	name of realm name of datastore type of datastore	Execute create datastore Commandline interface.	
AMCLI-2781	INFO	Create datastore succeeded.	name of realm name of datastore type of datastore	Execute create datastore Commandline interface.	
AMCLI-2782	INFO	Failed to create datastore.	name of realm name of datastore type of datastore	Execute create datastore Commandline interface.	Look under debug file for more information.
AMCLI-2790	INFO	Attempt to delete datastores.	name of realm names of datastore	Execute delete datastores Commandline interface.	
AMCLI-2791	INFO	Delete datastores succeeded.	name of realm names of datastore	Execute delete datastores Commandline interface.	
AMCLI-2792	INFO	Failed to delete datastores.	name of realm names of datastore	Execute delete datastore Commandline interface.	Look under debug file for more information.
AMCLI-2800	INFO	Attempt to update datastore profile.	name of realm name of datastore	Execute update datastore Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-2801	INFO	Update datastore succeeded.	name of realm name of datastore	Execute update datastore Commandline interface.	
AMCLI-2802	INFO	Failed to update datastore.	name of realm name of datastore error message	Execute update datastore Commandline interface.	Look under debug file for more information.
AMCLI-2900	INFO	Attempt to import service management configuration data.	name of file	Execute export configuration data Commandline interface.	
AMCLI-2901	INFO	Import service management configuration data succeeded.	name of file	Execute export configuration data Commandline interface.	
AMCLI-2902	INFO	Failed to import service management configuration data.	name of file error message	Execute export configuration data Commandline interface.	Look under debug file for more information.
AMCLI-3000	INFO	Attempt to export service management configuration data.	name of file	Execute export configuration data Commandline interface.	
AMCLI-3001	INFO	Export service management configuration data succeeded.	name of file	Execute export configuration data Commandline interface.	
AMCLI-3002	INFO	Failed to export service management configuration data.	name of file error message	Execute export configuration data Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-3010	INFO	Attempt to create server configuration xml.	name of file	Execute create server configuration xml Commandline interface.	
AMCLI-3011	INFO	Create server configuration xml succeeded.	name of file	Execute create server configuration xml Commandline interface.	
AMCLI-3012	INFO	Failed to create server configuration xml.	name of file error message	Execute create server configuration xml Commandline interface.	Look under debug file for more information.
AMCLI-3020	INFO	Attempt to remove service attribute values of realm.	name of realm name of service	Execute remove service attribute values of realm Commandline interface.	
AMCLI-3021	INFO	Service attribute values of realm are removed.	name of realm name of service	Execute remove service attribute values of realm Commandline interface.	
AMCLI-3022	INFO	Unable to remove service attribute values of realm.	name of realm name of service error message	Execute remove service attribute values of realm Commandline interface.	Look under debug file for more information.
AMCLI-3030	INFO	Attempt to add service attribute values of realm.	name of realm name of service	Execute add service attribute values of realm Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-3031	INFO	Service attribute values of realm are added.	name of realm name of service	Execute add service attribute values of realm Commandline interface.	
AMCLI-3032	INFO	Unable to add service attribute values of realm.	name of realm name of service error message	Execute add service attribute values of realm Commandline interface.	Look under debug file for more information.
AMCLI-3040	INFO	Attempt to list server configuration.	name of server	Execute list server configuration Commandline interface.	
AMCLI-3041	INFO	Server configuration is displayed.	name of server	Execute list server configuration Commandline interface.	
AMCLI-3042	INFO	Unable to list server configuration.	name of server error message	Execute list server configuration Commandline interface.	Check if servername is correct. Look under debug file for more information.
AMCLI-3050	INFO	Attempt to update server configuration.	name of server	Execute update server configuration Commandline interface.	
AMCLI-3051	INFO	Server configuration is updated.	name of server	Execute update server configuration Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-3052	INFO	Unable to update server configuration.	name of server error message	Execute update server configuration Commandline interface.	Check if servername is correct. Look under debug file for more information.
AMCLI-3060	INFO	Attempt to remove server configuration.	name of server	Execute remove server configuration Commandline interface.	
AMCLI-3061	INFO	Server configuration is removed.	name of server	Execute remove server configuration Commandline interface.	
AMCLI-3062	INFO	Remove server configuration.	name of server error message	Execute remove server configuration Commandline interface.	Check if servername is correct. Look under debug file for more information.
AMCLI-3070	INFO	Attempt to create server.	name of server	Execute create server Commandline interface.	
AMCLI-3071	INFO	Server is created.	name of server	Execute create server Commandline interface.	
AMCLI-3072	INFO	Unable to create server.	name of server error message	Execute create server Commandline interface.	Look under debug file for more information.
AMCLI-3080	INFO	Attempt to delete server.	name of server	Execute delete server Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-3081	INFO	Server is deleted.	name of server	Execute delete server Commandline interface.	
AMCLI-3082	INFO	Unable to delete server.	name of server error message	Execute delete server Commandline interface.	Check the name of the server. Look under debug file for more information.
AMCLI-3090	INFO	Attempt to list servers.		Execute list servers Commandline interface.	
AMCLI-3091	INFO	Servers are displayed.		Execute list servers Commandline interface.	
AMCLI-3092	INFO	Unable to list servers.	error message	Execute list servers Commandline interface.	Look under debug file for more information.
AMCLI-3100	INFO	Attempt to create site.	name of site primary URL of site	Execute create site Commandline interface.	
AMCLI-3101	INFO	Site is created.	name of site primary URL of site	Execute create site Commandline interface.	
AMCLI-3102	INFO	Unable to create site.	name of site primary URL of site error message	Execute create site Commandline interface.	Look under debug file for more information.
AMCLI-3110	INFO	Attempt to list sites.		Execute list sites Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-3111	INFO	Sites are displayed.		Execute list sites Commandline interface.	
AMCLI-3112	INFO	Unable to list sites.	error message	Execute list sites Commandline interface.	Look under debug file for more information.
AMCLI-3120	INFO	Attempt to show site members.	name of site	Execute show site members Commandline interface.	
AMCLI-3121	INFO	Site members are displayed.	name of site	Execute show site members Commandline interface.	
AMCLI-3122	INFO	Unable to show site members.	name of site error message	Execute show site members Commandline interface.	Look under debug file for more information.
AMCLI-3130	INFO	Attempt to add members to site.	name of site	Execute add members to site Commandline interface.	
AMCLI-3131	INFO	Members are added to site.	name of site	Execute add members to site Commandline interface.	
AMCLI-3132	INFO	Unable to add members to site.	name of site error message	Execute add members to site Commandline interface.	Look under debug file for more information.
AMCLI-3140	INFO	Attempt to remove members from site.	name of site	Execute remove members from site Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-3141	INFO	Members are removed from site.	name of site	Execute remove members from site Commandline interface.	
AMCLI-3142	INFO	Unable to remove members from site.	name of site error message	Execute remove members from site Commandline interface.	Look under debug file for more information.
AMCLI-3150	INFO	Attempt to delete site.	name of site	Execute delete site Commandline interface.	
AMCLI-3151	INFO	Site is deleted.	name of site	Execute delete site Commandline interface.	
AMCLI-3152	INFO	Unable to delete members from site.	name of site error message	Execute delete site Commandline interface.	Look under debug file for more information.
AMCLI-3160	INFO	Attempt to set site primary URL.	name of site primary URL of site	Execute set site primary URL Commandline interface.	
AMCLI-3161	INFO	Site primary URL is set.	name of site primary URL of site	Execute set site primary URL Commandline interface.	
AMCLI-3162	INFO	Unable to set site primary URL.	name of site primary URL of site error message	Execute set site primary URL Commandline interface.	Look under debug file for more information.
AMCLI-3170	INFO	Attempt to show site profile.	name of site	Execute show site profile Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-3171	INFO	Site profile is displayed.	name of site	Execute show site profile Commandline interface.	
AMCLI-3172	INFO	Unable to show site profile.	name of site error message	Execute show site profile Commandline interface.	Look under debug file for more information.
AMCLI-3180	INFO	Attempt to set site failover URLs.	name of site	Execute set site failover URLs Commandline interface.	
AMCLI-3181	INFO	Site failover URLs are set.	name of site	Execute set site failover URLs Commandline interface.	
AMCLI-3182	INFO	Unable to set site failover URLs.	name of site error message	Execute set site failover URLs Commandline interface.	Look under debug file for more information.
AMCLI-3190	INFO	Attempt to add site failover URLs.	name of site	Execute add site failover URLs Commandline interface.	
AMCLI-3191	INFO	Site failover URLs are added.	name of site	Execute add site failover URLs Commandline interface.	
AMCLI-3192	INFO	Unable to add site failover URLs.	name of site error message	Execute add site failover URLs Commandline interface.	Look under debug file for more information.
AMCLI-3200	INFO	Attempt to remove site failover URLs.	name of site	Execute remove site failover URLs Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-3201	INFO	Site failover URLs are removed.	name of site	Execute remove site failover URLs Commandline interface.	
AMCLI-3202	INFO	Unable to remove site failover URLs.	name of site error message	Execute remove site failover URLs Commandline interface.	Look under debug file for more information.
AMCLI-3210	INFO	Attempt to clone server.	name of server name of cloned server	Execute clone server Commandline interface.	
AMCLI-3211	INFO	Server is cloned.	name of server name of cloned server	Execute clone server Commandline interface.	
AMCLI-3212	INFO	Unable to clone server.	name of server name of cloned server error message	Execute clone server Commandline interface.	Look under debug file for more information.
AMCLI-3220	INFO	Attempt to export server.	name of server	Execute export server Commandline interface.	
AMCLI-3221	INFO	Server is cloned.	name of server	Execute export server Commandline interface.	
AMCLI-3222	INFO	Unable to export server.	name of server error message	Execute export server Commandline interface.	Look under debug file for more information.
AMCLI-3230	INFO	Attempt to import server configuration.	name of server	Execute import server configuration Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-3231	INFO	Server configuration is imported.	name of server	Execute import server configuration Commandline interface.	
AMCLI-3232	INFO	Unable to import server configuration.	name of server error message	Execute import server configuration Commandline interface.	Look under debug file for more information.
AMCLI-5000	INFO	Attempt to get the supported data types.		Execute get the supported data type Commandline interface.	
AMCLI-5001	INFO	The supported data types are retrieved.		Execute add service attribute values Commandline interface.	
AMCLI-5002	INFO	Unable to get the supported data types.	error message	Execute get the supported data types Commandline interface.	Look under debug file for more information.
AMCLI-4000	INFO	Attempt to create an agent.	realm agent type name of agent	Execute create agent Commandline interface.	
AMCLI-4001	INFO	Agent is created.	realm agent type name of agent	Execute create agent Commandline interface.	
AMCLI-4002	INFO	Unable to create agent.	realm agent type name of agent error message	Execute create agent Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-4010	INFO	Attempt to delete agents.	name of realm name of agents	Execute delete agents Commandline interface.	
AMCLI-4011	INFO	Agents are deleted.	name of realm name of agents	Execute delete agents Commandline interface.	
AMCLI-4012	INFO	Unable to delete agents.	name of realm name of agents error message	Execute delete agents Commandline interface.	Look under debug file for more information.
AMCLI-4020	INFO	Attempt to set attribute values of an agent.	name of realm name of agent	Execute update agent Commandline interface.	
AMCLI-4021	INFO	Agent profile is modified.	name of realm name of agent	Execute update agent Commandline interface.	
AMCLI-4022	INFO	Unable to update an agent.	name of realm name of agent error message	Execute update agent Commandline interface.	Look under debug file for more information.
AMCLI-4030	INFO	Attempt to list agents.	name of realm agent type search pattern	Execute list agents Commandline interface.	
AMCLI-4031	INFO	Search Result is returned.	name of realm agent type search pattern	Execute list agents Commandline interface.	
AMCLI-4032	INFO	Unable to list agents.	name of realm agent type search pattern error message	Execute list agents Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-4040	INFO	Attempt to get attribute values of an agent.	name of realm name of agent	Execute get the attribute values of an agent Commandline interface.	
AMCLI-4041	INFO	Attribute values are returned.	name of realm name of agent	Execute get the attribute values of an agent Commandline interface.	
AMCLI-4042	INFO	Unable to get the attribute values of an agent.	name of realm name of agent error message	Execute get the attribute values of an agent Commandline interface.	Look under debug file for more information.
AMCLI-4050	INFO	Attempt to create an agent group.	realm agent type name of agent group	Execute create agent group Commandline interface.	
AMCLI-4051	INFO	Agent group is created.	realm agent type name of agent group	Execute create agent group Commandline interface.	
AMCLI-4052	INFO	Unable to create agent group.	realm agent type name of agent group error message	Execute create agent group Commandline interface.	Look under debug file for more information.
AMCLI-4060	INFO	Attempt to delete agent groups.	name of realm name of agent groups	Execute delete agent groups Commandline interface.	
AMCLI-4061	INFO	Agent groups are deleted.	name of realm name of agent groups	Execute delete agent groups Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-4062	INFO	Unable to delete agent groups.	name of realm name of agent groups error message	Execute delete agent groups Commandline interface.	Look under debug file for more information.
AMCLI-4070	INFO	Attempt to list agent groups.	name of realm agent type search pattern	Execute list agent groups Commandline interface.	
AMCLI-4071	INFO	Search Result is returned.	name of realm agent type search pattern	Execute list agent groups Commandline interface.	
AMCLI-4072	INFO	Unable to list agent groups.	name of realm agent type search pattern error message	Execute list agent groups Commandline interface.	Look under debug file for more information.
AMCLI-4080	INFO	Attempt to add agent to group.	name of realm name of agent group name of agent	Execute add agents to group Commandline interface.	
AMCLI-4081	INFO	Agent is added to group.	name of realm name of agent group name of agent	Execute add agent to group Commandline interface.	
AMCLI-4082	INFO	Unable to add agent to group.	name of realm name of agent group name of agent error message	Execute add agent to group Commandline interface.	Look under debug file for more information.
AMCLI-4090	INFO	Attempt to remove agent from group.	name of realm name of agent group name of agent	Execute remove agent from group Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-4091	INFO	Agent is removed to group.	name of realm name of agent group name of agent	Execute remove agent from group Commandline interface.	
AMCLI-4092	INFO	Unable to remove agent from group.	name of realm name of agent group name of agent error message	Execute remove agent from group Commandline interface.	Look under debug file for more information.
AMCLI-4100	INFO	Attempt to set agent password.	realm name of agent	Execute set agent password Commandline interface.	
AMCLI-4101	INFO	Agent password is modified.	realm name of agent	Execute set agent password Commandline interface.	
AMCLI-4102	INFO	Unable to set agent password.	realm name of agent error message	Execute set agent password Commandline interface.	Look under debug file for more information.
AMCLI-4110	INFO	Attempt to get attribute values of an agent group.	name of realm name of agent group	Execute get the attribute values of an agent group Commandline interface.	
AMCLI-4111	INFO	Attribute values are returned.	name of realm name of agent group	Execute get the attribute values of an agent group Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-4112	INFO	Unable to get the attribute values of an agent group.	name of realm name of agent group error message	Execute get the attribute values of an agent group Commandline interface.	Look under debug file for more information.
AMCLI-4120	INFO	Attempt to set attribute values of an agent group.	name of realm name of agent group	Execute update agent group Commandline interface.	
AMCLI-4121	INFO	Agent group profile is modified.	name of realm name of agent group	Execute update agent group Commandline interface.	
AMCLI-4122	INFO	Unable to update an agent.	name of realm name of agent group error message	Execute update agent group Commandline interface.	Look under debug file for more information.
AMCLI-4130	INFO	Attempt to show supported agent types.		Execute show supported agent types Commandline interface.	
AMCLI-4131	INFO	Supported agent types is displayed.		Execute show supported agent types Commandline interface.	
AMCLI-4132	INFO	Unable to show supported agent types.	error message	Execute show supported agent types Commandline interface.	Look under debug file for more information.
AMCLI-4140	INFO	Attempt to show agent group members.	name of realm name of agent group	Execute show agent group members Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-4141	INFO	Agent group's members are displayed.	name of realm name of agent group	Execute show agent group members Commandline interface.	
AMCLI-4142	INFO	Unable to show agent group members.	name of realm name of agent group error message	Execute show agent group members Commandline interface.	Look under debug file for more information.
AMCLI-4150	INFO	Attempt to show agent's membership.	name of realm name of agent	Execute show agent's membership Commandline interface.	
AMCLI-4151	INFO	Agent's membership are displayed.	name of realm name of agent	Execute show agent's membership Commandline interface.	
AMCLI-4152	INFO	Unable to show agent's membership.	name of realm name of agent error message	Execute show agent's membership Commandline interface.	Look under debug file for more information.
AMCLI-4500	INFO	Attempt to register authentication module.	name of service	Execute register authentication module Commandline interface.	
AMCLI-4501	INFO	Authentication module is registered.	name of service	Execute register authentication module Commandline interface.	
AMCLI-4502	INFO	Unable to register authentication module.	name of service error message	Execute register authentication module Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-4510	INFO	Attempt to unregister authentication module.	name of service	Execute unregister authentication module Commandline interface.	
AMCLI-4511	INFO	Authentication module is unregistered.	name of service	Execute unregister authentication module Commandline interface.	
AMCLI-4512	INFO	Unable to unregister authentication module.	name of service error message	Execute unregister authentication module Commandline interface.	Look under debug file for more information.
AMCLI-4515	INFO	Attempt to get supported authentication modules in the system.		Execute get supported authentication modules in the system Commandline interface.	
AMCLI-4516	INFO	Supported authentication modules in the system are displayed.		Execute get supported authentication modules in the system module Commandline interface.	
AMCLI-4517	INFO	Failed to get supported authentication modules in the system.	error message	Execute get supported authentication modules in the system Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-4520	INFO	Attempt to remove property values of an agent.	name of realm name of agent property names	Execute remove property values of an agent Commandline interface.	
AMCLI-4521	INFO	Property values are removed.	name of realm name of agent property names	Execute remove property values of an agent Commandline interface.	
AMCLI-4522	INFO	Unable to remove property values of an agent.	name of realm name of agent property names error message	Execute remove property values of an agent Commandline interface.	Look under debug file for more information.
AMCLI-4600	INFO	Attempt to get server configuration XML.	name of server	Execute get server configuration XML Commandline interface.	
AMCLI-4601	INFO	Server configuration XML is displayed.	name of server	Execute get server configuration XML Commandline interface.	
AMCLI-4602	INFO	Unable to get server configuration XML.	name of server error message	Execute get server configuration XML Commandline interface.	Check if servername is correct. Look under debug file for more information.
AMCLI-4610	INFO	Attempt to set server configuration XML.	name of server	Execute set server configuration XML Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-4611	INFO	Server configuration XML is set.	name of server	Execute set server configuration XML Commandline interface.	
AMCLI-4612	INFO	Unable to set server configuration XML.	name of server error message	Execute set server configuration XML Commandline interface.	Check if servername is correct. Look under debug file for more information.
AMCLI-4700	INFO	Attempt to list supported datastore types.		Execute list supported datastore types Commandline interface.	
AMCLI-4701	INFO	List supported datastore types succeeded.		Execute list supported datastore types Commandline interface.	
AMCLI-4702	INFO	Failed to list supported datastore types.	error message	Execute list supported datastore types Commandline interface.	Look under debug file for more information.
AMCLI-5000	INFO	Attempt to create bootstrap URL.		Execute generate bootstrap URL Commandline interface.	
AMCLI-5001	INFO	Generate bootstrap URL succeeded.		Execute generate bootstrap URL Commandline interface.	

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-5002	INFO	Failed to generate bootstrap URL.	error message	Execute generate bootstrap URL Commandline interface.	Look under debug file for more information.
AMCLI-4800	INFO	Attempt to add authentication configuration entry.	name of realm name of authentication configuration name of module	Execute add authentication configuration entry Commandline interface.	
AMCLI-4801	INFO	Authentication instance configuration entry is created.	name of realm name of authentication configuration name of module	Execute add authentication configuration entry Commandline interface.	
AMCLI-4802	INFO	Failed to add authentication configuration entry.	name of realm name of authentication configuration name of module error message	Execute add authentication configuration entry Commandline interface.	Look under debug file for more information.
AMCLI-5000	INFO	Attempt to show datastore profile.	name of realm name of datastore	Execute show datastore Commandline interface.	
AMCLI-5001	INFO	Show datastore succeeded.	name of realm name of datastore	Execute show datastore Commandline interface.	
AMCLI-5002	INFO	Failed to show datastore profile.	name of realm name of datastore error message	Execute show datastore Commandline interface.	Look under debug file for more information.

TABLE 10–3 Log Reference Document for CLILogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
AMCLI-5100	INFO	Add AMSDK IdRepo Plugin.	name of datastore name	Execute add AMSDK IdRepo Plugin Commandline interface.	
AMCLI-5101	INFO	AMSDK plugin is added.	name of datastore name	Execute add AMSDK IdRepo Plugin Commandline interface.	
AMCLI-5102	INFO	Failed to add AMSDK IdRepo Plugin.	name of datastore name error message	Execute add AMSDK IdRepo Plugin Commandline interface.	Look under debug file for more information.

Console

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-1	INFO	Attempt to create Identity	identity name identity type realm name	Click on create button in Realm Creation Page.	
CONSOLE-2	INFO	Creation of Identity succeeded.	identity name identity type realm name	Click on create button in Realm Creation Page.	
CONSOLE-3	SEVERE	Creation of Identity failed	identity name identity type realm name error message	Unable to create an identity under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-4	SEVERE	Creation of Identity failed	identity name identity type realm name error message	Unable to create an identity under a realm due to data store error.	Look under data store log for more information.
CONSOLE-11	INFO	Attempt to search for Identities	base realm identity type search pattern search size limit search time limit	Click on Search button in identity search view.	
CONSOLE-12	INFO	Searching for Identities succeeded	base realm identity type search pattern search size limit search time limit	Click on Search button in identity search view.	
CONSOLE-13	SEVERE	Searching for identities failed	identity name identity type realm name error message	Unable to perform search operation on identities under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-14	SEVERE	Searching for identities failed	identity name identity type realm name error message	Unable to perform search operation on identities under a realm due to data store error.	Look under data store log for more information.
CONSOLE-21	INFO	Attempt to read attribute values of an identity	identity name name of attributes	View identity profile view.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-22	INFO	Reading of attribute values of an identity succeeded	identity name name of attributes	View identity profile view.	
CONSOLE-23	SEVERE	Reading of attribute values of an identity failed	identity name name of attributes error message	Unable to read attribute values of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-24	SEVERE	Reading of attribute values of an identity failed	identity name name of attributes error message	Unable to read attribute values of an identity due to data store error.	Look under data store log for more information.
CONSOLE-25	SEVERE	Reading of attribute values of an identity failed	identity name name of attributes error message	Unable to read attribute values of an identity due to exception service manager API.	Look under service manage log for more information.
CONSOLE-31	INFO	Attempt to modify attribute values of an identity	identity name name of attributes	Click on Save button in identity profile view.	
CONSOLE-32	INFO	Modification of attribute values of an identity succeeded	identity name name of attributes	Click on Save button in identity profile view.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-33	SEVERE	Modification of attribute values of an identity failed	identity name name of attributes error message	Unable to modify attribute values of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-34	SEVERE	Modification of attribute values of an identity failed	identity name name of attributes error message	Unable to modify attribute values of an identity due to data store error.	Look under data store log for more information.
CONSOLE-41	INFO	Attempt to delete identities	realm name name of identities to be deleted	Click on Delete button in identity search view.	
CONSOLE-42	INFO	Deletion of identities succeeded	realm name name of identities to be deleted	Click on Delete button in identity search view.	
CONSOLE-43	SEVERE	Deletion of identities failed	realm name name of identities to be deleted error message	Unable to delete identities. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-44	SEVERE	Deletion of identities failed	realm name name of identities to be deleted error message	Unable to delete identities due to data store error.	Look under data store log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-51	INFO	Attempt to read identity's memberships information	name of identity membership identity type	View membership page of an identity.	
CONSOLE-52	INFO	Reading of identity's memberships information succeeded	name of identity membership identity type	View membership page of an identity.	
CONSOLE-53	SEVERE	Reading of identity's memberships information failed.	name of identity membership identity type error message	Unable to read identity's memberships information. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-54	SEVERE	Reading of identity's memberships information failed.	name of identity membership identity type error message	Unable to read identity's memberships information due to data store error.	Look under data store log for more information.
CONSOLE-61	INFO	Attempt to read identity's members information	name of identity members identity type	View members page of an identity.	
CONSOLE-62	INFO	Reading of identity's members information succeeded	name of identity members identity type	View members page of an identity.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-63	SEVERE	Reading of identity's members information failed.	name of identity member identity type error message	Unable to read identity's members information. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-64	SEVERE	Reading of identity's members information failed.	name of identity member identity type error message	Unable to read identity's members information due to data store error.	Look under data store log for more information.
CONSOLE-71	INFO	Attempt to add member to an identity	name of identity name of identity to be added.	Select members to be added to an identity.	
CONSOLE-72	INFO	Addition of member to an identity succeeded	name of identity name of identity added.	Select members to be added to an identity.	
CONSOLE-73	SEVERE	Addition of member to an identity failed.	name of identity name of identity to be added. error message	Unable to add member to an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-74	SEVERE	Addition of member to an identity failed.	name of identity name of identity to be added. error message	Unable to add member to an identity due to data store error.	Look under data store log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-81	INFO	Attempt to remove member from an identity	name of identity name of identity to be removed.	Select members to be removed from an identity.	
CONSOLE-82	INFO	Removal of member from an identity succeeded	name of identity name of identity removed.	Select members to be removed from an identity.	
CONSOLE-83	SEVERE	Removal of member to an identity failed.	name of identity name of identity to be removed. error message	Unable to remove member from an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-84	SEVERE	Removal of member from an identity failed.	name of identity name of identity to be removed. error message	Unable to remove member to an identity due to data store error.	Look under data store log for more information.
CONSOLE-91	INFO	Attempt to read assigned service names of an identity	name of identity	Click on Add button in service assignment view of an identity.	
CONSOLE-92	INFO	Reading assigned service names of an identity succeeded	name of identity	Click on Add button in service assignment view of an identity.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-93	SEVERE	Reading assigned service names of an identity failed.	name of identity error message	Unable to read assigned service names of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-94	SEVERE	Reading assigned service names of an identity failed.	name of identity error message	Unable to read assigned service names of an identity due to data store error.	Look under data store log for more information.
CONSOLE-101	INFO	Attempt to read assignable service names of an identity	name of identity	View the services page of an identity.	
CONSOLE-102	INFO	Reading assignable service names of an identity succeeded	name of identity	View the services page of an identity.	
CONSOLE-103	SEVERE	Reading assignable service names of an identity failed.	name of identity error message	Unable to read assignable service names of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-104	SEVERE	Reading assignable service names of an identity failed.	name of identity error message	Unable to read assignable service names of an identity due to data store error.	Look under data store log for more information.
CONSOLE-111	INFO	Attempt to assign a service to an identity	name of identity name of service	Click Add button of service view of an identity.	
CONSOLE-112	INFO	Assignment of service to an identity succeeded	name of identity name of service	Click Add button of service view of an identity.	
CONSOLE-113	SEVERE	Assignment of service to an identity failed.	name of identity name of service error message	Unable to assign service to an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-114	SEVERE	Assignment of service to an identity failed.	name of identity name of service error message	Unable to assign service to an identity due to data store error.	Look under data store log for more information.
CONSOLE-121	INFO	Attempt to unassign a service from an identity	name of identity name of service	Click Remove button in service view of an identity.	
CONSOLE-122	INFO	Unassignment of service to an identity succeeded	name of identity name of service	Click Remove button in service view of an identity.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-123	SEVERE	Unassignment of service from an identity failed.	name of identity name of service error message	Unable to unassign service from an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-124	SEVERE	Unassignment of service from an identity failed.	name of identity name of service error message	Unable to unassign service from an identity due to data store error.	Look under data store log for more information.
CONSOLE-131	INFO	Attempt to read service attribute values of an identity	name of identity name of service	View service profile view of an identity.	
CONSOLE-132	INFO	Reading of service attribute values of an identity succeeded	name of identity name of service	View service profile view of an identity.	
CONSOLE-133	SEVERE	Reading of service attribute values of an identity failed.	name of identity name of service error message	Unable to read service attribute values of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation	Look under data store log for more information.
CONSOLE-134	SEVERE	Reading of service attribute values of an identity failed.	name of identity name of service error message	Unable to read service attribute values of an identity due to data store error.	Look under data store log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-141	INFO	Attempt to write service attribute values to an identity	name of identity name of service	Click on Save button in service profile view of an identity.	
CONSOLE-142	INFO	Writing of service attribute values to an identity succeeded	name of identity name of service	Click on Save button in service profile view of an identity.	
CONSOLE-143	SEVERE	Writing of service attribute values to an identity failed.	name of identity name of service error message	Unable to write service attribute values to an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-144	SEVERE	Writing of service attribute values to an identity failed.	name of identity name of service error message	Unable to write service attribute values to an identity due to data store error.	Look under data store log for more information.
CONSOLE-201	INFO	Attempt to read all global service default attribute values	name of service	View global configuration view of a service.	
CONSOLE-202	INFO	Reading of all global service default attribute values succeeded	name of service	View global configuration view of a service.	
CONSOLE-203	INFO	Attempt to read global service default attribute values	name of service name of attribute	View global configuration view of a service.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-204	INFO	Reading of global service default attribute values succeeded	name of service name of attribute	View global configuration view of a service.	
CONSOLE-205	INFO	Reading of global service default attribute values failed	name of service name of attribute	View global configuration view of a service.	Look under service management log for more information.
CONSOLE-211	INFO	Attempt to write global service default attribute values	name of service name of attribute	Click on Save button in global configuration view of a service.	
CONSOLE-212	INFO	Writing of global service default attribute values succeeded	name of service name of attribute	Click on Save button in global configuration view of a service.	
CONSOLE-213	SEVERE	Writing of global service default attribute values failed.	name of service name of attribute error message	Unable to write global service default attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-214	SEVERE	Writing of global service default attribute values failed.	name of service name of attribute error message	Unable to write service default attribute values due to service management error.	Look under service management log for more information.
CONSOLE-221	INFO	Attempt to get sub configuration names	name of service name of base global sub configuration	View a global service view of which its service has sub schema.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-222	INFO	Reading of global sub configuration names succeeded	name of service name of base global sub configuration	View a global service view of which its service has sub schema.	
CONSOLE-223	SEVERE	Reading of global sub configuration names failed.	name of service name of base global sub configuration error message	Unable to get global sub configuration names. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-224	SEVERE	Reading of global sub configuration names failed.	name of service name of base global sub configuration error message	Unable to get global sub configuration names due to service management error.	Look under service management log for more information.
CONSOLE-231	INFO	Attempt to delete sub configuration	name of service name of base global sub configuration name of sub configuration to be deleted	Click on delete selected button in global service profile view.	
CONSOLE-232	INFO	Deletion of sub configuration succeeded	name of service name of base global sub configuration name of sub configuration to be deleted	Click on delete selected button in global service profile view.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-233	SEVERE	Deletion of sub configuration failed.	name of service name of base global sub configuration name of sub configuration to be deleted error message	Unable to delete sub configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-234	SEVERE	Deletion of sub configuration failed.	name of service name of base global sub configuration name of sub configuration to be deleted error message	Unable to delete sub configuration due to service management error.	Look under service management log for more information.
CONSOLE-241	INFO	Attempt to create sub configuration	name of service name of base global sub configuration name of sub configuration to be created name of sub schema to be created	Click on add button in create sub configuration view.	
CONSOLE-242	INFO	Creation of sub configuration succeeded	name of service name of base global sub configuration name of sub configuration to be created name of sub schema to be created	Click on add button in create sub configuration view.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-243	SEVERE	Creation of sub configuration failed.	name of service name of base global sub configuration name of sub configuration to be created name of sub schema to be created error message	Unable to create sub configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-244	SEVERE	Creation of sub configuration failed.	name of service name of base global sub configuration name of sub configuration to be created name of sub schema to be created error message	Unable to create sub configuration due to service management error.	Look under service management log for more information.
CONSOLE-251	INFO	Reading of sub configuration's attribute values succeeded	name of service name of sub configuration	View sub configuration profile view.	
CONSOLE-261	INFO	Attempt to write sub configuration's attribute values	name of service name of sub configuration	Click on save button in sub configuration profile view.	
CONSOLE-262	INFO	Writing of sub configuration's attribute values succeeded	name of service name of sub configuration	Click on save button in sub configuration profile view.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-263	SEVERE	Writing of sub configuration's attribute value failed.	name of service name of sub configuration error message	Unable to write sub configuration's attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-264	SEVERE	Writing of sub configuration's attribute value failed.	name of service name of sub configuration error message	Unable to write sub configuration's attribute value due to service management error.	Look under service management log for more information.
CONSOLE-301	INFO	Attempt to get policy names under a realm.	name of realm	View policy main page.	
CONSOLE-302	INFO	Getting policy names under a realm succeeded	name of realm	View policy main page.	
CONSOLE-303	SEVERE	Getting policy names under a realm failed.	name of realm error message	Unable to get policy names under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under policy log for more information.
CONSOLE-304	SEVERE	Getting policy names under a realm failed.	name of realm error message	Unable to get policy names under a realm due to policy SDK related errors.	Look under policy log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-311	INFO	Attempt to create policy under a realm.	name of realm name of policy	Click on New button in policy creation page.	
CONSOLE-312	INFO	Creation of policy succeeded	name of realm name of policy	Click on New button in policy creation page.	
CONSOLE-313	SEVERE	Creation of policy failed.	name of realm name of policy error message	Unable to create policy under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under policy log for more information.
CONSOLE-314	SEVERE	Creation of policy failed.	name of realm name of policy error message	Unable to create policy under a realm due to policy SDK related errors.	Look under policy log for more information.
CONSOLE-321	INFO	Attempt to modify policy.	name of realm name of policy	Click on Save button in policy profile page.	
CONSOLE-322	INFO	Modification of policy succeeded	name of realm name of policy	Click on Save button in policy profile page.	
CONSOLE-323	SEVERE	Modification of policy failed.	name of realm name of policy error message	Unable to modify policy under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under policy log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-324	SEVERE	Modification of policy failed.	name of realm name of policy error message	Unable to modify policy due to policy SDK related errors.	Look under policy log for more information.
CONSOLE-331	INFO	Attempt to delete policy.	name of realm names of policies	Click on Delete button in policy main page.	
CONSOLE-332	INFO	Deletion of policy succeeded	name of realm name of policies	Click on Delete button in policy main page.	
CONSOLE-333	SEVERE	Deletion of policy failed.	name of realm name of policies error message	Unable to delete policy. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under policy log for more information.
CONSOLE-334	SEVERE	Deletion of policy failed.	name of realm name of policies error message	Unable to delete policy due to policy SDK related errors.	Look under policy log for more information.
CONSOLE-401	INFO	Attempt to get realm names	name of parent realm	View realm main page.	
CONSOLE-402	INFO	Getting realm names succeeded.	name of parent realm	View realm main page.	
CONSOLE-403	SEVERE	Getting realm names failed.	name of parent realm error message	Unable to get realm names due to service management SDK exception.	Look under service management log for more information.
CONSOLE-411	INFO	Attempt to create realm	name of parent realm name of new realm	Click on New button in create realm page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-412	INFO	Creation of realm succeeded.	name of parent realm name of new realm	Click on New button in create realm page.	
CONSOLE-413	SEVERE	Creation of realm failed.	name of parent realm name of new realm error message	Unable to create new realm due to service management SDK exception.	Look under service management log for more information.
CONSOLE-421	INFO	Attempt to delete realm	name of parent realm name of realm to delete	Click on Delete button in realm main page.	
CONSOLE-422	INFO	Deletion of realm succeeded.	name of parent realm name of realm to delete	Click on Delete button in realm main page.	
CONSOLE-423	SEVERE	Deletion of realm failed.	name of parent realm name of realm to delete error message	Unable to delete realm due to service management SDK exception.	Look under service management log for more information.
CONSOLE-431	INFO	Attempt to get attribute values of realm	name of realm	View realm profile page.	
CONSOLE-432	INFO	Getting attribute values of realm succeeded.	name of realm	View realm profile page.	
CONSOLE-433	SEVERE	Getting attribute values of realm failed.	name of realm error message	Unable to get attribute values of realm due to service management SDK exception.	Look under service management log for more information.
CONSOLE-441	INFO	Attempt to modify realm's profile	name of realm	Click on Save button in realm profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-442	INFO	Modification of realm's profile succeeded.	name of realm	Click on Save button in realm profile page.	
CONSOLE-443	SEVERE	Modification of realm's profile failed.	name of realm error message	Unable to modify realm's profile due to service management SDK exception.	Look under service management log for more information.
CONSOLE-501	INFO	Attempt to get delegation subjects under a realm	name of realm search pattern	View delegation main page.	
CONSOLE-502	INFO	Getting delegation subjects under a realm succeeded.	name of realm search pattern	View delegation main page.	
CONSOLE-503	SEVERE	Getting delegation subjects under a realm failed.	name of realm search pattern error message	Unable to get delegation subjects. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under delegation management log for more information.
CONSOLE-504	SEVERE	Getting delegation subjects under a realm failed.	name of realm search pattern error message	Unable to get delegation subjects due to delegation management SDK related errors.	Look under delegation management log for more information.
CONSOLE-511	INFO	Attempt to get privileges of delegation subject	name of realm ID of delegation subject	View delegation subject profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-512	INFO	Getting privileges of delegation subject succeeded.	name of realm ID of delegation subject	View delegation subject profile page.	
CONSOLE-513	SEVERE	Getting privileges of delegation subject failed.	name of realm ID of delegation subject error message	Unable to get privileges of delegation subject. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under delegation management log for more information.
CONSOLE-514	SEVERE	Getting privileges of delegation subject failed.	name of realm ID of delegation subject error message	Unable to get privileges of delegation subject due to delegation management SDK related errors.	Look under delegation management log for more information.
CONSOLE-521	INFO	Attempt to modify delegation privilege	name of realm ID of delegation privilege ID of subject	Click on Save button in delegation subject profile page.	
CONSOLE-522	INFO	Modification of delegation privilege succeeded.	name of realm ID of delegation privilege ID of subject	Click on Save button in delegation subject profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-523	SEVERE	Modification of delegation privilege failed.	name of realm ID of delegation privilege ID of subject error message	Unable to modify delegation privilege. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under delegation management log for more information.
CONSOLE-524	SEVERE	Modification of delegation privilege failed.	name of realm ID of delegation privilege ID of subject error message	Unable to modify delegation privilege due to delegation management SDK related errors.	Look under delegation management log for more information.
CONSOLE-601	INFO	Attempt to get data store names	name of realm	View data store main page.	
CONSOLE-602	INFO	Getting data store names succeeded.	name of realm	View data store main page.	
CONSOLE-603	SEVERE	Getting data store names failed.	name of realm error message	Unable to get data store names. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-604	SEVERE	Getting data store names failed.	name of realm error message	Unable to get data store names due to service management SDK exception.	Look under service management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-611	INFO	Attempt to get attribute values of identity repository	name of realm name of identity repository	View data store profile page.	
CONSOLE-612	INFO	Getting attribute values of data store succeeded.	name of realm name of identity repository	View data store profile page.	
CONSOLE-613	SEVERE	Getting attribute values of data store failed.	name of realm name of identity repository error message	Unable to get attribute values of identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-614	SEVERE	Getting attribute values of data store failed.	name of realm name of identity repository error message	Unable to get attribute values of data store due to service management SDK exception.	Look under service management log for more information.
CONSOLE-621	INFO	Attempt to create identity repository	name of realm name of identity repository type of identity repository	Click on New button in data store creation page.	
CONSOLE-622	INFO	Creation of data store succeeded.	name of realm name of identity repository type of identity repository	Click on New button in data store creation page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-623	SEVERE	Creation of data store failed.	name of realm name of identity repository type of identity repository error message	Unable to create identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-624	SEVERE	Creation data store failed.	name of realm name of identity repository type of identity repository error message	Unable to create data store due to service management SDK exception.	Look under service management log for more information.
CONSOLE-631	INFO	Attempt to delete identity repository	name of realm name of identity repository	Click on Delete button in data store main page.	
CONSOLE-632	INFO	Deletion of data store succeeded.	name of realm name of identity repository	Click on Delete button in data store main page.	
CONSOLE-633	SEVERE	Deletion of data store failed.	name of realm name of identity repository error message	Unable to delete identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-634	SEVERE	Deletion data store failed.	name of realm name of identity repository error message	Unable to delete data store due to service management SDK exception.	Look under service management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-641	INFO	Attempt to modify identity repository	name of realm name of identity repository	Click on Save button in data store profile page.	
CONSOLE-642	INFO	Modification of data store succeeded.	name of realm name of identity repository	Click on Save button in data store profile page.	
CONSOLE-643	SEVERE	Modification of data store failed.	name of realm name of identity repository error message	Unable to modify identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-644	SEVERE	Modification data store failed.	name of realm name of identity repository error message	Unable to modify data store due to service management SDK exception.	Look under service management log for more information.
CONSOLE-701	INFO	Attempt to get assigned services of realm	name of realm	View realm's service main page.	
CONSOLE-702	INFO	Getting assigned services of realm succeeded.	name of realm	View realm's service main page.	
CONSOLE-703	SEVERE	Getting assigned services of realm failed.	name of realm error message	Unable to get assigned services of realm due authentication configuration exception.	Look under authentication log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-704	SEVERE	Getting assigned services of realm failed.	name of realm error message	Unable to get assigned services of realm due to service management SDK exception.	Look under service management log for more information.
CONSOLE-705	SEVERE	Getting assigned services of realm failed.	name of realm error message	Unable to get assigned services of realm due to data store SDK exception.	Look under service management log for more information.
CONSOLE-706	SEVERE	Getting assigned services of realm failed.	name of realm error message	Unable to get assigned services of realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-711	INFO	Attempt to get assignable services of realm	name of realm	View realm's service main page.	
CONSOLE-712	INFO	Getting assignable services of realm succeeded.	name of realm	View realm's service main page.	
CONSOLE-713	SEVERE	Getting assignable services of realm failed.	name of realm error message	Unable to get assignable services of realm due authentication configuration exception.	Look under authentication log for more information.
CONSOLE-714	SEVERE	Getting assignable services of realm failed.	name of realm error message	Unable to get assignable services of realm due to service management SDK exception.	Look under service management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-715	SEVERE	Getting assignable services of realm failed.	name of realm error message	Unable to get assignable services of realm due to ID Repository management SDK exception.	Look under ID Repository management log for more information.
CONSOLE-716	SEVERE	Getting assignable services of realm failed.	name of realm error message	Unable to get assignable services of realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-721	INFO	Attempt to unassign service from realm	name of realm name of service	Click on Unassign button in realm's service page.	
CONSOLE-722	INFO	Unassign service from realm succeeded.	name of realm name of service	Click on Unassign button in realm's service page.	
CONSOLE-723	SEVERE	Unassign service from realm failed.	name of realm name of service error message	Unable to unassign service from realm due to service management SDK exception.	Look under service management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-725	SEVERE	Unassign service from realm failed.	name of realm name of service error message	Unable to unassign service from realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store management log for more information.
CONSOLE-724	SEVERE	Unassign service from realm failed.	name of realm name of service error message	Unable to unassign service from realm due to data store management SDK exception.	Look under data store management log for more information.
CONSOLE-731	INFO	Attempt to assign service to realm	name of realm name of service	Click on assign button in realm's service page.	
CONSOLE-732	INFO	Assignment of service to realm succeeded.	name of realm name of service	Click on assign button in realm's service page.	
CONSOLE-733	SEVERE	Assignment of service to realm failed.	name of realm name of service error message	Unable to assign service to realm due to service management SDK exception.	Look under service management log for more information.
CONSOLE-734	SEVERE	Assignment of service to realm failed.	name of realm name of service error message	Unable to assign service to realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-735	SEVERE	Assignment of service to realm failed.	name of realm name of service error message	Unable to assign service to realm due to data store SDK exception.	Look under service management log for more information.
CONSOLE-741	INFO	Attempt to get attribute values of service in realm	name of realm name of service name of attribute schema	View realm's service profile page.	
CONSOLE-742	INFO	Getting of attribute values of service under realm succeeded.	name of realm name of service name of attribute schema	View realm's service profile page.	
CONSOLE-743	SEVERE	Getting of attribute values of service under realm failed.	name of realm name of service name of attribute schema error message	Unable to get attribute values of service due to service management SDK exception.	Look under service management log for more information.
CONSOLE-744	INFO	Getting of attribute values of service under realm failed.	name of realm name of service name of attribute schema error message	Unable to get attribute values of service due to data store SDK exception.	Look under service management log for more information.
CONSOLE-745	SEVERE	Getting of attribute values of service under realm failed.	name of realm name of service name of attribute schema error message	Unable to get attribute values of service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-751	INFO	Attempt to modify attribute values of service in realm	name of realm name of service	Click on Save button in realm's service profile page.	
CONSOLE-752	INFO	Modification of attribute values of service under realm succeeded.	name of realm name of service	Click on Save button in realm's service profile page.	
CONSOLE-753	SEVERE	Modification of attribute values of service under realm failed.	name of realm name of service error message	Unable to modify attribute values of service due to service management SDK exception.	Look under service management log for more information.
CONSOLE-754	SEVERE	Modification of attribute values of service under realm failed.	name of realm name of service error message	Unable to modify attribute values of service due to data store error.	Look under data store log for more information.
CONSOLE-755	SEVERE	Modification of attribute values of service under realm failed.	name of realm name of service error message	Unable to modify attribute values of service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation	Look under data store log for more information.
CONSOLE-801	INFO	Attempt to get authentication type	server instance name	View authentication profile page.	
CONSOLE-802	INFO	Getting of authentication type succeeded.	server instance name	View authentication profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-803	SEVERE	Getting of authentication type failed.	error message	Unable to get authentication type due to authentication configuration SDK exception.	Look under authentication management log for more information.
CONSOLE-811	INFO	Attempt to get authentication instances under a realm	name of realm	View authentication profile page.	
CONSOLE-812	INFO	Getting of authentication instances under a realm succeeded.	name of realm	View authentication profile page.	
CONSOLE-813	SEVERE	Getting of authentication instances under a realm failed.	name of realm error message	Unable to get authentication instance due to authentication configuration SDK exception.	Look under authentication management log for more information.
CONSOLE-821	INFO	Attempt to remove authentication instances under a realm	name of realm name of authentication instance	View authentication profile page.	
CONSOLE-822	INFO	Removal of authentication instances under a realm succeeded.	name of realm name of authentication instance	View authentication profile page.	
CONSOLE-823	SEVERE	Removal of authentication instances under a realm failed.	name of realm name of authentication instance error message	Unable to remove authentication instance due to authentication configuration SDK exception.	Look under authentication management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-831	INFO	Attempt to create authentication instance under a realm	name of realm name of authentication instance type of authentication instance	Click on New button in authentication creation page.	
CONSOLE-832	INFO	Creation of authentication instance under a realm succeeded.	name of realm name of authentication instance type of authentication instance	Click on New button in authentication creation page.	
CONSOLE-833	SEVERE	Creation of authentication instance under a realm failed.	name of realm name of authentication instance type of authentication instance error message	Unable to create authentication instance due to authentication configuration exception.	Look under authentication configuration log for more information.
CONSOLE-841	INFO	Attempt to modify authentication instance	name of realm name of authentication service	Click on Save button in authentication profile page.	
CONSOLE-842	INFO	Modification of authentication instance succeeded.	name of realm name of authentication service	Click on Save button in authentication profile page.	
CONSOLE-843	SEVERE	Modification of authentication instance failed.	name of realm name of authentication service error message	Unable to modify authentication instance due to service management SDK exception.	Look under service anagement log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-844	SEVERE	Modification of authentication instance failed.	name of realm name of authentication service error message	Unable to modify authentication instance. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-851	INFO	Attempt to get authentication instance profile	name of realm name of authentication instance	View authentication instance profile page.	
CONSOLE-852	INFO	Getting of authentication instance profile succeeded.	name of realm name of authentication instance	View authentication instance profile page.	
CONSOLE-853	SEVERE	Getting of authentication instance profile failed.	name of realm name of authentication instance error message	Unable to get authentication instance profile due to authentication configuration SDK exception.	Look under authentication management log for more information.
CONSOLE-861	INFO	Attempt to modify authentication instance profile	name of realm name of authentication instance	Click on Save button in authentication instance profile page.	
CONSOLE-862	INFO	Modification of authentication instance profile succeeded.	name of realm name of authentication instance	Click on Save button in authentication instance profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-863	SEVERE	Modification of authentication instance profile failed.	name of realm name of authentication instance error message	Unable to modify authentication instance profile due to authentication configuration SDK exception.	Look under authentication management log for more information.
CONSOLE-864	SEVERE	Modification of authentication instance profile failed.	name of realm name of authentication instance error message	Unable to modify authentication instance profile due to service management SDK exception.	Look under service management log for more information.
CONSOLE-865	SEVERE	Modification of authentication instance profile failed.	name of realm name of authentication instance error message	Unable to modify authentication instance profile. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-871	INFO	Attempt to get authentication profile under a realm	name of realm	View authentication profile under a realm page.	
CONSOLE-872	INFO	Getting authentication profile under a realm succeeded.	name of realm	View authentication profile under a realm page.	
CONSOLE-873	SEVERE	Getting authentication profile under a realm failed.	name of realm error message	Unable to get authentication profile under a realm due to service management SDK exception.	Look under service management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-881	INFO	Attempt to get authentication configuration profile	name of realm name of authentication configuration	View authentication configuration profile page.	
CONSOLE-882	INFO	Getting authentication configuration profile succeeded.	name of realm name of authentication configuration	View authentication configuration profile page.	
CONSOLE-883	SEVERE	Getting authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to get authentication configuration profile. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-884	SEVERE	Getting authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to get authentication configuration profile due to service management SDK exception.	Look under service management log for more information.
CONSOLE-885	SEVERE	Getting authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to get authentication configuration profile due to authentication configuration SDK exception.	Look under authentication configuration log for more information.
CONSOLE-891	INFO	Attempt to modify authentication configuration profile	name of realm name of authentication configuration	Click on Save button in authentication configuration profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-892	INFO	Modification of authentication configuration profile succeeded.	name of realm name of authentication configuration	Click on Save button in authentication configuration profile page.	
CONSOLE-893	SEVERE	Modification of authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to modify authentication configuration profile. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-894	SEVERE	Modification of authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to modify authentication configuration profile due to service management SDK exception.	Look under service management log for more information.
CONSOLE-895	SEVERE	Modification of authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to modify authentication configuration profile due to authentication configuration SDK exception.	Look under authentication configuration log for more information.
CONSOLE-901	INFO	Attempt to create authentication configuration	name of realm name of authentication configuration	Click on New button in authentication configuration creation page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-902	INFO	Creation of authentication configuration succeeded.	name of realm name of authentication configuration	Click on New button in authentication configuration creation page.	
CONSOLE-903	SEVERE	Creation of authentication configuration failed.	name of realm name of authentication configuration error message	Unable to create authentication configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-904	SEVERE	Creation of authentication configuration failed.	name of realm name of authentication configuration error message	Unable to create authentication configuration due to service management SDK exception.	Look under service management log for more information.
CONSOLE-905	SEVERE	Creation of authentication configuration failed.	name of realm name of authentication configuration error message	Unable to create authentication configuration due to authentication configuration SDK exception.	Look under authentication configuration log for more information.
CONSOLE-1001	INFO	Attempt to get entity descriptor names.	search pattern	View entity descriptor main page.	
CONSOLE-1002	INFO	Getting entity descriptor names succeeded	search pattern	View entity descriptor main page.	
CONSOLE-1003	SEVERE	Getting entity descriptor names failed.	search pattern error message	Unable to get entity descriptor names due to federation SDK related errors.	Look under federation log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-1011	INFO	Attempt to create entity descriptor.	descriptor realm descriptor name descriptor protocol descriptor type	Click on New button in entity descriptor creation page.	
CONSOLE-1012	INFO	Creation entity descriptor succeeded	descriptor realm descriptor name descriptor protocol descriptor type	Click on New button in entity descriptor creation page.	
CONSOLE-1013	SEVERE	Creation entity descriptor failed.	descriptor realm descriptor name descriptor protocol descriptor type error message	Unable to create entity descriptor due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1021	INFO	Attempt to delete entity descriptors.	descriptor names	Click on Delete button in entity descriptor main page.	
CONSOLE-1022	INFO	Deletion entity descriptors succeeded	descriptor names	Click on Delete button in entity descriptor main page.	
CONSOLE-1023	SEVERE	Deletion entity descriptors failed.	descriptor names error message	Unable to delete entity descriptors due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1031	INFO	Attempt to get attribute values of an affiliate entity descriptor.	descriptor realm descriptor name descriptor protocol	View affiliate entity descriptor profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-1032	INFO	Getting of attribute values of an affiliate entity descriptor succeeded.	descriptor realm descriptor name descriptor protocol	View affiliate entity descriptor profile page.	
CONSOLE-1033	SEVERE	Getting of attribute values of an affiliate entity descriptor failed.	descriptor realm descriptor name descriptor protocol error message	Unable to get attribute value of an affiliate entity descriptor due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1041	INFO	Attempt to modify an affiliate entity descriptor.	descriptor realm descriptor name descriptor protocol	Click on Save button of affiliate entity descriptor profile page.	
CONSOLE-1042	INFO	Modification of an affiliate entity descriptor succeeded.	descriptor realm descriptor name descriptor protocol	Click on Save button of affiliate entity descriptor profile page.	
CONSOLE-1043	SEVERE	Modification of an affiliate entity descriptor failed.	descriptor realm descriptor name descriptor protocol error message	Unable to modify an affiliate entity descriptor due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1044	SEVERE	Modification of an affiliate entity descriptor failed.	descriptor name error message	Unable to modify an affiliate entity descriptor due to incorrect number format of one or more attribute values.	Look under federation log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-1051	INFO	Attempt to get attribute values of an entity descriptor.	descriptor realm descriptor name descriptor protocol descriptor type	View entity descriptor profile page.	
CONSOLE-1052	INFO	Getting attribute values of entity descriptor succeeded.	descriptor realm descriptor name descriptor protocol descriptor type	View entity descriptor profile page.	
CONSOLE-1053	SEVERE	Getting attribute values of entity descriptor failed.	descriptor realm descriptor name descriptor protocol descriptor type error message	Unable to get attribute values of entity descriptor due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1061	INFO	Attempt to modify entity descriptor.	descriptor realm descriptor name descriptor protocol descriptor type	Click on Save button in entity descriptor profile page.	
CONSOLE-1062	INFO	Modification of entity descriptor succeeded.	descriptor realm descriptor name descriptor protocol descriptor type	Click on Save button in entity descriptor profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-1063	SEVERE	Modification of entity descriptor failed.	descriptor realm descriptor name descriptor protocol descriptor type error message	Unable to modify entity descriptor due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1101	INFO	Attempt to get circle of trust names.	search pattern	View circle of trust main page.	
CONSOLE-1102	INFO	Getting circle of trust names succeeded.	search pattern	View circle of trust main page.	
CONSOLE-1103	SEVERE	Getting circle of trust names failed.	search pattern error message	Unable to get circle of trust names due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1111	INFO	Attempt to create circle of trust	name of circle of trust	Click on New button in circle of trust creation page.	
CONSOLE-1112	INFO	Creation circle of trust succeeded.	name of circle of trust	Click on New button in circle of trust creation page.	
CONSOLE-1113	SEVERE	Creation circle of trust failed.	name of circle of trust error message	Unable to create circle of trust due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1121	INFO	Attempt to delete circle of trusts	name of circle of trusts	Click on Delete button in circle of trust main page.	
CONSOLE-1122	INFO	Deletion circle of trust succeeded.	name of circle of trusts	Click on Delete button in circle of trust main page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-1123	SEVERE	Deletion circle of trust failed.	name of circle of trusts error message	Unable to delete circle of trust due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1131	INFO	Attempt to get circle of trust's attribute values	name of circle of trust	View circle of trust profile page.	
CONSOLE-1132	INFO	Getting attribute values of circle of trust succeeded.	name of circle of trust	View circle of trust profile page.	
CONSOLE-1133	SEVERE	Getting attribute values of circle of trust failed.	name of circle of trusts error message	Unable to get attribute values of circle of trust due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1141	INFO	Attempt to modify circle of trust	name of circle of trust	Click on Save button in circle of trust profile page.	
CONSOLE-1142	INFO	Modification circle of trust succeeded.	name of circle of trust	Click on Save button in circle of trust profile page.	
CONSOLE-1143	SEVERE	Modification circle of trust failed.	name of circle of trust error message	Unable to modify circle of trust due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1151	INFO	Attempt to get all provider names	realm name	View circle of trust profile page.	
CONSOLE-1152	INFO	Getting all provider names succeeded.	realm name	View circle of trust profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-1153	SEVERE	Getting all provider names failed.	error message	Unable to get all provider names due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1161	INFO	Attempt to get provider names under a circle of trust	name of circle of trust	View circle of trust profile page.	
CONSOLE-1162	INFO	Getting provider names under circle of trust succeeded.	name of circle of trust	View circle of trust profile page.	
CONSOLE-1163	SEVERE	Getting provider names under circle of trust failed.	name of circle of trust error message	Unable to get provider names under circle of trust due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1171	INFO	Attempt to add providers to an circle of trust	name of circle of trust name of providers	Click on Save button in provider assignment page.	
CONSOLE-1172	INFO	Addition of provider to an circle of trust succeeded.	name of circle of trust name of providers	Click on Save button in provider assignment page.	
CONSOLE-1173	SEVERE	Addition of provider to an circle of trust failed.	name of circle of trust name of providers error message	Unable to add provider to circle of trust due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1181	INFO	Attempt to remove providers from circle of trust	name of circle of trust name of providers	Click on Save button in provider assignment page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-1182	INFO	Deletion of providers from circle of trust succeeded.	name of circle of trust name of providers	Click on Save button in provider assignment page.	
CONSOLE-1183	SEVERE	Deletion of provider from circle of trust failed.	name of circle of trust name of providers error message	Unable to remove provider from circle of trust due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1301	INFO	Attempt to create provider	name of provider role of provider type of provider	Click on Save button in provider assignment page.	
CONSOLE-1302	INFO	Creation of providers succeeded.	name of provider role of provider type of provider	Click on Save button in provider assignment page.	
CONSOLE-1303	SEVERE	Creation of provider failed.	name of provider role of provider type of provider error message	Unable to create provider due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1304	SEVERE	Creation of provider failed.	name of provider role of provider type of provider error message	Unable to create provider due to federation SDK related errors.	Look under federation log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-1305	SEVERE	Creation of provider failed.	name of provider role of provider type of provider error message	Unable to create provider because Administration Console cannot find the appropriate methods to set values for this provider.	This is a web application error. Please contact Sun Support for assistant.
CONSOLE-1311	INFO	Attempt to get attribute values for provider	name of provider role of provider type of provider	View provider profile page.	
CONSOLE-1312	INFO	Getting attribute values of providers succeeded.	name of provider role of provider type of provider	View provider profile page.	
CONSOLE-1321	INFO	Attempt to get handler to provider	name of provider role of provider	View provider profile page.	
CONSOLE-1322	INFO	Getting handler to provider succeeded.	name of provider role of provider	View provider profile page.	
CONSOLE-1323	SEVERE	Getting handler to provider failed.	name of provider role of provider error message	Unable to get handler to provider due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1331	INFO	Attempt to modify provider	name of provider role of provider	Click on Save button in provider profile page.	
CONSOLE-1332	INFO	Modification of provider succeeded.	name of provider role of provider	Click on Save button in provider profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-1333	SEVERE	Modification of provider failed.	name of provider role of provider error message	Unable to modify provider due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1334	SEVERE	Modification of provider failed.	name of provider role of provider error message	Unable to modify provider because Administration Console cannot find the appropriate methods to set values for this provider.	This is a web application error. Please contact Sun Support for assistant.
CONSOLE-1341	INFO	Attempt to delete provider	name of provider role of provider	Click on delete provider button in provider profile page.	
CONSOLE-1342	INFO	Deletion of provider succeeded.	name of provider role of provider	Click on delete provider button in provider profile page.	
CONSOLE-1343	SEVERE	Deletion of provider failed.	name of provider role of provider error message	Unable to delete provider due to federation SDK related errors.	Look under federation log for more information.
CONSOLE-1351	INFO	Attempt to get prospective trusted provider	name of provider role of provider	View add trusted provider page.	
CONSOLE-1352	INFO	Getting of prospective trusted provider succeeded.	name of provider role of provider	View add trusted provider page.	
CONSOLE-1353	SEVERE	Getting of prospective trusted provider failed.	name of provider role of provider error message	Unable to get prospective trusted provider due to federation SDK related errors.	Look under federation log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-2001	INFO	Attempt to get attribute values of schema type of a service schema	name of service name of schema type name of attribute schemas	View service profile page.	
CONSOLE-2002	INFO	Getting attribute values of schema type of a service schema succeeded.	name of service name of schema type name of attribute schemas	View service profile page.	
CONSOLE-2003	SEVERE	Getting attribute values of schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to get attribute values of schema type of a service schema. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
CONSOLE-2004	SEVERE	Getting attribute values of schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to get attribute values of schema type of a service schema due to service management SDK related errors.	Look under service management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-2005	INFO	Getting attribute values of schema type of a service schema failed.	name of service name of schema type name of attribute schemas	View service profile page.	Need no action on this event. Console attempts to get a schema from a service but schema does not exist.
CONSOLE-2011	INFO	Attempt to get attribute values of attribute schema of a schema type of a service schema	name of service name of schema type name of attribute schemas	View service profile page.	
CONSOLE-2012	INFO	Getting attribute values of attribute schema of a schema type of a service schema succeeded.	name of service name of schema type name of attribute schemas	View service profile page.	
CONSOLE-2013	SEVERE	Getting attribute values of attribute schema of a schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to get attribute values of schema type of a service schema. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-2014	SEVERE	Getting attribute values of attribute schema of a schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to get attribute values of schema type of a service schema due to service management SDK related errors.	Look under service management log for more information.
CONSOLE-2021	INFO	Attempt to modify attribute values of attribute schema of a schema type of a service schema	name of service name of schema type name of attribute schemas	Click on Save button in service profile page.	
CONSOLE-2022	INFO	Modification attribute values of attribute schema of a schema type of a service schema succeeded.	name of service name of schema type name of attribute schemas	Click on Save button in service profile page.	
CONSOLE-2023	SEVERE	Modification attribute values of attribute schema of a schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to modify attribute values of schema type of a service schema. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-2024	SEVERE	Modification attribute values of attribute schema of a schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to modify attribute values of schema type of a service schema due to service management SDK related errors.	Look under service management log for more information.
CONSOLE-2501	INFO	Attempt to get device names of client detection service	name of profile name of style search pattern	View client profile page.	
CONSOLE-2502	INFO	Getting device names of client detection service succeeded.	name of profile name of style search pattern	View client profile page.	
CONSOLE-2511	INFO	Attempt to delete client in client detection service	type of client	Click on client type delete hyperlink page.	
CONSOLE-2512	INFO	Deletion of client in client detection service succeeded.	type of client	Click on client type delete hyperlink page.	
CONSOLE-2513	SEVERE	Deletion of client in client detection service failed.	type of client error message	Unable to delete client due to client detection SDK related errors.	Look under client detection management log for more information.
CONSOLE-2521	INFO	Attempt to create client in client detection service	type of client	Click on New button in Client Creation Page.	
CONSOLE-2522	INFO	Creation of client in client detection service succeeded.	type of client	Click on New button in Client Creation Page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-2523	SEVERE	Creation of client in client detection service failed.	type of client error message	Unable to create client due to client detection SDK related errors.	Look under client detection management log for more information.
CONSOLE-2524	INFO	Creation of client in client detection service failed.	type of client error message	Unable to create client because client type is invalid.	Check the client type again before creation.
CONSOLE-2531	INFO	Attempt to get client profile in client detection service	type of client classification	View client profile page.	
CONSOLE-2532	INFO	Getting of client profile in client detection service succeeded.	type of client classification	View client profile page.	
CONSOLE-2541	INFO	Attempt to modify client profile in client detection service	type of client	Click on Save button client profile page.	
CONSOLE-2542	INFO	Modification of client profile in client detection service succeeded.	type of client	Click on Save button client profile page.	
CONSOLE-2543	SEVERE	Modification of client profile in client detection service failed.	type of client error message	Unable to modify client profile due to client detection SDK related errors.	Look under client detection management log for more information.
CONSOLE-3001	INFO	Attempt to get current sessions	name of server search pattern	View session main page.	
CONSOLE-3002	INFO	Getting of current sessions succeeded.	name of server search pattern	View session main page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-3003	SEVERE	Getting of current sessions failed.	name of server name of realm error message	Unable to get current sessions due to session SDK exception.	Look under session management log for more information.
CONSOLE-3011	INFO	Attempt to invalidate session	name of server ID of session	Click on Invalidate button in session main page.	
CONSOLE-3012	INFO	Invalidation of session succeeded.	name of server ID of session	Click on Invalidate button in session main page.	
CONSOLE-3013	SEVERE	Invalidation of session failed.	name of server ID of session error message	Unable to invalidate session due to session SDK exception.	Look under session management log for more information.
CONSOLE-10001	INFO	Attempt to search for containers from an organization	DN of organization search pattern	Click on Search button in Organization's containers page.	
CONSOLE-10002	INFO	Searching for containers from an organization succeeded.	DN of organization search pattern	Click on Search button in Organization's containers page.	
CONSOLE-10003	SEVERE	Searching for containers from an organization failed.	DN of organization search pattern error message	Unable to search for containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10004	SEVERE	Searching for containers from an organization failed.	DN of organization search pattern error message	Unable to search for containers due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10011	INFO	Attempt to search for containers from a container	DN of container search pattern	Click on Search button in Container's sub containers page.	
CONSOLE-10012	INFO	Searching for containers from a container succeeded.	DN of container search pattern	Click on Search button in Container's sub containers page.	
CONSOLE-10013	SEVERE	Searching for containers from a container failed.	DN of container search pattern error message	Unable to search for containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10014	SEVERE	Searching for containers from a container failed.	DN of container search pattern error message	Unable to search for containers due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10021	INFO	Attempt to create containers under an organization	DN of organization Name of container	Click on New button in Container Creation page.	
CONSOLE-10022	INFO	Creation of container under an organization succeeded.	DN of organization Name of container	Click on New button in Container Creation page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10023	SEVERE	Creation of container under an organization failed.	DN of organization Name of container error message	Unable to create container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10024	SEVERE	Creation of container under an organization failed.	DN of organization Name of container error message	Unable to create container due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10031	INFO	Attempt to create containers under an container	DN of container Name of container	Click on New button in Container Creation page.	
CONSOLE-10032	INFO	Creation of container under an container succeeded.	DN of container Name of container	Click on New button in Container Creation page.	
CONSOLE-10033	SEVERE	Creation of container under an container failed.	DN of container Name of container error message	Unable to create container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10034	SEVERE	Creation of container under an container failed.	DN of container Name of container error message	Unable to create container due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10041	INFO	Attempt to get assigned services to container	DN of container	View Container's service profile page.	
CONSOLE-10042	INFO	Getting assigned services to container succeeded.	DN of container	View Container's service profile page.	
CONSOLE-10043	SEVERE	Getting assigned services to container failed.	DN of container error message	Unable to get services assigned to container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10044	SEVERE	Getting assigned services to container failed.	DN of container error message	Unable to get services assigned to container due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10101	INFO	Attempt to get service template under an organization	DN of organization Name of service Type of template	View Organization's service profile page.	
CONSOLE-10102	INFO	Getting service template under an organization succeeded.	DN of organization Name of service Type of template	View Organization's service profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10103	SEVERE	Getting service template under an organization failed.	DN of organization Name of service Type of template error message	Unable to get service template. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10104	SEVERE	Getting service template under an organization failed.	DN of organization Name of service Type of template error message	Unable to get service template due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10111	INFO	Attempt to get service template under a container	DN of container Name of service Type of template	View container's service profile page.	
CONSOLE-10112	INFO	Getting service template under a container succeeded.	DN of container Name of service Type of template	View container's service profile page.	
CONSOLE-10113	SEVERE	Getting service template under a container failed.	DN of container Name of service Type of template error message	Unable to get service template. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10114	SEVERE	Getting service template under a container failed.	DN of container Name of service Type of template error message	Unable to get service template due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10121	INFO	Attempt to delete directory object	Name of object	Click on Delete button in object main page.	
CONSOLE-10122	INFO	Deletion of directory object succeeded.	Name of object	Click on Delete button in object main page.	
CONSOLE-10123	SEVERE	Deletion of directory object failed.	Name of object error message	Unable to delete directory object. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10124	SEVERE	Deletion of directory object failed.	Name of object error message	Unable to delete directory object due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10131	INFO	Attempt to modify directory object	DN of object	Click on object profile page.	
CONSOLE-10132	INFO	Modification of directory object succeeded.	DN of object	Click on object profile page.	
CONSOLE-10133	SEVERE	Modification of directory object failed.	DN of object error message	Unable to modify directory object due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10141	INFO	Attempt to delete service from organization	DN of organization Name of service	Click on unassign button in organization's service page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10142	INFO	Deletion of service from organization succeeded.	DN of organization Name of service	Click on unassign button in organization's service page.	
CONSOLE-10143	SEVERE	Deletion of service from organization failed.	DN of organization Name of service error message	Unable to delete service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10144	SEVERE	Deletion of service from organization failed.	DN of organization Name of service error message	Unable to delete service due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10151	INFO	Attempt to delete service from container	DN of container Name of service	Click on unassign button in container's service page.	
CONSOLE-10152	INFO	Deletion of service from container succeeded.	DN of container Name of service	Click on unassign button in container's service page.	
CONSOLE-10153	SEVERE	Deletion of service from container failed.	DN of container Name of service error message	Unable to delete service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10154	SEVERE	Deletion of service from container failed.	DN of container Name of service error message	Unable to delete service due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10201	INFO	Attempt to serch for group containers under organization	DN of organization Search pattern	Click on Search button in organization's group containers page.	
CONSOLE-10202	INFO	Searching for group containers under organization succeeded.	DN of organization Search pattern	Click on Search button in organization's group containers page.	
CONSOLE-10203	SEVERE	Searching for group containers under organization failed.	DN of organization Search pattern error message	Unable to search group containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10204	SEVERE	Searching for group containers under organization failed.	DN of organization Search pattern error message	Unable to search group containers due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10211	INFO	Attempt to serch for group containers under container	DN of container Search pattern	Click on Search button in container's group containers page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10212	INFO	Searching for group containers under container succeeded.	DN of container Search pattern	Click on Search button in container's group containers page.	
CONSOLE-10213	SEVERE	Searching for group containers under container failed.	DN of container Search pattern error message	Unable to search group containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10214	SEVERE	Searching for group containers under container failed.	DN of container Search pattern error message	Unable to search group containers due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10221	INFO	Attempt to search for group containers under group container	DN of group container Search pattern	Click on Search button in group container's group containers page.	
CONSOLE-10222	INFO	Searching for group containers under group container succeeded.	DN of group container Search pattern	Click on Search button in group container's group containers page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10223	SEVERE	Searching for group containers under group container failed.	DN of group container Search pattern error message	Unable to search group containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10224	SEVERE	Searching for group containers under group container failed.	DN of group container Search pattern error message	Unable to search group containers due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10231	INFO	Attempt to create group container in organization	DN of organization Name of group container	Click on New button in group container creation page.	
CONSOLE-10232	INFO	Creation of group container under organization succeeded.	DN of organization Name of group container	Click on New button in group container creation page.	
CONSOLE-10233	SEVERE	Creation of group container under organization failed.	DN of organization Name of group container error message	Unable to create group container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10234	SEVERE	Creation of group container under organization failed.	DN of organization Name of group container error message	Unable to create group container due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10241	INFO	Attempt to create group container in container	DN of container Name of group container	Click on New button in group container creation page.	
CONSOLE-10242	INFO	Creation of group container under container succeeded.	DN of container Name of group container	Click on New button in group container creation page.	
CONSOLE-10243	SEVERE	Creation of group container under container failed.	DN of container Name of group container error message	Unable to create group container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10244	SEVERE	Creation of group container under container failed.	DN of container Name of group container error message	Unable to create group container due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10251	INFO	Attempt to create group container in group container	DN of group container Name of group container	Click on New button in group container creation page.	
CONSOLE-10252	INFO	Creation of group container under group container succeeded.	DN of group container Name of group container	Click on New button in group container creation page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10253	SEVERE	Creation of group container under group container failed.	DN of group container Name of group container error message	Unable to create group container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10254	SEVERE	Creation of group container under group container failed.	DN of group container Name of group container error message	Unable to create group container due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10301	INFO	Attempt to search groups under organization	DN of organization search pattern	Click on Search button in organization's group page.	
CONSOLE-10302	INFO	Searching for groups under organization succeeded.	DN of organization search pattern	Click on Search button in organization's group page.	
CONSOLE-10303	SEVERE	Searching for groups under organization failed.	DN of organization search pattern error message	Unable to search for groups. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10304	SEVERE	Searching for groups under organization failed.	DN of organization search pattern error message	Unable to search groups due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10311	INFO	Attempt to search groups under container	DN of container search pattern	Click on Search button in container's group page.	
CONSOLE-10312	INFO	Searching for groups under container succeeded.	DN of container search pattern	Click on Search button in container's group page.	
CONSOLE-10313	SEVERE	Searching for groups under container failed.	DN of container search pattern error message	Unable to search for groups. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10314	SEVERE	Searching for groups under container failed.	DN of container search pattern error message	Unable to search groups due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10321	INFO	Attempt to search groups under static group	DN of static group search pattern	Click on Search button in static group's group page.	
CONSOLE-10322	INFO	Searching for groups under static group succeeded.	DN of static group search pattern	Click on Search button in static group's group page.	
CONSOLE-10323	SEVERE	Searching for groups under static group failed.	DN of static group search pattern error message	Unable to search for groups. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10324	SEVERE	Searching for groups under static group failed.	DN of static group search pattern error message	Unable to search groups due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10331	INFO	Attempt to search groups under dynamic group	DN of dynamic group search pattern	Click on Search button in dynamic group's group page.	
CONSOLE-10332	INFO	Searching for groups under dynamic group succeeded.	DN of dynamic group search pattern	Click on Search button in dynamic group's group page.	
CONSOLE-10333	SEVERE	Searching for groups under dynamic group failed.	DN of dynamic group search pattern error message	Unable to search for groups. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10334	SEVERE	Searching for groups under dynamic group failed.	DN of dynamic group search pattern error message	Unable to search groups due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10341	INFO	Attempt to search groups under assignable dynamic group	DN of assignable dynamic group search pattern	Click on Search button in assignable dynamic group's group page.	
CONSOLE-10342	INFO	Searching for groups under assignable dynamic group succeeded.	DN of assignable dynamic group search pattern	Click on Search button in assignable dynamic group's group page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10343	SEVERE	Searching for groups under assignable dynamic group failed.	DN of assignable dynamic group search pattern error message	Unable to search for groups. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10344	SEVERE	Searching for groups under assignable dynamic group failed.	DN of assignable dynamic group search pattern error message	Unable to search groups due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10351	INFO	Attempt to create group under organization	DN of organization Name of group	Click on New button in group creation page.	
CONSOLE-10352	INFO	Creation of groups under organization succeeded.	DN of organization Name of group	Click on New button in group creation page.	
CONSOLE-10353	SEVERE	Creation of group under organization failed.	DN of organization Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10354	SEVERE	Creation of group under organization failed.	DN of organization Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10361	INFO	Attempt to create group under container	DN of container Name of group	Click on New button in group creation page.	
CONSOLE-10362	INFO	Creation of groups under container succeeded.	DN of container Name of group	Click on New button in group creation page.	
CONSOLE-10363	SEVERE	Creation of group under container failed.	DN of container Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10364	SEVERE	Creation of group under container failed.	DN of container Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10371	INFO	Attempt to create group under group container	DN of group container Name of group	Click on New button in group creation page.	
CONSOLE-10372	INFO	Creation of groups under group container succeeded.	DN of group container Name of group	Click on New button in group creation page.	
CONSOLE-10373	SEVERE	Creation of group under group container failed.	DN of group container Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10374	SEVERE	Creation of group under group container failed.	DN of group container Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10381	INFO	Attempt to create group under dynamic group	DN of dynamic group Name of group	Click on New button in group creation page.	
CONSOLE-10382	INFO	Creation of groups under dynamic group succeeded.	DN of dynamic group Name of group	Click on New button in group creation page.	
CONSOLE-10383	SEVERE	Creation of group under dynamic group failed.	DN of dynamic group Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10384	SEVERE	Creation of group under dynamic group failed.	DN of dynamic group Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10391	INFO	Attempt to create group under static group	DN of static group Name of group	Click on New button in group creation page.	
CONSOLE-10392	INFO	Creation of groups under static group succeeded.	DN of static group Name of group	Click on New button in group creation page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10393	SEVERE	Creation of group under static group failed.	DN of static group Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10394	SEVERE	Creation of group under static group failed.	DN of static group Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10401	INFO	Attempt to create group under assignable dynamic group	DN of assignable dynamic group Name of group	Click on New button in group creation page.	
CONSOLE-10402	INFO	Creation of groups under assignable dynamic group succeeded.	DN of assignable dynamic group Name of group	Click on New button in group creation page.	
CONSOLE-10403	SEVERE	Creation of group under assignable dynamic group failed.	DN of assignable dynamic group Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10404	SEVERE	Creation of group under assignable dynamic group failed.	DN of assignable dynamic group Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10411	INFO	Attempt to modify group	DN of group	Click on Save button in group profile page.	
CONSOLE-10412	INFO	Modification of groups succeeded.	DN of group	Click on Save button in group profile page.	
CONSOLE-10414	SEVERE	Modification of group failed.	DN of assignable dynamic group Name of group error message	Unable to modify group due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10421	INFO	Attempt to search for users in group	DN of group Search pattern	View group's user page.	
CONSOLE-10422	INFO	Searching for users in group succeeded.	DN of group Search pattern	View group's user page.	
CONSOLE-10423	SEVERE	Searching for users in group failed.	DN of group Search pattern error message	Unable to search for users. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10424	SEVERE	Searching for users in group failed.	DN of group Search pattern error message	Unable to search for users due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10431	INFO	Attempt to get nested groups	DN of group	View group's members page.	
CONSOLE-10432	INFO	Getting nested groups succeeded.	DN of group	View group's members page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10433	SEVERE	Getting nested groups failed.	DN of group error message	Unable to get nested group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10434	SEVERE	Getting nested groups failed.	DN of group error message	Unable to get nested group due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10441	INFO	Attempt to remove nested groups	DN of group DN of nested groups	Click on remove button in group's members page.	
CONSOLE-10442	INFO	Removal of nested groups succeeded.	DN of group DN of nested groups	Click on remove button in group's members page.	
CONSOLE-10443	SEVERE	Removal of nested groups failed.	DN of group DN of nested groups error message	Unable to remove nested group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10444	SEVERE	Removal of nested groups failed.	DN of group DN of nested groups error message	Unable to remove nested group due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10451	INFO	Attempt to remove users from group	DN of group DN of users	Click on remove button in group's members page.	
CONSOLE-10452	INFO	Removal of users from group succeeded.	DN of group DN of users	Click on remove button in group's members page.	
CONSOLE-10453	SEVERE	Removal of users from group failed.	DN of group DN of users error message	Unable to remove users. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10454	SEVERE	Removal of users from group failed.	DN of group DN of users error message	Unable to remove users due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10501	INFO	Attempt to search people containers in organization	DN of organization Search pattern	View organization's people containers page.	
CONSOLE-10502	INFO	Searching of people containers in organization succeeded.	DN of organization Search pattern	View organization's people containers page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10503	SEVERE	Searching of people containers in organization failed.	DN of organization Search pattern error message	Unable to search for people containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10504	SEVERE	Searching of people containers in organization failed.	DN of organization Search pattern error message	Unable to search for people containers due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10511	INFO	Attempt to search people containers in container	DN of container Search pattern	View container's people containers page.	
CONSOLE-10512	INFO	Searching of people containers in container succeeded.	DN of container Search pattern	View container's people containers page.	
CONSOLE-10513	SEVERE	Searching of people containers in container failed.	DN of container Search pattern error message	Unable to search for people containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10514	SEVERE	Searching of people containers in container failed.	DN of container Search pattern error message	Unable to search for people containers due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10521	INFO	Attempt to search people containers in people container	DN of people container Search pattern	View people container's people containers page.	
CONSOLE-10522	INFO	Searching of people containers in people container succeeded.	DN of people container Search pattern	View people container's people containers page.	
CONSOLE-10523	SEVERE	Searching of people containers in people container failed.	DN of people container Search pattern error message	Unable to search for people containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10524	SEVERE	Searching of people containers in people container failed.	DN of people container Search pattern error message	Unable to search for people containers due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10531	INFO	Attempt to create people container in organization	DN of organization Name of people container	Click on New button in people container creation page.	
CONSOLE-10532	INFO	Creation of people containers in organization succeeded.	DN of organization Name of people container	Click on New button in people container creation page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10533	SEVERE	Creation of people container in organization failed.	DN of organization Name of people container error message	Unable to create for people containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10534	SEVERE	Creation of people container in organization failed.	DN of organization Name of people container error message	Unable to create for people container due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10541	INFO	Attempt to create people container in container	DN of container Name of people container	Click on New button in people container creation page.	
CONSOLE-10542	INFO	Creation of people container in container succeeded.	DN of container Name of people container	Click on New button in people container creation page.	
CONSOLE-10543	SEVERE	Creation of people container in container failed.	DN of container Name of people container error message	Unable to create for people container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10544	SEVERE	Creation of people container in container failed.	DN of container Name of people container error message	Unable to create for people container due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10551	INFO	Attempt to create people container in people container	DN of people container Name of people container	Click on New button in people container creation page.	
CONSOLE-10552	INFO	Creation of people container in people container succeeded.	DN of people container Name of people container	Click on New button in people container creation page.	
CONSOLE-10553	SEVERE	Creation of people container in people container failed.	DN of people container Name of people container error message	Unable to create for people container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10554	SEVERE	Creation of people container in people container failed.	DN of people container Name of people container error message	Unable to create for people container due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10601	INFO	Attempt to get assigned services to an organization	DN of organization	View organization's service profile page.	
CONSOLE-10602	INFO	Getting of assigned services to organization succeeded.	DN of organization	View organization's service profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10603	SEVERE	Getting of assigned services to organization failed.	DN of organization error message	Unable to get assigned services. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10604	SEVERE	Getting of assigned services to organization failed.	DN of organization error message	Unable to get assigned services due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10611	INFO	Attempt to remove services from an organization	DN of organization Name of service	Click on unassign button in organization's service profile page.	
CONSOLE-10612	INFO	Removal of services from organization succeeded.	DN of organization Name of service	Click on unassign button in organization's service profile page.	
CONSOLE-10613	SEVERE	Removal of services from organization failed.	DN of organization Name of service error message	Unable to remove services. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10614	SEVERE	Removal of services from organization failed.	DN of organization Name of service error message	Unable to remove services due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10621	INFO	Attempt to search organization in an organization	DN of organization Search pattern	View organization's sub organization page.	
CONSOLE-10622	INFO	Searching for organization in an organization succeeded.	DN of organization Search pattern	View organization's sub organization page.	
CONSOLE-10623	SEVERE	Searching for organization in an organization failed.	DN of organization Search pattern error message	Unable to search for organizations. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10624	SEVERE	Searching for organization in an organization failed.	DN of organization Search pattern error message	Unable to search for organizations due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10631	INFO	Attempt to modify organization	DN of organization	Click on Save button in organization profile page.	
CONSOLE-10632	INFO	Modificaition of organization succeeded.	DN of organization	Click on Save button in organization profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10633	SEVERE	Modificaition of organization failed.	DN of organization error message	Unable to modify organization. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10634	SEVERE	Modificaition of organization failed.	DN of organization error message	Unable to modify organization due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10641	INFO	Attempt to create organization in an organization	DN of organization Name of new organization	Click on New button in organization creation page.	
CONSOLE-10642	INFO	Creation of organization in an organization succeeded.	DN of organization Name of new organization	Click on New button in organization creation page.	
CONSOLE-10643	SEVERE	Creation of organization in an organization failed.	DN of organization Name of new organization error message	Unable to create organization. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10644	SEVERE	Creation of organization in an organization failed.	DN of organization Name of new organization error message	Unable to create organization due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10651	INFO	Attempt to get attribute values of an organization	DN of organization	View organization profile page.	
CONSOLE-10652	INFO	Getting of attribute values of an organization succeeded.	DN of organization	View organization profile page.	
CONSOLE-10653	SEVERE	Getting of attribute values of an organization failed.	DN of organization error message	Unable to get attribute values of organization. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10654	SEVERE	Getting of attribute values of an organization failed.	DN of organization error message	Unable to get attribute values of organization due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10661	INFO	Attempt to add service to an organization	DN of organization Name of service	Click on assign button in organization's service page.	
CONSOLE-10662	INFO	Addition of service to an organization succeeded.	DN of organization Name of service	Click on assign button in organization's service page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10663	SEVERE	Addition of service to an organization failed.	DN of organization Name of service error message	Unable to add service to organization. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10664	SEVERE	Addition of service to an organization failed.	DN of organization Name of service error message	Unable to add service to organization due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10701	INFO	Attempt to remove users from role	DN of role Name of users	Click on remove button in role's user page.	
CONSOLE-10702	INFO	Removal of users from role succeeded.	DN of role Name of users	Click on remove button in role's user page.	
CONSOLE-10703	SEVERE	Removal of users from role failed.	DN of role Name of users error message	Unable to remove users. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10704	SEVERE	Removal of users from role failed.	DN of role Name of users error message	Unable to remove users due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10711	INFO	Attempt to get attribute values of role	DN of role	View role profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10712	INFO	Getting attribute values of rolesucceeded.	DN of role	View role profile page.	
CONSOLE-10713	SEVERE	Getting attribute values of role failed.	DN of role error message	Unable to get attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10714	SEVERE	Getting attribute values of role failed.	DN of role error message	Unable to get attribute values due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10721	INFO	Attempt to modify role	DN of role	Click on Save button in role profile page.	
CONSOLE-10722	INFO	Modification of role succeeded.	DN of role	Click on Save button in role profile page.	
CONSOLE-10723	SEVERE	Modification of role failed.	DN of role error message	Unable to modify role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10724	SEVERE	Modification of role failed.	DN of role error message	Unable to modify role due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10731	INFO	Attempt to getting members in role	DN of role Search pattern	View role's members page.	
CONSOLE-10732	INFO	Getting members in role succeeded.	DN of role Search pattern	View role's members page.	
CONSOLE-10733	SEVERE	Getting members in role failed.	DN of role Search pattern error message	Unable to getting members. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10734	SEVERE	Getting members in role failed.	DN of role Search pattern error message	Unable to getting members due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10741	INFO	Attempt to getting roles in organization	DN of role Search pattern	View organization's roles page.	
CONSOLE-10742	INFO	Getting roles in organization succeeded.	DN of role Search pattern View role's members page.	View organization's roles page.	
CONSOLE-10743	SEVERE	Getting roles in organization failed.	DN of role Search pattern error message	Unable to getting roles. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10744	SEVERE	Getting roles in organization failed.	DN of role Search pattern error message	Unable to getting roles due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10751	INFO	Attempt to getting roles in container	DN of role Search pattern	View container's roles page.	
CONSOLE-10752	INFO	Getting roles in container succeeded.	DN of role Search pattern View role's members page.	View container's roles page.	
CONSOLE-10753	SEVERE	Getting roles in container failed.	DN of role Search pattern error message	Unable to getting roles. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10754	SEVERE	Getting roles in container failed.	DN of role Search pattern error message	Unable to getting roles due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10761	INFO	Attempt to creating roles in container	DN of container Name of role	Click on New button in roles creation page.	
CONSOLE-10762	INFO	Creation of roles in container succeeded.	DN of container Name of role	Click on New button in roles creation page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10763	SEVERE	Creation of roles in container failed.	DN of container Name of role	Unable to create role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10764	SEVERE	Creation of role in container failed.	DN of container Name of role error message	Unable to create role due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10771	INFO	Attempt to creating roles in organization	DN of organization Name of role	Click on New button in roles creation page.	
CONSOLE-10772	INFO	Creation of roles in organization succeeded.	DN of organization Name of role	Click on New button in roles creation page.	
CONSOLE-10773	SEVERE	Creation of roles in organization failed.	DN of organization Name of role	Unable to create role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10774	SEVERE	Creation of role in organization failed.	DN of organization Name of role error message	Unable to create role due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10781	INFO	Attempt to get assigned services in role	DN of role	View role's service page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10782	INFO	Getting of assigned services in role succeeded.	DN of role	View role's service page.	
CONSOLE-10783	SEVERE	Getting of assigned services in role failed.	DN of role error message	Unable to get services in role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10784	SEVERE	Getting of assigned services in role failed.	DN of role error message	Unable to get services in role due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10791	INFO	Attempt to remove service from role	DN of role Name of service	Click on unassign button in role's service page.	
CONSOLE-10792	INFO	Removal of service from role succeeded.	DN of role Name of service	Click on unassign button in role's service page.	
CONSOLE-10793	SEVERE	Removal of service from role failed.	DN of role Name of service error message	Unable to remove service from role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10794	SEVERE	Removal of service from role failed.	DN of role Name of service error message	Unable to remove service from role due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10801	INFO	Attempt to add service to role	DN of role Name of service	Click on assign button in role's service page.	
CONSOLE-10802	INFO	Addition of service to role succeeded.	DN of role Name of service	Click on assign button in role's service page.	
CONSOLE-10803	SEVERE	Addition of service to role failed.	DN of role Name of service error message	Unable to add service to role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10804	SEVERE	Addition of service to role failed.	DN of role Name of service error message	Unable to add service to role due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10901	INFO	Attempt to get assigned role of user	DN of user	View user's role page.	
CONSOLE-10902	INFO	Getting of assigned role of user succeeded.	DN of user	View user's role page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10903	SEVERE	Getting of assigned role of user failed.	DN of user error message	Unable to get assigned roles. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10904	SEVERE	Getting of assigned role of user failed.	DN of user Name of service error message	Unable to get assigned roles due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10911	INFO	Attempt to remove role from user	DN of user DN of role	Click on delete button in user's role page.	
CONSOLE-10912	INFO	Removal of role from user succeeded.	DN of user DN of role	Click on delete button in user's role page.	
CONSOLE-10913	SEVERE	Removal of role from user failed.	DN of user DN of role error message	Unable to remove role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10914	SEVERE	Removal of role from user failed.	DN of user DN of role Name of service error message	Unable to remove role due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10921	INFO	Attempt to add role to user	DN of user DN of role	Click on add button in user's role page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10922	INFO	Addition of role to user succeeded.	DN of user DN of role	Click on add button in user's role page.	
CONSOLE-10923	SEVERE	Addition of role to user failed.	DN of user DN of role error message	Unable to add role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10924	SEVERE	Addition of role to user failed.	DN of user DN of role Name of service error message	Unable to add role due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10931	INFO	Attempt to get assigned services of user	DN of user	View user's services page.	
CONSOLE-10932	INFO	Getting assigned services of user succeeded.	DN of user	View user's services page.	
CONSOLE-10933	SEVERE	Getting assigned services of user failed.	DN of user error message	Unable to get services. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10934	SEVERE	Getting assigned services of user failed.	DN of user error message	Unable to get services due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10941	INFO	Attempt to remove service from user	DN of user Name of service	Click on remove button in user's services page.	
CONSOLE-10942	INFO	Removal of service from user succeeded.	DN of user Name of service	Click on remove button in user's services page.	
CONSOLE-10943	SEVERE	Removal of service from user failed.	DN of user Name of service error message	Unable to remove services. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10944	SEVERE	Removal of service from user failed.	DN of user Name of service error message	Unable to remove services due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10951	INFO	Attempt to search for user in an organization	DN of organization Search pattern	View organization's user page.	
CONSOLE-10952	INFO	Searching for user in organization succeeded.	DN of organization Search pattern	View organization's user page.	
CONSOLE-10953	SEVERE	Searching for user in organization failed.	DN of organization Search pattern error message	Unable to search for user. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10954	SEVERE	Searching for user in organization failed.	DN of organization Search pattern error message	Unable to search for user due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10961	INFO	Attempt to modify user	DN of user	Click on Save button in user profile page.	
CONSOLE-10962	INFO	Modification of user profile succeeded.	DN of user	Click on Save button in user profile page.	
CONSOLE-10963	SEVERE	Modification of user profile failed.	DN of user error message	Unable to modify user. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10964	SEVERE	Modification of user profile failed.	DN of user error message	Unable to modify user due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10971	INFO	Attempt to create user	DN of people container Name of user	Click on Add button in user creation page.	
CONSOLE-10972	INFO	Creation of user succeeded.	DN of people container Name of user	Click on Add button in user creation page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10973	SEVERE	Creation of user failed.	DN of people container Name of user error message	Unable to create user. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10974	SEVERE	Creation of user failed.	DN of people container Name of user error message	Unable to create user due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10981	INFO	Attempt to get attribute values of user	DN of user	View user profile page.	
CONSOLE-10982	INFO	Getting attribute values of user succeeded.	DN of user	View user profile page.	
CONSOLE-10983	SEVERE	Getting attribute values of user failed.	DN of user error message	Unable to get attribute values . It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10984	SEVERE	Getting attribute values of user failed.	DN of user error message	Unable to get attribute values due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-10991	INFO	Attempt to add service to user	DN of user Name of service	Click on add button in user's service page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-10992	INFO	Addition of service to user succeeded.	DN of user Name of service	Click on add button in user's service page.	
CONSOLE-10993	SEVERE	Addition of service to user failed.	DN of user Name of service error message	Unable to add service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-10994	SEVERE	Addition of service to user failed.	DN of user Name of service error message	Unable to add service due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-11001	INFO	Attempt to get assigned groups of user	DN of user	View user's group page.	
CONSOLE-11002	INFO	Getting of assigned group of user succeeded.	DN of user	View user's group page.	
CONSOLE-11003	SEVERE	Getting of assigned group of user failed.	DN of user error message	Unable to get assigned group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-11004	SEVERE	Getting of assigned group of user failed.	DN of user error message	Unable to get assigned group due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-11011	INFO	Attempt to remove group from user	DN of user DN of group	Click on remove button in user's group page.	
CONSOLE-11012	INFO	Removal of group from user succeeded.	DN of user DN of group	Click on remove button in user's group page.	
CONSOLE-11013	SEVERE	Removal of group from user failed.	DN of user DN of group error message	Unable to remove group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-11014	SEVERE	Removal of group from user failed.	DN of user DN of group error message	Unable to remove group due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-11021	INFO	Attempt to add group to user	DN of user DN of group	Click on add button in user's group page.	
CONSOLE-11022	INFO	Addition of group to user succeeded.	DN of user DN of group	Click on add button in user's group page.	
CONSOLE-11023	SEVERE	Addition of group to user failed.	DN of user DN of group error message	Unable to add group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-11024	SEVERE	Addition of group to user failed.	DN of user DN of group error message	Unable to add group due to access management SDK exception.	Look under access management SDK log for more information.
CONSOLE-12001	INFO	Attempt to get site names	server instance name	View site and server management page.	
CONSOLE-12002	INFO	Site names are returned.	server instance name	View site and server management page.	
CONSOLE-12003	SEVERE	Get site names.	error message	Unable to get site names. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12004	SEVERE	Get site names.	error message	Unable to get site names due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12011	INFO	Attempt to get primary URL of site.	Site Name	View site profile page.	
CONSOLE-12012	INFO	Primary URL of site is returned.	Site Name	View site profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12013	SEVERE	Get primary URL of site.	Site Name error message	Unable to get primary URL of site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12014	SEVERE	Get primary URL of site.	Site Name error message	Unable to get primary URL of site due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12021	INFO	Attempt to get failover URLs of site.	Site Name	View site profile page.	
CONSOLE-12022	INFO	Failover URLs of site is returned.	Site Name	View site profile page.	
CONSOLE-12023	SEVERE	Get failover URLs of site.	Site Name error message	Unable to get failover URLs of site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12024	SEVERE	Get failover URLs of site.	Site Name error message	Unable to get failover URLs of site due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12031	INFO	Attempt to get members of site.	Site Name	View site profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12032	INFO	Members of site is returned.	Site Name	View site profile page.	
CONSOLE-12033	SEVERE	Get members of site.	Site Name error message	Unable to get members of site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12034	SEVERE	Get members of site.	Site Name error message	Unable to get members of site due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12041	INFO	Attempt to create site.	Site Name	View create site page.	
CONSOLE-12042	INFO	Site is created.	Site Name	Click on create button on creation page.	
CONSOLE-12043	SEVERE	Create site.	Site Name error message	Unable to create site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12044	SEVERE	Create site.	Site Name error message	Unable to create site due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12051	INFO	Attempt to create server.	Server Name	View create server page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12052	INFO	Server is created.	Server Name	Click on create button on creation page.	
CONSOLE-12053	SEVERE	Create server.	Server Name error message	Unable to create server. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12054	SEVERE	Create server.	Server Name error message	Unable to create server due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12055	SEVERE	Create server.	Server Name error message	Unable to create server due the incorrect data format error.	Look under console log for more information.
CONSOLE-12056	SEVERE	Create server.	Server Name error message	Unable to create server due the incorrect data format error.	Look under console log for more information.
CONSOLE-12061	INFO	Attempt to delete site.	Site Name	Click on delete site button.	
CONSOLE-12062	INFO	Site is deleted.	Site Name	Click on delete button.	
CONSOLE-12063	SEVERE	Delete site.	Site Name error message	Unable to delete site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12064	SEVERE	Delete site.	Site Name error message	Unable to delete site due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12071	INFO	Attempt to modify site.	Site Name	Click on OK button in site profile page.	
CONSOLE-12072	INFO	Site is nodified.	Site Name	Click on OK button in site profile page.	
CONSOLE-12073	SEVERE	Modify site.	Site Name error message	Unable to modify site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12074	SEVERE	Modify site.	Site Name error message	Unable to modify site due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12075	SEVERE	Modify site.	Site Name error message	Unable to modify site due the incorrect data format.	Look under console log for more information.
CONSOLE-12081	INFO	Attempt to get server names.	server instance name	View site and server management page.	
CONSOLE-12082	INFO	Server names are returned.	server instance name	View site and server management page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12083	SEVERE	Get server name.	error message	Unable to get server names. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12084	SEVERE	Get server name.	error message	Unable to get server names due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12091	INFO	Attempt to get server's site.	Server Name	View server profile page.	
CONSOLE-12092	INFO	Server's site name is returned.	Server Name	View server profile page.	
CONSOLE-12093	SEVERE	Get server's site name.	Server Name error message	Unable to get server's site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12094	SEVERE	Get server's site name.	Server Name error message	Unable to get server's site due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12101	INFO	Attempt to delete server.	Server Name	Click on delete button in server management page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12102	INFO	Server is delete.	Server Name	Click on delete button in server management page.	
CONSOLE-12103	SEVERE	Delete server.	Server Name error message	Unable to delete server. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12104	SEVERE	Delete server.	Server Name error message	Unable to delete server due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12201	INFO	Attempt to clone server.	Server Name Cloned Server Name	Click on clone button in server management page.	
CONSOLE-12202	INFO	Server is cloned.	Server Name Cloned Server Name	Click on clone button in server management page.	
CONSOLE-12203	SEVERE	clone server.	Server Name Cloned Server Name error message	Unable to clone server. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12204	SEVERE	clone server.	Server Name Cloned Server Name error message	Unable to clone server due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12205	SEVERE	clone server.	Server Name Cloned Server Name error message	Unable to clone server due the data format error.	Look under console log for more information.
CONSOLE-12211	INFO	Attempt to get server's configuration.	Server Name	View server profile page.	
CONSOLE-12212	INFO	Server's configuration is returned.	Server Name	View server profile page.	
CONSOLE-12213	SEVERE	Get server's configuration.	Server Name error message	Unable to get server's configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12214	SEVERE	Get server's configuration.	Server Name error message	Unable to get server's configuration due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12215	SEVERE	get server's configuration.	Server Name error message	Unable to get server's configuration due the data parsing error.	Look under console log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12221	INFO	Attempt to get server default configuration.	server instance name	View server profile page.	
CONSOLE-12222	INFO	Server default configuration is returned.	server instance name	View server profile page.	
CONSOLE-12231	INFO	Attempt to modify server.	Server Name	Click on OK button in server profile page.	
CONSOLE-12232	INFO	Server is modified.	Server Name	Click on OK button in server profile page.	
CONSOLE-12233	SEVERE	modify server.	Server Name error message	Unable to modify server. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12234	SEVERE	modify server.	Server Name error message	Unable to modify server due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12235	SEVERE	modify server.	Server Name error message	Unable to modify server due the data parsing error.	Look under console log for more information.
CONSOLE-12236	SEVERE	modify server.	Server Name error message	Unable to modify server due the incorrect data format error.	Look under console log for more information.
CONSOLE-12241	INFO	Attempt to modify server's inheritance.	Server Name	Click on OK button in server inheritance setting page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12242	INFO	Server's inheritance setting is modified.	Server Name	Click on OK button in server inheritance setting page.	
CONSOLE-12243	SEVERE	Modify server's inheritance.	Server Name error message	Unable to modify server's inheritance. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12244	SEVERE	Modify server's inheritance.	Server Name error message	Unable to modify server's inheritance due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12245	SEVERE	modify server's inheritance.	Server Name error message	Unable to modify server's inheritance due the data parsing error.	Look under console log for more information.
CONSOLE-12246	SEVERE	modify server's inheritance.	Server Name error message	Unable to modify server's inheritance due the incorrect data format error.	Look under console log for more information.
CONSOLE-12251	INFO	Attempt to get server's configuration XML.	Server Name	View server's server configuration XML profile page.	
CONSOLE-12252	INFO	Server's configuration XML is returned.	Server Name	View server's server configuration XML profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12253	SEVERE	Get server's configuration XML.	Server Name error message	Unable to get server's configuration XML. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12254	SEVERE	sGget server's configuration XML.	Server Name error message	Unable to get server's configuration XML due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-12255	SEVERE	sGget server's configuration XML.	Server Name error message	Unable to get server's configuration XML due the data parsing error.	Look under console log for more information.
CONSOLE-12261	INFO	Attempt to set server's configuration XML.	Server Name	Click on OK button in server's server configuration XML profile page.	
CONSOLE-12262	INFO	Server's configuration XML is modified.	Server Name	Click on OK button in server's server configuration XML profile page.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-12263	SEVERE	set server's configuration XML.	Server Name error message	Unable to set server's configuration XML. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
CONSOLE-12264	SEVERE	sGset server's configuration XML.	Server Name error message	Unable to set server's configuration XML due the SMS API error.	Look under service management SDK log for more information.
CONSOLE-13001	INFO	Attempt to search for agents	base realm agent type search pattern search size limit search time limit	Click on Search button in agent search view.	
CONSOLE-13002	INFO	Searching for agents succeeded	base realm agent type search pattern search size limit search time limit	Click on Search button in agent search view.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-13003	SEVERE	Searching for agents failed	base realm agent type search pattern search size limit search time limit error message	Unable to perform search operation on agents under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-13011	INFO	Attempt to delete agents	base realm agent names	Click on Delete button in agent home page.	
CONSOLE-13012	INFO	Agents are deleted	base realm agent names	Click on Delete button in agent home page.	
CONSOLE-13013	SEVERE	Deletion of agents failed	base realm agent names error message	Unable to perform delete operation on agents under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-13021	INFO	Attempt to search for agent groups	base realm agent type search pattern search size limit search time limit	Click on Search button in agent search view.	

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-13022	INFO	Searching for agent groups succeeded	base realm agent type search pattern search size limit search time limit	Click on Search button in agent search view.	
CONSOLE-13023	SEVERE	Searching for agent groups failed	base realm agent type search pattern search size limit search time limit error message	Unable to perform search operation on agent groups under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-13031	INFO	Attempt to delete agent groups	base realm agent group names	Click on Delete button in agent home page.	
CONSOLE-13032	INFO	Agent groups are deleted	base realm agent group names	Click on Delete button in agent home page.	
CONSOLE-13033	SEVERE	Deletion of agent groups failed	base realm agent group names error message	Unable to perform delete operation on agents under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-13041	INFO	Attempt to create agent	base realm agent name agent type	Click on New button in agent home page.	
CONSOLE-13042	INFO	Agent is created	base realm agent name agent type	Click on New button in agent home page.	
CONSOLE-13043	SEVERE	Creation of agent failed	base realm agent name agent type error message	Unable to perform create agent. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-13051	INFO	Attempt to create agent group	base realm agent group name agent type	Click on New button in agent home page.	
CONSOLE-13052	INFO	Agent group is created	base realm agent group name agent type	Click on New button in agent home page.	
CONSOLE-13053	SEVERE	Creation of agent group failed	base realm agent group name agent type error message	Unable to perform create agent group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.

TABLE 10–4 Log Reference Document for ConsoleLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
CONSOLE-13061	INFO	Attempt to get agent attribute values	agent universal Id	Visit agent profile page.	
CONSOLE-13062	INFO	Agent attribute values is retrieved.	agent universal Id	Visit agent profile page.	
CONSOLE-13063	SEVERE	Unable to get agent attribute values	agent universal Id error message	Unable to perform get agent attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
CONSOLE-13071	INFO	Attempt to set agent attribute values	agent universal Id	Click on save button in agent profile page.	
CONSOLE-13072	INFO	Agent attribute values is retrieved.	agent universal Id	Click on save button in agent profile page.	
CONSOLE-13073	SEVERE	Unable to set agent attribute values	agent universal Id error message	Unable to perform set agent attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.

Circle of Trust

TABLE 10–5 Log Reference Document for COTLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
COT-1	INFO	Invalid circle of trust name.	Realm or organization name Circle of Trust Name	Accessing the circle of trust.	Check the name and retry accessing the circle of trust.
COT-2	INFO	Configuration error modifying the circle of trust.	Error message Name of the circle of trust Realm or organization name	Modifying the circle of trust.	Check COT debug , fmCOT, for more detailed error message.
COT-3	INFO	Error retreiving all circle of trusts.	Error message Realm or organization name	Getting all circle of trust.	Check configuration; check debug for more detailed error message.
COT-4	INFO	Invalid name , error creating the circle of trust.	Realm or organization name	Creating the circle of trust.	Check the name to create circle of trust descriptor.
COT-5	INFO	Circle of Trust exists.	Name of the circle of trust Realm or organization name	Creating the circle of trust.	Create Circle of Trust with a unique name.
COT-6	INFO	Circle of Trust Type is invalid	Realm or organization name Circle of Trust Type	Creating the circle of trust.	The values for Circle of Trust type are IDFF , SAML2. Create Circle of Trust using either of these values.

TABLE 10–5 Log Reference Document for COTLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
COT-7	INFO	Configuration error while creating circle of trust.	Error message Entity ID Realm or organization name	Create circle of trust.	Check the fmCOT debug file for detailed errors.
COT-8	INFO	Circle of trust created.	Name of the circle of trust Realm or organization name	Creating the circle of trust.	
COT-9	INFO	Circle of Trust name is null, error adding to circle of trust.	Realm or organization name	Adding to the circle of trust.	Check the name of the circle of trust.
COT-10	INFO	Entity Identifier is null , cannot add entity to circle of trust	Realm or organization name	Adding to the circle of trust.	Check the value of entity id.
COT-11	INFO	Error adding entity to the circle of trust.	Error message Name of the circle of trust Entity Id Realm or organization name	Adding entity to circle of trust.	Check COT debug for more detailed error message.
COT-12	INFO	Null circle of trust name.	Realm or organization name	Removing member from the circle of trust.	Check the name of the circle of trust.
COT-13	INFO	Null entity identifier.	Name of the circle of trust Realm or organization name	Removing member from the circle of trust.	Check the value of the entity identifier.

TABLE 10–5 Log Reference Document for COTLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
COT-14	INFO	Error while removing entity from the circle of trust.	Error message Name of the circle of trust Entity Id Realm or organization name	Removing entity identifier from the circle of trust.	Check COT debug for more detailed error message.
COT-15	INFO	Null circle of trust name.	Realm or organization name	Listing entities in Circle of Trust	Check the name of the circle of trust.
COT-16	INFO	Error listing providers in the circle of trust.	Error message Name of the circle of trust Realm or organization name	Listing providers in the circle of trust.	Check COT debug for more detailed error message.
COT-17	INFO	Error while deleting the circle of trust.	Error message Name of the circle of trust Realm or organization name	Deleting the circle of trust.	Check COT debug for more detailed error message.
COT-18	INFO	Invalid name, cannot delete circle of trust.	Circle of Trust Name Realm or organization name	Deleting the circle of trust.	Check the circle of trust name and retry deletion.
COT-19	INFO	Cannot delete circle of trust which has entities.	Circle of Trust Name Realm or organization name	Deleting the circle of trust.	Remove all entities from the circle of trust and retry deletion.

TABLE 10–5 Log Reference Document for COTLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
COT-20	INFO	Invalid type cannot delete circle of trust.	Realm or organization name Circle of Trust Name Circle of Trust Type	Deleting the circle of trust.	Specify correct Circle of Trust type and retry delete.
COT-21	INFO	Circle of trust deleted.	Name of the circle of trust Realm or organization name	Deleting the circle of trust.	
COT-22	FINE	Retrieved the circle of trust from cache.	Name of the circle of trust Realm or organization name	Retreived the circle of trust from cache.	
COT-23	INFO	Error while getting the circle of trust from data store.	Error message Name of the circle of trust Realm or organization name	Retreiving the circle of trust	Check configuration check debug for more detailed error message.
COT-24	INFO	Error determining an entity is in a circle of trust.	Error message Name of the circle of trust ID of an entity Realm or organization name	Determining an entity is in a circle of trust.	Check debug for more detailed error message.
COT-25	INFO	Retrieved the circle of trust descriptor.	Name of the circle of trust Realm or organization name	Retrieving the circle of trust under a realm.	

Liberty ID-FF

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-14	INFO	Write Account Federation Info	user DN federation info key federation info value	Acccount Federation Info with key was added to user	
IDFF-15	INFO	Remove Account Federation Info	user DN provider id existing federation info key	Account federation info with key and provider ID was removed from user	
IDFF-16	FINER	Create Assertion	assertion id or string	Assertion Created	
IDFF-18	INFO	Logout Request processing failed.	message	Logout Request processing failed	
IDFF-19	INFO	Termination request processing failed	message	Termination request processing failed	
IDFF-20	INFO	Failed in creating SOAP URL End point.	soap end point url	Failed in creating SOAP URL End point	
IDFF-21	INFO	Mismatched AuthType and the protocol (based on SOAPUrl).	protocol authentication type	AuthType and the protocol (based on SOAPUrl) do not match.	
IDFF-22	INFO	Wrong Authentication type	authentication type	Wrong Authentication type	
IDFF-23	FINER	SAML SOAP Receiver URL	soap url	SAML SOAP Receiver URL	
IDFF-24	INFO	SOAP Response is Invalid	message	SOAP Response is Invalid.	

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-25	INFO	Assertion is invalid	message	This Assertion is invalid	
IDFF-26	INFO	Single SignOn Failed	message	Single SignOn Failed	
IDFF-27	INFO	Redirect to URL after granting access.	redirect url	Redirecting to URL after granting access.	
IDFF-28	INFO	Authentication Response is missing	message	Authentication Response not found	
IDFF-29	INFO	Account Federation Failed	message	Account Federation Failed	
IDFF-30	INFO	SSOToken Generation Failed	message	Failed to generate SSOToken	
IDFF-31	INFO	Authentication Response is invalid	invalid authentication response	Authentication Response is invalid	
IDFF-32	INFO	Authentication Request processing failed	message	Authentication Request processing failed.	
IDFF-33	INFO	Signature Verification Failed.	message	Signature Verification Failed.	
IDFF-34	INFO	Created SAML Response	sending saml response to remote server's IP address saml response or response ID and InResponseTo ID	Created SAML Response	
IDFF-35	FINER	Redirect URL	redirect url	Redirect to :	

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-36	INFO	Common Domain Service Information not found	message	Common Domain Service Information not found.	
IDFF-37	INFO	Provider is not trusted	provider id	Provider is not trusted.	
IDFF-38	INFO	Authentication Request is invalid	message	Authentication Request is invalid	
IDFF-39	INFO	Account Federation Information not found for user	user name	Account Federation Information not found for user :	
IDFF-40	INFO	User not found.	user name	User not found.	
IDFF-41	INFO	Logout profile not supported.	logout profile	Logout profile not supported.	Verify metadata is correct.
IDFF-42	INFO	Logout is successful.	user name	Logout is successful.	
IDFF-43	INFO	Logout failed to redirect due to incorrect URL.	message	Logout failed to redirect due to incorrect URL.	
IDFF-44	INFO	Logout request not formed properly.	user name	Logout request not formed properly.	
IDFF-45	INFO	Failed to get Pre/Logout handler.	logout url	Failed to get Pre/Logout handler.	
IDFF-46	INFO	Single logout failed.	user name	Single logout failed.	
IDFF-47	INFO	Failed to create SPProvidedNameIdentifier.	message	Failed to create SPProvidedNameIdentifier.	
IDFF-48	INFO	Invalid Signature.	message	Invalid Signature.	
IDFF-49	INFO	Federation Termination failed.	user name	Federation Termination failed. Cannot update account.	

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-50	FINER	Federation Termination succeeded.	userDN	Federation Termination succeeded. User account updated.	
IDFF-51	INFO	Response is Invalid	saml response	SAML Response is Invalid.	
IDFF-52	INFO	Invalid Provider Registration.	provider id Realm or Organization Name	Invalid Provider.	
IDFF-61	INFO	Error getting Configuration instance.	message	Trying to initialize IDFF Metadata configuration.	Check if the Data Repository has the IDFFMetaData Service. If it is not present then it wil need to be loading using the FM Administration command. Check the Administration Guide on how to load services.
IDFF-62	INFO	EntityDescriptor is null.	message	Trying to create EntityDescriptor.	Pass a valid non-null EntityDescriptorElement object to the IDFFMetaManager:createEn method.
IDFF-63	INFO	Entity Identifier in the EntityDescriptor is null.	message	Trying to create, modify, retrieve or delete EntityDescriptor or extended Entity Config.	The EntityDescriptor Element passed should have the Entity Identifier , this is the "providerID" attribute in the IDFF MetaData schema.

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-64	INFO	Creating of Entity Descriptor succeeded.	Entity ID Realm or Organization Name	EntityDescriptor is stored in the data repository.	
IDFF-65	INFO	Storing of IDFF Meta Data in the repository failed.	Entity ID Realm or Organization Name	Trying to create EntityDescriptor.	Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors. Check if the data repository exists and is accessible. Check if the IDFF Meta Data Service exists in the data repository.
IDFF-66	INFO	Unsupported operation.	message	Trying to create, modify or delete EntityDescriptor or extended EntityConfig.	Check the System Configuration Implementation to find out how IDFF Meta Data can be stored in the repository.
IDFF-67	INFO	The EntityDescriptor object is not valid.	Entity ID Realm or Organization Name	Trying to retrieve or modify EntityDescriptor.	Check the EntityDescriptor Element is valid and follows the IDFF Standard Meta Data Schema Description.
IDFF-68	INFO	Retrieval of Entity Configuration failed.	Entity ID Realm or Organization Name	EntityDescriptor is retrieved.	Check if the entity identifier is correct.

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-69	INFO	Retrieval of Entity Descriptor succeeded.	Entity ID Realm or Organization Name	Entity Configuration is returned to the requester.	
IDFF-70	INFO	Storing of Entity Configuration failed.	Entity ID Realm or Organization Name	Trying to modify IDFF Standard Meta data.	Check if the entity identifier is correct. Check if the data repository exists and is accessible.
IDFF-71	INFO	Modifying Entity Descriptor succeeded.	Entity ID Realm or Organization Name	Entity Descriptor is modified in the data repository.	
IDFF-72	INFO	Deleting of IDFF Standard Meta Data succeeded.	Entity ID Realm or Organization Name	IDFF Standard Meta data for the entity is deleted in the data repository.	
IDFF-73	INFO	Deleting of Standard Metadata for entity identifier failed.	Entity ID Realm or Organization Name	Trying to delete IDFF Standard Meta data for the entity.	Check if the entity identifier is correct. Check if the data repository exists and is accessible
IDFF-74	INFO	Extended Entity Configuration is null.	message	Trying to create IDFF extended Meta data.	Check the validity of the extended entity configuration.
IDFF-75	INFO	Entity Configuration could not be found.	Entity ID Realm or Organization Name	Trying to create IDFF extended Meta data.	Check the validity of the entity configuration.

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-76	INFO	Creation of Extended Entity Configuration failed since it already exists.	Entity ID Realm or Organization Name	Trying to create IDFF extended Meta data.	Cannot create entity configuration if it already exists. If new attributes are to be set in the extended entity configuration then use the setConfiguration method or delete the existing entity configuration and then try create again.
IDFF-77	INFO	Failed to get entity configuration.	Entity ID Realm or Organization Name	Trying to retrieve IDFF extended Meta data.	Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors.
IDFF-78	INFO	Retrieval of Entity Configuration succeeded.	Entity ID Realm or Organization Name	Entity Configuration is retrieved from the data repository	
IDFF-79	INFO	Extended Entity Configuration was modified.	Entity ID Realm or Organization Name	Extended Entity Configuration is modified in the data repository	
IDFF-80	INFO	Failed to modify Extended Entity Configuration.	Entity ID Realm or Organization Name	Extended Entity Configuration is modified in the data repository	Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors.
IDFF-81	INFO	Extended Entity Configuration was created.	Entity ID Realm or Organization Name	Extended Entity Configuration is stored in the data repository	

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-82	INFO	Storing of IDFF Extended Configuration in the repository failed.	Entity ID Realm or Organization Name	Trying to create Extended Entity Configuration.	Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors. Check if the data repository exists and is accessible. Check if the IDFF Meta Data Service exists in the data repository.
IDFF-83	INFO	The Extended Entity Configuration is invalid.	Entity ID Realm or Organization Name	Trying to create, modify or retrieve Extended Entity Configuration.	Check the Extended Entity Configuration is valid and retry creating the entity config.
IDFF-84	INFO	Retrieve all Entity Descriptors succeeded.	message	Retrieve all Entity Descriptors	
IDFF-85	INFO	Failed to get all Entity Descriptors.	message	Retrieve all Entity Descriptors	Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors. Check if the data repository exists and is accessible. Check if the IDFF Meta Data Service exists in the data repository.
IDFF-86	INFO	Retrieve names of all Entities.	message	Retrieve names of all Entities.	

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-87	INFO	Failed to get names for all Entities.	message	Retrieving names of all Entities.	Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors. Check if the data repository exists and is accessible. Check if the IDFF Meta Data Service exists in the data repository.
IDFF-88	INFO	Retrieve all hosted Entities succeeded.	message	Retrieving all hosted Entities.	
IDFF-89	INFO	Failed to get all hosted Entities.	message	Retrieving all hosted Entities.	Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors. Check if the data repository exists and is accessible. Check if the IDFF Meta Data Service exists in the data repository.
IDFF-90	INFO	Retrieval of all remote Entities succeeded.	message	Retrieve all remote Entities.	

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-91	INFO	Failed to get all remote Entities.	message	Retrieving all remote Entities.	Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors. Check if the data repository exists and is accessible. Check if the IDFF Meta Data Service exists in the data repository.
IDFF-92	INFO	Retrieval of all hosted services providers succeeded.	message	Retrieving all hosted services providers.	
IDFF-93	INFO	Retrieval of all remote services providers succeeded.	message	Retrieve all remote services providers.	
IDFF-94	INFO	Retrieval of all hosted identity providers succeeded.	message	Retrieve all hosted identity providers.	
IDFF-95	INFO	Retrieval of all remote identity providers succeeded.	message	Retrieve all remote identity providers.	
IDFF-96	INFO	Checking Affiliation member succeeded.	Entity ID Affiliation ID Realm or Organization Name	Checks if the provider is a member of the Affiliation.	

TABLE 10–6 Log Reference Document for IDFFLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
IDFF-97	INFO	No entity configuration to delete.	Entity ID Realm or Organization Name	Delete Entity Configuration.	Check the entityID to make sure the Entity Configuration does exist.
IDFF-98	INFO	Failed to delete entity configuration.	Entity ID Realm or Organization Name	Delete Entity Configuration.	Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors. Check if the data repository exists and is accessible. Check if the IDFF Meta Data Service exists in the data repository.
IDFF-99	INFO	Entity configuration deleted successfully.	Entity ID Realm or Organization Name	Delete Entity Configuration.	
IDFF-100	INFO	Entity does not exist.	Entity ID Realm or Organization Name	Delete Entity Descriptor.	Check to make sure you have the right entity ID. Check if the data repository exists and is accessible. Check if the IDFF Meta Data Service exists in the data repository.

Liberty ID-WSF

TABLE 10–7 Log Reference Document for LibertyLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
LIBERTY-1	INFO	Unable to process SASL Request	message id authentication mechanism authorization id advisory authentication id	Unable to process SASL Request.	
LIBERTY-2	INFO	SASL Response Ok	message id authentication mechanism authorization id advisory authentication id	SASL Response Ok.	
LIBERTY-3	INFO	Return SASL Authenticaton Response	message id authentication mechanism authorization id advisory authentication id	Returned SASL Response , continue Authentication.	
LIBERTY-4	INFO	User not found in Data store	user name	User not found in Data store	
LIBERTY-5	INFO	User found in Data Store	user name	User found in Data Store	
LIBERTY-6	INFO	Cannot locate user from resourceID	resourceID	Cannot locate user from resourceID	
LIBERTY-7	INFO	Successfully updated user profile	user name	Successfully updated user profile	

TABLE 10–7 Log Reference Document for LibertyLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
LIBERTY-8	INFO	UnAuthorized. Failed to Query Personal Profile Service	resource id	Failed to Query Personal Profile Service	
LIBERTY-9	INFO	Interaction Failed	resource id	Interaction with Personal Profile Service Failed	
LIBERTY-10	INFO	Successfully queried PP Service	resource id	Personal Profile Service Query Succeeded	
LIBERTY-11	INFO	Modify Failure	resource id	Failed to modify Personal Profile Service	
LIBERTY-12	INFO	Modify Success	resource id	Personal Profile Service Successfully modified.	
LIBERTY-13	INFO	Interaction Successful	successful interaction message	Successful interaction with Personal Profile Service	
LIBERTY-14	INFO	Sending Message	request message id	Sending SOAP Request Message to WSP.	
LIBERTY-15	INFO	Returning Response Message	response message id request message id	Returning Response Message for SOAP Request.	
LIBERTY-16	INFO	Resending Message	message id	Resending SOAP Request Message to WSP	
LIBERTY-17	INFO	Interaction manager redirecting user agent to interaction service	request message id	Interaction manager redirecting user agent to interaction service	

TABLE 10–7 Log Reference Document for LibertyLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
LIBERTY-18	INFO	Interaction manager returning response element	message id reference message id cache entry status	Interaction manager returning response element	
LIBERTY-19	INFO	Interaction query presented to user agent	message id	Interaction query presented to user agent	
LIBERTY-20	INFO	User agent responded to interaction query	message id	User agent responded to interaction query	
LIBERTY-21	INFO	User agent redirected back to SP	message id	User agent redirected back to SP	
LIBERTY-22	INFO	Webservices Success	message id handler key	Webservices success.	
LIBERTY-23	INFO	Webservices Failure	error message	Webservices Failure.	

Logging

TABLE 10–8 Log Reference Document for LoggingLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
LOG-1	INFO	Logging Started - New Logger	current location	Logging started by getting a new Logger.	
LOG-2	INFO	Logging Terminated - Server Stopped	current location	Logging terminated by server shutdown.	

TABLE 10–8 Log Reference Document for LoggingLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
LOG-3	INFO	Logging Started - Configuration Change	old location new location old backend new backend old security status new security status old status new status old level new level	Logging started after logging configuration change.	
LOG-4	INFO	Logging Terminated - Configuration Change	old location new location old backend new backend old security status new security status old status new status old level new level	Logging terminated by logging configuration change.	

Policy

TABLE 10–9 Log Reference Document for PolicyLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
POLICY-1	INFO	Evaluating policy succeeded	policy name realm name service type name resource name action names policy decision	Evaluating policy.	
POLICY-2	INFO	Getting protected policy resources succeeded	principal name resource name protecting policies	Getting protected policy resources.	
POLICY-3	INFO	Creating policy in a realm succeeded	policy name realm name	Creating policy in a realm.	
POLICY-4	INFO	Modifying policy in a realm succeeded	policy name realm name	Modifying policy in a realm.	
POLICY-5	INFO	Removing policy from a realm succeeded	policy name realm name	Removing policy from a realm.	
POLICY-6	INFO	Policy already exists in the realm	policy name realm name	Creating policy in the realm.	
POLICY-7	INFO	Creating policy in a realm failed	policy name realm name	Creating policy in a realm.	Check if the user has privilege to create a policy in the realm.
POLICY-8	INFO	Replacing policy in a realm failed	policy name realm name	Replacing policy in a realm.	Check if the user has privilege to replace a policy in the realm.

TABLE 10–9 Log Reference Document for PolicyLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
POLICY-81	INFO	Did not replace policy - A diifferent policy with the new name already exists in the realm	new policy name realm name	Replacing policy in a realm	
POLICY-9	INFO	Removing policy from a realm failed	policy name realm name	Removing policy from a realm.	Check if the user has privilege to remove a policy from the realm.
POLICY-10	INFO	Computing policy decision by an administrator succeeded	admin name principal name resource name policy decision	Computing policy decision by an administrator.	
POLICY-11	INFO	Computing policy decision by an administrator ignoring subjects succeeded	admin name resource name policy decision	Computing policy decision by an administrator ignoring subjects.	

SAML 1.x

TABLE 10–10 Log Reference Document for SAMLLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML-1	INFO	New assertion created	message id Assertion ID or Assertion if log level is LL_FINER	Browser Artifact Profile Browser POST Profile Create Assertion Artifact Authentication Query Attribute Query Authorization Decision Query	
SAML-2	INFO	New assertion artifact created	message id Assertion Artifact ID of the Assertion corresponding to the Artifact	Browser Artifact Profile Creating Assertion Artifact	
SAML-3	FINE	Assertion artifact removed from map	message id Assertion Artifact	SAML Artifact Query Assertion artifact expires	
SAML-4	FINE	Assertion removed from map	message id Assertion ID	SAML Artifact Query Assertion expires	
SAML-5	INFO	Access right by assertion artifact verified	message id Assertion Artifact	SAML Artifact Query	

TABLE 10–10 Log Reference Document for SAMLLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML-6	INFO	Authentication type configured and the actual SOAP protocol do not match.	message id	SAML SOAP Query	Login to console, go to Federation, then SAML, edit the Trusted Partners Configuration, check the selected Authentication Type field, make sure it matches the protocol specified in SOAP URL field.
SAML-7	INFO	Invalid authentication type	message id	SAML SOAP Query	Login to console, go to Federation, then SAML, edit the Trusted Partners Configuration, select one of the values for Authentication Type field, then save.
SAML-8	FINE	Remote SOAP receiver URL	message id SOAP Receiver URL	SAML SOAP Query	
SAML-9	INFO	No assertion present in saml response	message id SAML Response	SAML Artifact Query	Contact remote partner on what's wrong
SAML-10	INFO	Number of assertions in SAML response does not equal to number of artifacts in SAML request.	message id SAML Response	SAML Artifact Query	Contact remote partner on what's wrong
SAML-11	INFO	Artifact to be sent to remote partner	message id SAML Artifact	SAML Artifact Query	

TABLE 10–10 Log Reference Document for SAMLLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML-12	INFO	Wrong SOAP URL in trusted partner configuration	message id	SAML Artifact Query	Login to console, go to Federation, then SAML, edit the Trusted Partners Configuration, enter value for SOAP URL field, then save.
SAML-13	FINE	SAML Artifact Query SOAP request	message id SAML Artifact Query message	SAML Artifact Query	
SAML-14	INFO	No reply from remote SAML SOAP Receiver	message id	SAML Artifact Query	Check remote partner on what's wrong
SAML-15	FINE	SAML Artifact Query response	message id SAML Artifact Query response message	SAML Artifact Query	
SAML-16	INFO	No SAML response inside SOAP response	message id	SAML Artifact Query	Check remote partner on what's wrong
SAML-17	INFO	XML signature for SAML response is not valid	message id	SAML Artifact Query	Check remote partner on what's wrong on XML digital signature
SAML-18	INFO	Error in getting SAML response status code	message id	SAML Artifact Query	Check remote partner on what's wrong on response status code
SAML-19	INFO	TARGET parameter is missing from the request	message id	SAML Artifact Profile SAML POST Profile	Add "TARGET=target_url" as query parameter in the request

TABLE 10–10 Log Reference Document for SAMLLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML-20	INFO	Redirection URL in SAML artifact source site	message id target redirection URL SAML response message in case of POST profile and log level is LL_FINER	SAML Artifact Profile source SAML POST Profile source	
SAML-21	INFO	The specified target site is forbidden	message id target URL	SAML Artifact Profile source SAML POST Profile source	TARGET URL specified in the request is not handled by any trusted partner, check your TARGET url, make sure it matches one of the Target URL configured in trusted partner sites
SAML-22	INFO	Failed to create single-sign-on token	message id	SAML Artifact Profile destination SAML POST Profile destination	Authentication component failed to create SSO token, please check authentication log and debug for more details
SAML-23	INFO	Single sign on successful, access to target is granted	message id Response message in case of POST profile and log levele is LL_FINER or higher	SAML Artifact Profile destination SAML POST Profile destination	
SAML-24	INFO	Null servlet request or response	message id	SAML Artifact Profile SAML POST Profile	Check web container error log for details

TABLE 10–10 Log Reference Document for SAMLLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML-25	INFO	Missing SAML response in POST body	message id	SAML POST Profile destination	Check with remote SAML partner to see why SAML response object is missing from HTTP POST body
SAML-26	INFO	Error in response message	message id	SAML POST Profile destination	Unable to convert encoded POST body attribute to SAML Response object, check with remote SAML partner to see if there is any error in the SAML response create, for example, encoding error, invalid response sub-element etc.
SAML-27	INFO	Response is not valid	message id	SAML POST Profile destination	recipient attribute in SAML response does not match this site's POST profile URL Response status code is not success
SAML-28	INFO	Failed to get an instance of the message factory	message id	SAML SOAP Receiver init	Check your SOAP factory property (javax.xml.soap.MessageFac to make sure it is using a valid SOAP factory implementation

TABLE 10–10 Log Reference Document for SAMLLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML-29	INFO	Received Request from an untrusted site	message id Remote site Hostname or IP Address	SAML SOAP Queries	Login to console, go to Federation, then SAML service, edit the Trusted Partners Configuration, check the Host List field, make sure remote host/IP is one the values. In case of SSL with client auth, make sure Host List contains the client certificate alias of the remote site.
SAML-30	INFO	Invalid request from remote partner site	message id and request hostname/IP address return response	SAML SOAP Queries	Check with administrator of remote partner site
SAML-31	FINE	Request message from partner site	message id and request hostname/IP address request xml	SAML SOAP Queries	
SAML-32	INFO	Failed to build response due to internal server error	message id	SAML SOAP Queries	Check debug message to see why it is failing, for example, cannot create response status, major/minor version error, etc.
SAML-33	INFO	Sending SAML response to partner site	message id SAML response or response id	SAML SOAP Queries	

TABLE 10–10 Log Reference Document for SAMLLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML-34	INFO	Failed to build SOAP fault response body	message id	SAML SOAP Queries	Check debug message to see why it is failing, for example, unable to create SOAP fault, etc.

SAMLv2

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-1	INFO	Invalid Service Provider Identifier	Service Provider Entity Identifier	Invalid Service Provider,cannot process request	Check the Service Provider Name.
SAML2-2	INFO	Invalid Identity Provider Identifier	Identity Provider Entity Identifier	Invalid Identity Provider,cannot process request	Check the Identity Provider Name.
SAML2-3	INFO	Unable to retreive Service Provider Metadata.	Service Provider Entity Identifier	Cannot retrieve Service Provider Metadata	Check the Data Store is accessible . Check the Realm name. Check the Service Provider Entity Identifier.
SAML2-4	INFO	Unable to retrieve Identity Provider Metadata.	Identity Provider Entity Identifier	Cannot retreive Identity Provider Metadata	Check the Data Store is accessible . Check the Realm name. Check the Identity Provider Entity Identifier.

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-5	INFO	Unable to retrieve SingleSignOnService URL.	Identity Provider Entity Identifier	Error retreiving SingleSignOnService URL.	Check the Data Store is accessible . Check the Realm name. Check the Identity Provider Entity Identifier.
SAML2-6	INFO	Redirecting to SingleSignOnService URL	SingleSignOnService URL	Sending Authentication Request by redirecting to Single SignOn Service URL.	
SAML2-7	INFO	Unable to retrieve Response using Response ID after local login.	Response ID	Response doesn't exist in the SP cache.	Check the SP cache clean up interval configuration.
SAML2-8	INFO	Unable to retrieve Artifact from HTTP Request.		SAMLart is missing from HTTP Request	Check with sender. Check web container server log.
SAML2-9	INFO	Received Artifact from HTTP Request.	Artifact value	Received Artifact from HTTP Request in the process of Single Sign On using Artifact Profile.	
SAML2-10	INFO	Unable to find Identity Provider Entity ID based on the SourceID in Artifact.	Artifact value Realm or organization name	No matching Identity Provider Entity ID found in meta data configuration.	Check if Identity Provider's meta data is loaded.

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-11	INFO	Unable to load Identity Provider's meta data.	Realm or organization name Identity Provider Entity ID	Unable to load Identity Provider's meta data.	Check Identity Provider Entity ID. Check Realm or organization name. Check if the identity provider's meta is loaded.
SAML2-12	INFO	Unable to find Identity Provider's Artifact resolution service URL.	Identity Provider Entity ID	Artifact resolution service URL is not defined in Identity Provider's metadata.	Check Identity Provider's meta data.
SAML2-13	INFO	Unable to create ArtifactResolve.	Hosted Service Provider Entity ID Artifact value	Error when creating ArtifactResolve instance.	Check implementation of ArtifactResolve.
SAML2-14	INFO	Unable to obtain response from SOAP communication with Identity Provider's artifact resolution service.	Hosted Service Provider Entity ID Identity Provider's Artifact Resolution Service URL	Error in SOAP communication.	Check Identity Provider's Artifact Resolution Service URL. Check SOAP message authentication requirements for Identity Provider's Artifact Resolution Service.

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-15	INFO	Obtained response using artifact profile.	Hosted Service Provider Entity ID Remote Identity Provider Entity ID Artifact value Response xml String if the log level was set to LL_FINE at run time	Single Sign On using Artifact Profile.	
SAML2-16	INFO	Unable to obtain Artifact Response due to SOAP error.	Identity Provider Entity ID	Error in SOAP communication.	Check configuration for Identity Provider
SAML2-17	INFO	Received SOAP Fault instead of Artifact Response.	Identity Provider Entity ID	Error in Identity Provider's Artifact Resolution.	Check Identity Provider Check debug file for detailed fault info.
SAML2-18	INFO	Received too many Artifact Response.	Identity Provider Entity ID	Identity Provider sent more than one Artifact Response in SOAPMessage.	Check Identity Provider
SAML2-19	INFO	Unable to instantiate Artifact Response.	Identity Provider Entity ID	Error while instantiating Artifact Response.	Check Identity Provider Check debug message for detailed error.
SAML2-20	INFO	Unable to obtain Artifact Response from SOAP message.	Identity Provider Entity ID	No ArtifactResponse is included in SOAPMessage.	Check Identity Provider

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-21	INFO	Unable to verify signature on Artifact Response.	Identity Provider Entity ID	Error while trying to verify signature on ArtifactResponse.	Check configuration for Identity Provider Check debug file for detailed info
SAML2-22	INFO	Invalid InResponseTo attribute in Artifact Response.	Identity Provider Entity ID	InResponseTo attribute in Artifact Response is missing or doesn't match with Artifact Resolve ID.	Check with Identity Provider
SAML2-23	INFO	Invalid Issuer in Artifact Response.	Identity Provider Entity ID	Issuer in Artifact Response is missing or doesn't match with Identity Provider Entity ID.	Check with Identity Provider
SAML2-24	INFO	Invalid status code in Artifact Response.	Identity Provider Entity ID Status code if the log level was set to LL_FINE at runtime	Status in Artifact Response is missing or status code is not Success.	Check with Identity Provider
SAML2-25	INFO	Unable to instantiate Respones from Artifact Response.	Identity Provider Entity ID	Error occurred while instantiating Response.	Check debug file for detailed error.
SAML2-26	INFO	SAML Response is missing from http post.		Parameter SAMLResponse is missing from http POST.	
SAML2-27	INFO	Unable to instantiate Response from POST.		Error occurred while instantiating Response.	Check debug file for more info

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-28	INFO	Unable to decode Response.		Error occurred while decoding Response.	Check debug file for more info
SAML2-29	INFO	Obtained response using POST profile.	Response xml String if the log level was set to LL_FINE at runtime	Single Sign On using POST Profile.	
SAML2-30	INFO	Written federation info.	Username NameIDInfo value string if the log level was set to LL_FINE at runtime	Federation is done.	
SAML2-31	INFO	Redirect request to IDP.	redirection url	Single logout.	
SAML2-32	INFO	Unable to find Assertion Consumer Service URL.	meta alias	Single Sign On.	
SAML2-33	INFO	Unable to find return binding.	meta alias	Single Sign On.	
SAML2-34	INFO	Unable to post the response to target.	Assertion Consumer Service URL	Single Sign On with POST binding.	
SAML2-35	INFO	Unable to create an artifact.	IDP entity ID	Single Sign On with Artifact binding.	
SAML2-36	INFO	Received AuthnRequest.	SP entity ID IDP meta alias authnRequest xml string	Single Sign On.	
SAML2-37	INFO	Post response to SP.	SP entity ID IDP meta alias response xml string	Single Sign On with POST binding.	

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-38	INFO	Send an artifact to SP.	IDP entity ID IDP realm redirect URL	Single Sign On with Artifact binding.	
SAML2-39	INFO	Encounter invalid SOAP message in IDP.	IDP entity ID	Single Sign On with Artifact binding.	
SAML2-40	INFO	The artifact response being sent to SP.	IDP entity ID artifact string artifact response	Single Sign On with Artifact binding.	
SAML2-41	FINE	Entity descriptor obtained.	Entity ID Realm or organization name	Obtain entity descriptor.	
SAML2-42	INFO	Invaid realm while getting entity descriptor.	Realm or organization name	Obtain entity descriptor.	Check the Realm name.
SAML2-43	INFO	Obtained invalid entity descriptor.	Entity ID Realm or organization name	Obtain entity descriptor.	Delete invalid entity descriptor and import it again.
SAML2-44	INFO	Configuration error while getting entity descriptor.	Error message Entity ID Realm or organization name	Obtain entity descriptor.	Check debug message for detailed error.
SAML2-45	INFO	No entity ID while setting entity descriptor.	Realm or organization name	Set entity descriptor.	Set entity ID in entity descriptor.
SAML2-46	INFO	Invaid realm while setting entity descriptor.	Realm or organization name	Set entity descriptor.	Check the Realm name.

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-47	INFO	Entity descriptor doesn't exist while setting entity descriptor.	Entity ID Realm or organization name	Set entity descriptor.	Create entity descriptor before set.
SAML2-48	INFO	Entity descriptor was set.	Entity ID Realm or organization name	Set entity descriptor.	
SAML2-49	INFO	Configuration error while setting entity descriptor.	Error message Entity ID Realm or organization name	Set entity descriptor.	Check debug message for detailed error.
SAML2-50	INFO	Invalid entity descriptor to set.	Entity ID Realm or organization name	Set entity descriptor.	Check entity descriptor if it follows the schema.
SAML2-51	INFO	No entity ID while creating entity descriptor.	Realm or organization name	Create entity descriptor.	Set entity ID in entity descriptor.
SAML2-52	INFO	Invaid realm while creating entity descriptor.	Realm or organization name	Create entity descriptor.	Check the Realm name.
SAML2-53	INFO	Entity descriptor exists while creating entity descriptor.	Entity ID Realm or organization name	Create entity descriptor.	Delete existing entity descriptor first.
SAML2-54	INFO	Entity descriptor was created.	Entity ID Realm or organization name	Create entity descriptor.	

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-55	INFO	Configuration error while creating entity descriptor.	Error message Entity ID Realm or organization name	Create entity descriptor.	Check debug message for detailed error.
SAML2-56	INFO	Invalid entity descriptor to create.	Entity ID Realm or organization name	Create entity descriptor.	Check entity descriptor if it follows the schema.
SAML2-57	INFO	Invaid realm while deleting entity descriptor.	Realm or organization name	Delete entity descriptor.	Check the Realm name.
SAML2-58	INFO	Entity descriptor doesn't exist while deleting entity descriptor.	Entity ID Realm or organization name	Delete entity descriptor.	
SAML2-59	INFO	Entity descriptor was deleted.	Entity ID Realm or organization name	Delete entity descriptor.	
SAML2-60	INFO	Configuration error while deleting entity descriptor.	Error message Entity ID Realm or organization name	Delete entity descriptor.	Check debug message for detailed error.
SAML2-61	FINE	Entity config obtained.	Entity ID Realm or organization name	Obtain entity config.	
SAML2-62	INFO	Invaid realm while getting entity config.	Realm or organization name	Obtain entity config.	Check the Realm name.

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-63	INFO	Obtained invalid entity config.	Entity ID Realm or organization name	Obtain entity config.	Delete invalid entity config and import it again.
SAML2-64	INFO	Configuration error while getting entity config.	Error message Entity ID Realm or organization name	Obtain entity config.	Check debug message for detailed error.
SAML2-65	INFO	No entity ID while setting entity config.	Realm or organization name	Set entity config.	Set entity ID in entity config.
SAML2-66	INFO	Invaid realm while setting entity config.	Realm or organization name	Set entity config.	Check the Realm name.
SAML2-67	INFO	Entity config doesn't exist while setting entity config.	Entity ID Realm or organization name	Set entity config.	Create entity descriptor before set entity config.
SAML2-68	INFO	Entity config was set.	Entity ID Realm or organization name	Set entity config.	
SAML2-69	INFO	Configuration error while setting entity config.	Error message Entity ID Realm or organization name	Set entity config.	Check debug message for detailed error.
SAML2-70	INFO	Invalid entity config to set.	Entity ID Realm or organization name	Set entity config.	Check entity config if it follows the schema.
SAML2-71	INFO	No entity ID while creating entity config.	Realm or organization name	Create entity config.	Set entity ID in entity config.

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-72	INFO	Invaid realm while creating entity config.	Realm or organization name	Create entity config.	Check the Realm name.
SAML2-73	INFO	Entity config doesn't exist while creating entity config.	Entity ID Realm or organization name	Create entity config.	Create entity descriptor before create entity config.
SAML2-74	INFO	Entity config exists while creating entity config.	Entity ID Realm or organization name	Create entity config.	Delete existing entity config first.
SAML2-75	INFO	Entity config was created.	Entity ID Realm or organization name	Create entity config.	
SAML2-76	INFO	Configuration error while creating entity config.	Error message Entity ID Realm or organization name	Create entity config.	Check debug message for detailed error.
SAML2-77	INFO	Invalid entity config to create.	Entity ID Realm or organization name	Create entity config.	Check entity config if it follows the schema.
SAML2-78	INFO	Invaid realm while deleting entity config.	Realm or organization name	Delete entity config.	Check the Realm name.
SAML2-79	INFO	Entity config doesn't exist while deleting entity config.	Entity ID Realm or organization name	Delete entity config.	Check debug message for detailed error.
SAML2-80	INFO	Entity config was deleted.	Entity ID Realm or organization name	Delete entity config.	

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-81	INFO	Configuration error while deleting entity config.	Error message Entity ID Realm or organization name	Delete entity config.	Check debug message for detailed error.
SAML2-82	INFO	Invaid realm while getting all hosted entities.	Realm or organization name	Get all hosted entities.	Check the Realm name.
SAML2-83	INFO	Configuration error while getting all hosted entities.	Error message Realm or organization name	Get all hosted entities.	Check debug message for detailed error.
SAML2-84	FINE	Obtained all hosted entities.	Error message Realm or organization name	Get all hosted entities.	
SAML2-85	INFO	Invaid realm while getting all remote entities.	Realm or organization name	Get all remote entities.	Check the Realm name.
SAML2-86	INFO	Configuration error while getting all remote entities.	Error message Realm or organization name	Get all remote entities.	Check debug message for detailed error.
SAML2-87	FINE	Obtained all remote entities.	Error message Realm or organization name	Get all remote entities.	
SAML2-88	INFO	InResponseTo attribute in Response is invalid.	Response ID	Service Provider received a Response for Single Sign On.	Check debug message for detailed error.
SAML2-89	INFO	Issuer in Response is invalid.	Hosted Entity ID Name of Realm or organization Response ID	Issuer in Response is not configured or not trusted by the hosted provider	Check configuration.

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-90	INFO	Status code in Response was not Success.	Response ID Status code (if log level is set to LL_FINE)	Service provider received a Response with wrong Status code. Most likely an error occurred at Identity Provider.	Check the status code. Contact Identity Provider if needed.
SAML2-91	INFO	Assertion in Response was not encrypted.	Response ID	Service provider requested the assertion in Response to be encrypted, but it received a Response with unencrypted assertion(s).	Check configuration. Notify Identity Provider regarding the requirement.
SAML2-92	INFO	Response had no Assertion.	Response ID	Service provider received a Response for Single Sign On, but the response contained no Assertion.	Check error code of the Response. Notify Identity Provider if needed.
SAML2-93	INFO	Issuer in Assertion is not valid.	Assertion ID	Issuer in Assertion for single sign on was not configured at service provider, or not trusted by the service provider.	Check configuration
SAML2-94	INFO	Issuer in Assertion didn't match the Issuer in Response or other Assertions in the Response.	Assertion ID	Service provider received Response which had mismatch Issuer inside the Assertion it contained.	Check debug message

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-95	INFO	Assertion is not signed or signature is not valid.	Assertion ID	Service provider requested the Assertion to be signed but the assertion received was not; or the signature on the Assertion received was not valid.	Check configuration; check debug for more detailed error message.
SAML2-96	INFO	SubjectConfirmationData had no Subject.	Assertion ID	Service provider received an Assertion whose SubjectConfirmationData had no Subject.	Check debug for the Assertion received. Contact Identity Provider if needed.
SAML2-97	INFO	SubjectConfirmationData had no Recipient.	Assertion ID	Service provider received an Assertion whose SubjectConfirmationData had no Recipient.	Check debug for the Assertion received. Contact Identity Provider if needed.
SAML2-98	INFO	Service Provider is not the intended recipient.	Assertion ID	Service provider received an Assertion. But the provider is not the intended recipient of the Assertion.	Check debug for the Assertion received. Check meta data. Contact Identity Provider if needed.
SAML2-99	INFO	Time in SubjectConfirmationData of the Assertion is invalid.	Assertion ID	The assertion service provider received had expired timewise.	Synchronize the time between service provider and identity provider. Increase the time skew attribute for the service provider in its entity config.

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-100	INFO	SubjectConfirmationData of the Assertion had NotBefore.	Assertion ID	The assertion service provider received had NotBefore.	Check debug for the Assertion received. Contact identity provider if needed.
SAML2-101	INFO	Assertion contained wrong InResponseTo attribute.	Assertion ID	InResponseTo in Assertion is different from the one in Response. Or Assertion didn't contain InResponseTo, but Response did.	Check debug for the Assertion received. Contact identity provider if needed.
SAML2-102	INFO	Assertion contained no Conditions.	Assertion ID	Conditions is missing from the Single Sign On Assertion.	Check debug for the Assertion received. Contact identity provider if needed.
SAML2-103	INFO	Assertion contained no AudienceRestriction.	Assertion ID	AudienceRestriction is missing from the Single Sign On Assertion.	Check debug for the Assertion received. Contact identity provider if needed.
SAML2-104	INFO	Assertion contained wrong Audience.	Assertion ID	This service provider was not the intended audience of the single sign on assertion.	Check debug for the Assertion received. Check meta data. Contact identity provider if needed.
SAML2-105	INFO	Found authentication assertion in the Response.	Assertion ID Subject if the log level was set to LL_FINE SesionIndex if any	Both the Response and Assertion(s) inside the Response are valid.	

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-106	INFO	Invalid SSOToken found in Request.	SSOToken value	Initiate Single Logout without SSOToken.	
SAML2-107	INFO	No entity ID is specified in Request.	EntityID value	Initiate Request without EntityID.	Specify EntityID parameter in request URL.
SAML2-108	INFO	No metaAlias is specified in Request.	MetaAlias value	Initiate Request without metaAlias.	Specify metaAlias parameter in request URL.
SAML2-109	INFO	Redirect request to authentication page.	URL to Authentication page	Initiate Request without SSOToken.	
SAML2-110	INFO	Can not decode URL encoded Query parameter.	URL encoded Query parameter	Initiate to decode incorrectly URL encoded Query parameter.	
SAML2-111	INFO	Can not instantiate MNI Response with input xml.	Input XML string for MNI Response	Initiate parse MNI Response with incorrect XML string.	
SAML2-112	INFO	Can not instantiate MNI Request with input XML.	Input XML string for MNI Request	Initiate parse MNI Request with incorrect XML string.	
SAML2-113	INFO	Can not instantiate SLO Response with input XML.	Input XML string for SLO Response	Initiate parse SLO Response with incorrect XML string.	
SAML2-114	INFO	Can not instantiate SLO Request with input XML.	Input XML string for SLO Request	Initiate parse SLO Request with incorrect XML string.	
SAML2-115	INFO	Can not varify signature in MNI Request.	MNI Request with signature	Sinature in MNI Request is incorrect.	

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-116	INFO	Can not valify signature in MNI Response.	MNI Response with signature	Sinature in MNI Response is incorrect.	
SAML2-117	INFO	Can not valify signature in SLO Request.	SLO Request with signature	Sinature in SLO Request is incorrect.	
SAML2-118	INFO	Can not valify signature in SLO Response.	SLO Response with signature	Sinature in SLO Response is incorrect.	
SAML2-119	INFO	Can not decrypt EncryptedID.	Exception message	Decrypt the incorrectly encrypted EncryptedID.	
SAML2-120	INFO	MNI Response has error status.	Status message	Requested MNI Request caused problem.	
SAML2-121	INFO	SLO Response has error status.	Status message	Requested SLO Request caused problem.	
SAML2-122	INFO	Entity Role is not specified in the request.	Entity Role value	Initiate request without Role value.	Specify Entity Role parameter in the request.
SAML2-123	INFO	Issuer in Request is invalid.	Hosted Entity ID Name of Realm or organization Request ID	Issuer in Request is not configured or not trusted by the hosted provider	Check configuration.
SAML2-124	INFO	Invaid realm while getting all entities.	Realm or organization name	Get all entities.	Check the Realm name.
SAML2-125	INFO	Configuration error while getting all entities.	Error message Realm or organization name	Get all entities.	Check debug message for detailed error.
SAML2-126	FINE	Obtained all entities.	Realm or organization name	Get all entities.	

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-127	INFO	Invalid Policy Enforcement Point (PEP) Identifier.	PEP Identifier	Cannot retrieve PEP Metadata	Provide valid PEP Identifier and retry.
SAML2-128	INFO	Invalid Policy Decision Point (PDP) Identifier.	PDP Identifier	Cannot retrieve PDP Metadata	Provide valid PDP Identifier and retry.
SAML2-129	INFO	Certificate Alias is null, cannot sign the message.	The realm from which the metadata was retreived. Entity Identifier for the Policy Decision Point.	Cannot sign the message.	Check the entity's metadata to verify the certificate alias is correct.
SAML2-130	INFO	Certificate Alias is null,cannot retreive the certificate.	The realm from which the metadata was retreived. Entity Identifier for the Policy Enforcement Point.	Cannot validate the signature in the request message.	Check the entity's metadata to verify the certificate alias is correct.
SAML2-131	INFO	Invalid Signature in Query Request.	The realm from which the metadata was retreived. Entity Identifier for the Policy Decision Point. Cert Alias used to retrieve certificate from keystore.	Cannot process the request, server will send back error to the Requester.	Check the entity's metadata to verify the certificate alias is correct. Check the certificate in the keystore for its existance and validity.
SAML2-132	INFO	Issuer in Request is invalid.	Name of Realm or organization Identity of the Issuer Hosted Entity Identifier	Issuer in Request is not configured or not trusted by the hosted provider therefore Query will fail.	Check the hosted entity configuration attribute cotlist to make sure the issuer identifier is in the list.

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-133	INFO	Unable to retreive Policy Enforcement Point (PEP) Metadata.	PEP Provider Entity Identifier	Cannot retrieve PEP Provider Metadata	Check the Data Store is accessible . Check the PEP Provider Entity Identifier.
SAML2-134	INFO	Unable to retrieve Policy Decision Point (PDP) Metadata.	PDP Provider Entity Identifier	Cannot retreive PDP Provider Metadata	Check the Data Store is accessible . Check the PDP Provider Entity Identifier.
SAML2-135	INFO	Assertion in Response not encrypted.	Identity of the Issuer Response ID	Policy Enforcement Point (PEP) Provider requested the assertion in Response to be encrypted, but it received a Response with unencrypted assertion(s).	Check PEP metadata published to the PDP. Notify Policy Decision Point (PDP) Provider regarding the requirement.
SAML2-136	INFO	Response has no Assertion.	Identity of Issuer Response ID	Policy Enforcement Point (PEP) Provider received a Response with no Assertion.	Check error code of the Response. Notify Policy Decision Point (PDP) Provider to check for errors or possible misconfiguration.

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-137	INFO	Issuer in Assertion is not valid.	Assertion Issuer Assertion ID	Issuer in Assertion was not configured at Policy Enforcement Point (PEP) provider, or not trusted by the PEP provider.	Check the configuration.
SAML2-138	INFO	Issuer in Assertion doesn't match the Issuer in Response.	Issuer Identifier in the Resposnse Issuer Identity in the Assertion	Error condition, Response will not be accepted.	Check the Policy Decision Point instance to debug the cause of the problem.
SAML2-139	INFO	Assertion is not signed or signature is not valid.	Issuer Identity in the Assertion Assertion ID	Policy Enforcement Point (PEP) provider requested the Assertion to be signed but the assertion received was not; or the signature on the Assertion received was not valid.	Check PEP metadata configuration. Check debug for more detailed error message.
SAML2-140	FINE	Request message from Query Requester	policy decision point entity descriptor SAMLv2 Query Request Message	SAMLv2 SOAP Query	

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-141	INFO	Valid Signature in Query Request.	The realm from which the metadata was retreived. Entity Identifier for the Policy Decision Point. Cert Alias used to retrieve certificate from keystore.	The Request will be processed.	
SAML2-142	INFO	Successful federation/Single Sign On.	user id NameID value	Successful federation/Single Sign On.	
SAML2-143	INFO	SAE_IDP succeeded.	SAE attributes	SAE_IDP succeeded.	
SAML2-144	INFO	SAE_IDP failed.	Error message SAE attributes	SAE_IDP failed.	
SAML2-145	INFO	SAE_IDP invoked without attributes.	Error message	SAE_IDP invoked without attributes.	Add SAE attributes to request.
SAML2-146	INFO	SAE_IDP delegated to Auth.	SAE attributes	SAE_IDP invoked but no user session.	
SAML2-147	INFO	SAE_SP succeeded.	SAE attributes	SAE_SP succeeded.	
SAML2-148	INFO	SAE_SP failed.	Error message	SAE_SP failed.	

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-149	INFO	Send a response to ECP.	Identity Provider Entity Identifier Realm or organization name Assertion Consumer Service URL SOAP message string if the log level was set to LL_FINE at run time	Received AuthnRequest.	
SAML2-150	INFO	Unable to send a response to ECP.	Identity Provider Entity Identifier Realm or organization name Assertion Consumer Service URL	Send a response to ECP.	
SAML2-151	INFO	Unable to instantiate a SOAP message sent from ECP.	Service Provider Entity Identifier	Received a response from ECP.	
SAML2-152	INFO	Received a SOAP fault from ECP.	Service Provider Entity Identifier	Received a response from ECP.	
SAML2-153	INFO	Unable to instantiate a SAML Response sent from ECP.	Service Provider Entity Identifier	Received a response from ECP.	
SAML2-154	INFO	Assertion received from ECP is not signed.	Identity Provider Entity Identifier	Received a response from ECP.	

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-155	INFO	Assertion received from ECP has invalid signature.	Identity Provider Entity Identifier	Assertion signature verification.	
SAML2-156	INFO	Received AuthnRequest from ECP.	Service Provider Entity Identifier IDP meta alias authnRequest xml string	Single Sign On.	
SAML2-157	INFO	Received HTTP request from ECP.	Service Provider Entity Identifier Realm or organization name	ECP accessed SP Resource.	
SAML2-158	INFO	Send a PAOS request to ECP.	Service Provider Entity Identifier Realm or organization name SOAP message string if the log level was set to LL_FINE at run time	Received HTTP request from ECP.	
SAML2-159	INFO	Unable to send a PAOS request to ECP.	Service Provider Entity Identifier Realm or organization name	Send a PAOS request to ECP.	
SAML2-160	INFO	Federation termination succeeded.	user id	Federation termination succeeded.	
SAML2-161	INFO	New name identifier succeeded.	user id	New name identifier succeeded.	

TABLE 10–11 Log Reference Document for SAML2LogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SAML2-162	INFO	Unknown princial in manage name ID request.	Manage Name ID request XML	Unable to find old name id in the management name id request.	
SAML2-163	INFO	Unable to terminate federation.	user id	Unable to terminate federation.	
SAML2-164	INFO	Unable to verify signature in Single Sign-On Response using POST binding.	Identity Provider Entity ID	Error while trying to verify signature in Response.	Check Identity Provider metadata Check debug file for detailed info

Session

TABLE 10–12 Log Reference Document for SessionLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SESSION-1	INFO	Session is Created	User ID	User is authenticated.	
SESSION-2	INFO	Session has idle timedout	User ID	User session idle for long time.	
SESSION-3	INFO	Session has Expired	User ID	User session has reached its maximun time limit.	
SESSION-4	INFO	User has Logged out	User ID	User has logged out of the system.	
SESSION-5	INFO	Session is Reactivated	User ID	User session state is active.	
SESSION-6	INFO	Session is Destroyed	User ID	User session is destroyed and cannot be referenced.	

TABLE 10–12 Log Reference Document for SessionLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
SESSION-7	INFO	Session's property is changed.	User ID	User changed session's unprotected property.	
SESSION-8	INFO	Session received Unknown Event	User ID	Unknown session event	
SESSION-9	INFO	Attempt to set protected property	User ID	Attempt to set protected property	
SESSION-10	INFO	User's session quota has been exhausted.	User ID	Session quota exhausted	
SESSION-11	INFO	Session database used for session failover and session constraint is not available.	User ID	Unable to reach the session database.	
SESSION-12	INFO	Session database is back online.	User ID	Session database is back online..	
SESSION-13	INFO	The total number of valid sessions hosted on the OpenSSO server has reached the max limit.	User ID	Session max limit reached.	

Web Services Security

TABLE 10–13 Log Reference Document for WebServicesSecurityLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WebServicesSecurity-1	INFO	Unsupported Token Type sent to STS for Security Token creation.	Token Type sent by client to STS	Invalid or unsupported token type sent by client to STS.	Check the Token Type sent by client to STS.

TABLE 10–13 Log Reference Document for WebServicesSecurityLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WebServicesSecurity-INFO-302	INFO	Successfully created SAML 1.1 assertion by STS.	Assertion ID Issuer of this SAML assertion Service Provider for which this Assertion is created or applies to Confirmation Method Token Type Key Type	Valid parameters sent by client to STS to create SAML assetion.	
WebServicesSecurity-INFO-303	INFO	Successfully created SAML 2.0 assertion by STS.	Assertion ID Issuer of this SAML assertion Service Provider for which this Assertion is created or applies to Confirmation Method Token Type Key Type	Valid parameters sent by client to STS to create SAML assetion.	
WebServicesSecurity-INFO-304	INFO	Error during signing SAML assertion by STS.	Actual Error message	Problem in STS's Certificate or Private key.	Check the certificate of STS. Check the Private Key of STS.
WebServicesSecurity-INFO-305	INFO	Error during creation of SAML 1.1 Assertion by STS.	Actual Error message	Invalid parameters sent to create SAML 1.1 Assertion.	Check all the parameters sent to create SAML 1.1 Assertion.

TABLE 10–13 Log Reference Document for WebServicesSecurityLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WebServicesSecurity-16	INFO	Error during creation of SAML 2.0 Assertion by STS.	Actual Error message	Invalid parameters sent to create SAML 2.0 Assertion.	Check all the parameters sent to create SAML 2.0 Assertion.
WebServicesSecurity-17	INFO	Security token being created for this Identity.	Subject or Identity of the token		
WebServicesSecurity-18	INFO	Security token being created with this Attribute Map for Service Provider.	Attribute Map required by Service Provider	Service Provider needs Attributes to be populated in Security token.	
WebServicesSecurity-19	INFO	Successfully validated the incoming SOAP request.	Provider name to identify the STS service or WSP profile Security Mechanism or authentication token sent by client		
WebServicesSecurity-10	FINE	Incoming SOAP request to be validated.	Complete SOAP request		
WebServicesSecurity-11	FINE	Outgoing SOAP response to be secured.	Complete SOAP response		
WebServicesSecurity-12	INFO	Successfully secured the outgoing SOAP response.	Provider name to identify the STS service or WSP profile		
WebServicesSecurity-13	FINE	Outgoing SOAP request to be secured.	Complete SOAP request		

TABLE 10–13 Log Reference Document for WebServicesSecurityLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WebServicesSecurity14	INFO	Successfully secured the outgoing SOAP request.	Provider name to identify the STS client or WSC profile Security Mechanism or authentication token sent by client		
WebServicesSecurity15	FINE	Incoming SOAP response to be validated.	Complete SOAP response		
WebServicesSecurity16	INFO	Successfully validated the incoming SOAP response.	Provider name to identify the STS client or WSC profile		
WebServicesSecurity17	INFO	Authentication of the incoming SOAP request failed at server or WSP.	Security Mechanism or Security token sent by client	Invalid Security Mechanism or Security token sent by client.	Check Security Mechanism or Security token sent by client.
WebServicesSecurity18	INFO	Error in parsing SOAP headers from incoming SOAP request.	Actual error message	Client has sent incorrect SOAP headers.	Check SOAP headers.
WebServicesSecurity19	INFO	Error in adding Security header in outgoing SOAP request.	Actual error message	Error in adding namespaces or creating Security Header element.	Check namespaces and Secuirty Header.
WebServicesSecurity20	INFO	Signature validation failed in incoming SOAP request / response.	Actual error message	Error in signing request / response by client / server.	Check keystore and certificate used for signing.
WebServicesSecurity20	INFO	Unable to sign SOAP request or response.	Actual error message	Error in retrieving certificate from the keystore.	Check keystore configuration and certificate used for signing. Check debug file for detailed info.

TABLE 10–13 Log Reference Document for WebServicesSecurityLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WebServicesSecurity-220	INFO	Unable to encrypt SOAP request or response.	Actual error message	Error in retrieving certificate from the keystore.	Check keystore configuration and certificate used for encryption. Check debug file for detailed info.
WebServicesSecurity-230	INFO	Unable to decrypt SOAP request or response.	Actual error message	Error in retrieving certificate from the keystore.	Check keystore configuration and certificate used for decryption. Check debug file for detailed info.
WebServicesSecurity-240	INFO	Successfully retrieved Security Token from STS service.	Web Service Provider end point for which Security Token being generated Security Token Service end point to which STS client talks to Security Token Service MEX end point address End user credential (if "null" then the Identity of the generated Security token is Web Service Client, else it is owned by Authenticated End user) Key Type Token Type	All the required input data parameters are correct.	

TABLE 10–13 Log Reference Document for WebServicesSecurityLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WebServicesSecurity-25	INFO	Error in retrieving Security Token from STS service.	Actual error message	Some or more required input data parameters are not correct.	Check all the required input data parameters. Check debug file for detailed error.
WebServicesSecurity-26	SEVERE	Error in retrieving Security Token from STS service.	Actual error message	Some or more required input data parameters are not correct.	Check all the required input data parameters. Check debug file for detailed error.
WebServicesSecurity-27	SEVERE	Error during creation of SAML 1.1 Assertion by STS.	Actual Error message	Invalid parameters sent to create SAML 1.1 Assertion.	Check all the parameters sent to create SAML 1.1 Assertion. Check debug file for detailed error.
WebServicesSecurity-28	SEVERE	Error during creation of SAML 2.0 Assertion by STS.	Actual Error message	Invalid parameters sent to create SAML 2.0 Assertion.	Check all the parameters sent to create SAML 2.0 Assertion. Check debug file for detailed error.

WS-Federation

TABLE 10–14 Log Reference Document for WSFederationLogMessageIDs

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WSFederation-1	INFO	Assertion is not signed or signature is not valid.	Assertion or assertion ID Realm or organization name Assertion issuer	Service provider requested the Assertion to be signed but the assertion received was not; or the signature on the Assertion received was not valid.	Check configuration; check debug for more detailed error message.
WSFederation-2	INFO	Assertion conditions are missing notOnOrAfter attribute.	Assertion or assertion ID	The Conditions element of the assertion is missing its notOnOrAfter attribute.	Check the assertion. Contact Identity Provider if needed.
WSFederation-3	INFO	Assertion has expired.	Assertion or assertion ID Assertion notOnOrAfter time Time skew in seconds Current time	The current time is after the assertion's notOnOrAfter time plus the time skew.	Synchronize server clocks. Contact Identity Provider if needed.
WSFederation-4	INFO	Assertion conditions are missing notBefore attribute.	Assertion or assertion ID	The Conditions element of the assertion is missing its notBefore attribute.	Check the assertion. Contact Identity Provider if needed.

TABLE 10–14 Log Reference Document for WSFederationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WSFederation-5	INFO	Assertion not yet valid.	Assertion or assertion ID Assertion notBefore time Time skew in seconds Current time	The current time is before the assertion's notBefore time minus the time skew.	Synchronize server clocks. Contact Identity Provider if needed.
WSFederation-6	INFO	WS-Federation response is missing wresult.	WS-Federation response	The WS-Federation response is missing its wresult parameter.	Check the response. Contact Identity Provider if needed.
WSFederation-7	INFO	WS-Federation response is missing wctx.	WS-Federation response	The WS-Federation response is missing its wctx parameter.	Check the response. Contact Identity Provider if needed.
WSFederation-8	INFO	WS-Federation response is invalid.	WS-Federation response	The WS-Federation response is not a valid RequestSecurityTokenResponse element.	Check the response. Contact Identity Provider if needed.
WSFederation-9	INFO	Configuration error while getting entity config.	Error message MetaAlias Realm or organization name	Obtain entity config.	Check debug message for detailed error.
WSFederation-10	INFO	Can't find SP Account Mapper.	Error message Account mapper class name	Cannot get class object for SP account mapper class.	Check the configuration. Ensure that SP account mapper class name is correct and that the account mapper class is on the classpath.

TABLE 10–14 Log Reference Document for WSFederationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WSFederation-11	INFO	Can't create SP Account Mapper.	Error message Account mapper class name	Cannot create SP account mapper object.	Check the configuration. Ensure that SP account mapper class name is correct and that the account mapper class is on the classpath.
WSFederation-12	INFO	Can't create session for user.	Error message Realm or organization name User name Auth level	Cannot create session for user.	Check the configuration. Ensure that SP account mapper is finding a user in the local store.
WSFederation-13	INFO	Single sign-on completed successfully.	Assertion or assertion ID Realm or organization name User ID Authentication Level Target URL	Successful WS-Federation RP Signin Response.	
WSFederation-14	INFO	Assertion issuer is not trusted by this service provider.	Assertion or assertion ID Realm or organization name Service provider ID Target URL	Cannot create session for user.	Check the configuration. Ensure that SP account mapper is finding a user in the local store.
WSFederation-15	INFO	Assertion does not contain a subject element.	Assertion or assertion ID	Assertion does not contain a subject element.	Check the assertion. Contact Identity Provider if needed.

TABLE 10–14 Log Reference Document for WSFederationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WSFederation-16	FINE	Federation obtained.	Federation ID Realm or organization name	Obtain federation.	
WSFederation-17	INFO	Obtained invalid entity descriptor.	Entity ID Realm or organization name	Obtain entity descriptor.	Delete invalid entity descriptor and import it again.
WSFederation-18	INFO	Configuration error while getting entity descriptor.	Error message Entity ID Realm or organization name	Obtain entity descriptor.	Check debug message for detailed error.
WSFederation-19	INFO	Entity descriptor was set.	Entity ID Realm or organization name	Set entity descriptor.	
WSFederation-20	INFO	Configuration error while setting entity descriptor.	Error message Entity ID Realm or organization name	Set entity descriptor.	Check debug message for detailed error.
WSFederation-21	INFO	Invalid entity descriptor to set.	Entity ID Realm or organization name	Set entity descriptor.	Check entity descriptor if it follows the schema.
WSFederation-22	INFO	Entity descriptor was created.	Entity ID Realm or organization name	Create entity descriptor.	
WSFederation-23	INFO	Configuration error while creating entity descriptor.	Error message Entity ID Realm or organization name	Create entity descriptor.	Check debug message for detailed error.

TABLE 10–14 Log Reference Document for WSFederationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WSFederation-24	INFO	Invalid entity descriptor to create.	Entity ID Realm or organization name	Create entity descriptor.	Check entity descriptor if it follows the schema.
WSFederation-25	INFO	Entity descriptor was deleted.	Entity ID Realm or organization name	Delete entity descriptor.	
WSFederation-26	INFO	Configuration error while deleting entity descriptor.	Error message Entity ID Realm or organization name	Delete entity descriptor.	Check debug message for detailed error.
WSFederation-27	FINE	Entity config obtained.	Entity ID Realm or organization name	Obtain entity config.	
WSFederation-28	INFO	Obtained invalid entity config.	Entity ID Realm or organization name	Obtain entity config.	Delete invalid entity config and import it again.
WSFederation-29	INFO	Configuration error while getting entity config.	Error message Entity ID Realm or organization name	Obtain entity config.	Check debug message for detailed error.
WSFederation-30	INFO	No entity ID while setting entity config.	Realm or organization name	Set entity config.	Set entity ID in entity config.
WSFederation-31	INFO	Entity config was set.	Entity ID Realm or organization name	Set entity config.	

TABLE 10–14 Log Reference Document for WSFederationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WSFederation-32	INFO	Configuration error while setting entity config.	Error message Entity ID Realm or organization name	Set entity config.	Check debug message for detailed error.
WSFederation-33	INFO	Invalid entity config to set.	Entity ID Realm or organization name	Set entity config.	Check entity config if it follows the schema.
WSFederation-34	INFO	No entity ID while creating entity config.	Realm or organization name	Create entity config.	Set entity ID in entity config.
WSFederation-35	INFO	Entity config doesn't exist while creating entity config.	Entity ID Realm or organization name	Create entity config.	Create entity descriptor before create entity config.
WSFederation-36	INFO	Entity config exists while creating entity config.	Entity ID Realm or organization name	Create entity config.	Delete existing entity config first.
WSFederation-37	INFO	Entity config was created.	Entity ID Realm or organization name	Create entity config.	
WSFederation-38	INFO	Configuration error while creating entity config.	Error message Entity ID Realm or organization name	Create entity config.	Check debug message for detailed error.
WSFederation-39	INFO	Invalid entity config to create.	Entity ID Realm or organization name	Create entity config.	Check entity config if it follows the schema.

TABLE 10–14 Log Reference Document for WSFederationLogMessageIDs *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
WSFederation-40	INFO	Entity config doesn't exist while deleting entity config.	Entity ID Realm or organization name	Delete entity config.	Check debug message for detailed error.
WSFederation-41	INFO	Entity config was deleted.	Entity ID Realm or organization name	Delete entity config.	
WSFederation-42	INFO	Configuration error while deleting entity config.	Error message Entity ID Realm or organization name	Delete entity config.	Check debug message for detailed error.
WSFederation-43	INFO	Configuration error while getting all hosted entities.	Error message Realm or organization name	Get all hosted entities.	Check debug message for detailed error.
WSFederation-44	FINE	Obtained all hosted entities.	Error message Realm or organization name	Get all hosted entities.	
WSFederation-45	INFO	Configuration error while getting all remote entities.	Error message Realm or organization name	Get all remote entities.	Check debug message for detailed error.
WSFederation-46	FINE	Obtained all remote entities.	Error message Realm or organization name	Get all remote entities.	
WSFederation-47	INFO	Configuration error while getting all entities.	Error message Realm or organization name	Get all entities.	Check debug message for detailed error.
WSFederation-48	FINE	Obtained all entities.	Realm or organization name	Get all entities.	