FORGEROCK®

Reference
OpenAM 11

Mark Craig
Vanessa Richie
Mike Jang

Copyright © 2011-2017 ForgeRock AS.

Abstract

Reference documentation for OpenAM. OpenAM provides open source Authentication, Authorization, Entitlement and Federation software.

Table of Contents

Preface

This reference covers OpenAM tools, log formats, error codes, file layout, ports used, standards supported, locales supported, and configuration file semantics.

1. Who Should Use this Reference

This references is written for access management designers, developers, and administrators using OpenAM tools, logs, and configuration files. For API specifications, see the appropriate Javadoc.

2. Formatting Conventions

Most examples in the documentation are created in GNU/Linux or Mac OS X operating environments. If distinctions are necessary between operating environments, examples are labeled with the operating environment name in parentheses. To avoid repetition file system directory names are often given only in UNIX format as in `/path/to/server`, even if the text applies to `C:\path\to\server` as well.

Absolute path names usually begin with the placeholder `/path/to/`. This path might translate to `/opt/`, `C:\Program Files\`, or somewhere else on your system.

Command-line, terminal sessions are formatted as follows:

```
$ echo $JAVA_HOME
/path/to/jdk
```

Command output is sometimes formatted for narrower, more readable output even though formatting parameters are not shown in the command.

Program listings are formatted as follows:

```
class Test {
    public static void main(String [] args)  {
        System.out.println("This is a program listing.");
    }
}
```

3. Accessing Documentation Online

ForgeRock publishes comprehensive documentation online:

- The ForgeRock Knowledge Base offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.

  While many articles are visible to community members, ForgeRock customers have access to much more, including advanced information for customers using ForgeRock software in a mission-critical capacity.

- ForgeRock product documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.

4. Using the ForgeRock.org Site

The ForgeRock.org site has links to source code for ForgeRock open source software, as well as links to the ForgeRock forums and technical blogs.

If you are a *ForgeRock customer*, raise a support ticket instead of using the forums. ForgeRock support professionals will get in touch to help you.

OpenAM Command Line Tools

Table of Contents

FORGEROCK

Name

agentadmin — manage OpenAM policy agent installation

Synopsis

agentadmin {options}

Description

This command manages OpenAM policy agent installations. The **agentadmin** command requires a Java runtime environment.

Options

The following options are supported.

--install

Installs a new Agent instance.

Usage: **agentadmin --install [--useResponse | --saveResponse *file-name*]**

--useResponse

Use this option to install in silent mode by specifying all the responses in a response specified by *file-name*. When this option is used the installer runs in non-interactive mode.

--saveResponse

Use this option to save all the supplied responses to a response file specified by *file-name*.

--custom-install

Installs a new Agent instance

Usage: **agentadmin --custom-install [--useResponse | --saveResponse *file-name*]**

--useResponse

Use this option to install in silent mode by specifying all the responses in a response specified by *file-name*. When this option is used the installer runs in non-interactive mode.

--saveResponse

Use this option to save all the supplied responses to a response file specified by *file-name*.

--uninstall

Uninstalls an existing Agent instance.

Usage: **agentadmin --uninstall [--useResponse | --saveResponse *file-name*]**

`--useResponse`

> Use this option to install in silent mode by specifying all the responses in a response specified by *file-name*. When this option is used the installer runs in non-interactive mode.

`--saveResponse`

> Use this option to save all the supplied responses to a response file specified by *file-name*.

`--version`

Displays the version information.

`--uninstallAll`

Uninstalls all the agent instances.

`--migrate`

Migrate agent to newer version

`--listAgents`

Displays details of all the configured agents.

`--agentInfo`

Displays details of the agent corresponding to the specified agent ID.

Usage: **agentadmin --agentInfo *agent-id***

`--agentInfo`

Displays details of the agent corresponding to the specified *agent-id*.

Example: **agentadmin --agentInfo agent_001**

`--encrypt`

Encrypts a given string.

Usage: **agentadmin --encrypt *agent-instance password-file***

agent-instance

> Agent instance identifier. The encryption functionality requires the use of agent instance specific encryption key present in its configuration file.

password-file

> File containing the password to encrypt.

--getEncryptKey

> Generates an agent encryption key.

Examples

The following example installs an Apache HTTP Server 2.2 interactively, where Apache HTTP Server has been installed under /path/to/apache22.

```
$ ./agentadmin --install
...
----------------------------------------------
SUMMARY OF YOUR RESPONSES
----------------------------------------------
Apache Server Config Directory : /path/to/apache22/conf
OpenSSO server URL : http://openam.example.com:8080/openam
Agent URL : http://www.example.com:80
Agent Profile name : Apache Web Agent
Agent Profile Password file name : /tmp/pwd.txt


...
SUMMARY OF AGENT INSTALLATION
----------------------------
Agent instance name: Agent_001
Agent Bootstrap file location:
/path/to/web_agents/apache22_agent/Agent_001/config/
 OpenSSOAgentBootstrap.properties
Agent Configuration Tag file location
/path/to/web_agents/apache22_agent/Agent_001/config/
 OpenSSOAgentConfiguration.properties
Agent Audit directory location:
/path/to/web_agents/apache22_agent/Agent_001/logs/audit
Agent Debug directory location:
/path/to/web_agents/apache22_agent/Agent_001/logs/debug


Install log file location:
/path/to/web_agents/apache22_agent/installer-logs/audit/install.log
...
```

Name

ampassword — change passwords for the OpenAM Administrator

Synopsis

`ampassword` {options}

Description

This command allows you to change passwords held in the configuration store, and to encrypt passwords.

Options

The following options are supported.

-a | --admin [-o | --old *old-password-file* -n | --new *new-password-file*]

Change the password for `amAdmin` from the value stored in *old-password-file* to the value stored in *new-password-file*.

-p | --proxy [-o | --old *old-password-file* -n | --new *new-password-file*]

Change the password for the proxy administrator from the value stored in *old-password-file* to the value stored in *new-password-file*.

The proxy administrator password is shown encrypted in the output from **ssoadm get-svrcfg-xml**.

-e | --encrypt [*password-file*]

Display the password value provided encrypted with the key generated during OpenAM installation.

-h | --help

Display the usage message.

Examples

The following example encrypts the value `password`.

```
$ echo password > pwd.file
$ ampassword -e pwd.file
AQICkZs3qy5QUCXir9tebIEEZYGFXI2lCC4B
```

Name

amverifyarchive — check OpenAM log archives for tampering

Synopsis

amverifyarchive {options}

Description

This command checks log archive integrity.

Options

The following options are required.

-l *logName*

> Verify log files of the specified type. To specify an individual log rather than a type, provide the entire log file name.

-p *path*

> Path to log files to verify.

-u *userName*

> User who can read log files.

-w *password*

> Password of the user who can read log files.

Examples

The following example checks the `amConsole` logs.

```
$ amverifyarchive -l amConsole -p $HOME/openam/openam/log
  -u amadmin -w password
```

Name

configurator.jar — install or upgrade OpenAM using a configuration file

Synopsis

`configurator.jar` {options}

Description

This executable .jar file, openam-configurator-tool-11.0.0.jar, lets you perform silent installation, configuring a deployed OpenAM server by applying settings from a configuration file.

Options

The following options are supported.

-f | --file *configuration-file*

Configure a deployed OpenAM web application archive using the specified configuration file. Installation and upgrade configuration files are described in the sections below.

-? | --help

Display the usage message.

Installation Configuration File

Base your configuration on the `sampleconfiguration` file delivered with OpenAM, and using the hints in this section, or the comments included in the file.

Server Properties

These properties pertain to the OpenAM server instance.

SERVER_URL

URL to the web container where you want OpenAM to run, such as `http://openam.example.com:8080`

DEPLOYMENT_URI

URI where you want to deploy OpenAM on the web container, such as `/openam`

BASE_DIR

Configuration directory where OpenAM stores files and embedded configuration directory servers, such as `$HOME/openam`

locale

The user locale, such as `en_GB`

PLATFORM_LOCALE

The locale of the OpenAM server, such as `en_US`

AM_ENC_KEY

The password encryption key, which must be the same on all servers in a multi-server installation, such as `06QWwHPO4os+zEz3Nqn/2daAYWyiFE32`. If left blank, installing OpenAM generates a random password encryption key that you can later view in OpenAM console under Configuration > Servers and Sites > *Server Name* > Security.

ADMIN_PWD

Password of the OpenAM administrator user `amadmin`, which must be at least 8 characters in length and must match that of other servers in a multiserver deployment

AMLDAPUSERPASSWD

Password of the default policy agent `UrlAccessAgent`, which must be at least 8 characters in length and must not be the same as the value of `ADMIN_PWD`

COOKIE_DOMAIN

Name of the trusted DNS domain OpenAM returns to a browser when it grants a session ID to a user, such as `.example.com`

Configuration Store Properties

These properties pertain to the directory server where OpenAM stores its configuration.

DATA_STORE

Type of the configuration data store. The value `embedded` means set up OpenAM with an embedded, OpenDJ based configuration store. The value `dirServer` means an external directory server, such as OpenDJ, or Sun Java System Directory Server. If you set this to `dirServer`, and the configuration store contains the configuration of other OpenAM servers, then the server is added to the existing multiserver installation.

DIRECTORY_SSL

To use LDAP without SSL, set this to `SIMPLE`. To use LDAP with SSL, set this to `SSL`.

DIRECTORY_SERVER

Fully qualified domain name of the configuration store directory server host, such as `opendj.example.com`

DIRECTORY_PORT

LDAP or LDAPS port number for the configuration store directory server, such as 389 or 636

DIRECTORY_ADMIN_PORT

Administration port number for the configuration store directory server, such as 4444

DIRECTORY_JMX_PORT

Java Management eXtension port number, such as `1689`, used with the OpenDJ embedded configuration store

ROOT_SUFFIX

Root suffix distinguished name (DN) for the configuration store, such as `o=openam`

DS_DIRMGRDN

Distinguished name of the directory manager of the configuration store, such as `cn=Directory Manager`

DS_DIRMGRPASSWD

Password for the directory manager of the configuration store

User Data Store Properties

These properties pertain to the directory server where OpenAM stores user profiles. If you do not include these properties, or you leave these properties commented out, then OpenAM uses the same directory server as it uses for the configuration store.

USERSTORE_TYPE

The type of directory server used. Valid values include the following.

- `LDAPv3ForOpenDS`: ForgeRock 0penDJ or Sun OpenDS

- `LDAPv3ForAD`: Active Directory with host and port settings

- `LDAPv3ForADDC`: Active Directory with a Domain Name setting

- `LDAPv3ForADAM`: Active Directory Application Mode

- `LDAPv3ForODSEE`: Sun Java System Directory Server

- `LDAPv3ForTivoli`: IBM Tivoli Directory Server

USERSTORE_SSL

To use LDAP without SSL, set this to `SIMPLE`. To use LDAP with SSL, set this to `SSL`.

USERSTORE_DOMAINNAME

If `USERSTORE_TYPE` is `LDAPv3ForADDC`, you set this to the Active Directory Domain Name, such as `ad.example.com`, and then set only the `USERSTORE_SSL`, `USERSTORE_MGRDN`, and `USERSTORE_PASSWD` additional parameters. This lets Active Directory use DNS to retrieve service locations. Otherwise, do not use.

USERSTORE_HOST

Fully qualified domain name of the user data store directory server, such as `opendj.example.com`

USERSTORE_PORT

Port number of the user data store. Default for LDAP is 389, and for LDAP over SSL is 636.

USERSTORE_SUFFIX

Root suffix distinguished name for the user data in the directory, such as `dc=example,dc=com`

USERSTORE_MGRDN

Distinguished name of the directory manager of the user data store, such as `cn=Directory Manager`

USERSTORE_PASSWD

Password for the directory manager of the user data store

Site Properties

These properties pertain when you configure multiple OpenAM servers in a site deployment, where a load balancer spreads request across multiple servers. Use the `DS_EMB_REPL*` and `existingserverid` properties only for the second and subsequent servers in a site configuration.

LB_SITE_NAME

The name of the OpenAM site

LB_PRIMARY_URL

The load balancer URL for the site, such as `http://lb.example.com:80/openam`.

LB_SESSION_HA_SFO

Whether to enable session persistence and failover for the site. Default: `false`

DS_EMB_REPL_FLAG

Enable use of the embedded configuration store by setting this parameter to `embReplFlag`, only if the `DATA_STORE` parameter is set to `embedded`. Use the other `DS_EMB_REPL*` parameters in this section to set up configuration store data replication.

DS_EMB_REPL_REPLPORT1

Replication port number for the new OpenAM server you are installing, such as 58989

DS_EMB_REPL_HOST2

Host name of an existing OpenAM server housing the configuration store directory server with which to replicate, such as `openam1.example.com`

DS_EMB_REPL_ADMINPORT2

Administration port number for the configuration store directory server used by the existing OpenAM server, such as 4444

DS_EMB_REPL_REPLPORT2

Replication port number for the configuration store directory server used by the existing OpenAM server, such as 50899

existingserverid

Full URL of the existing OpenAM server, such as `http://server1.example.com:8080/openam`

Upgrade Configuration File

Base your configuration on the `sampleconfiguration` file delivered with OpenAM, and using the hints in this section, or the comments included in the file.

Upgrade Properties

SERVER_URL

URL to the web container where OpenAM runs, such as `http://openam.example.com:8080`

DEPLOYMENT_URI

URI where OpenAM is deployed on the web container, such as `/openam`

Examples

The following example shows a configuration file to install a server with an external user data store.

```
# Server properties, AM_ENC_KEY="" means generate random key
SERVER_URL=http://openam.example.com:8080
DEPLOYMENT_URI=/openam
BASE_DIR=$HOME/openam
locale=en_US
PLATFORM_LOCALE=en_US
AM_ENC_KEY=
ADMIN_PWD=change3me
```

```
AMLDAPUSERPASSWD=secret12
COOKIE_DOMAIN=.example.com

# Embedded configuration data store
DATA_STORE=embedded
DIRECTORY_SSL=SIMPLE
DIRECTORY_SERVER=openam.example.com
DIRECTORY_PORT=50389
DIRECTORY_ADMIN_PORT=4444
DIRECTORY_JMX_PORT=1689
ROOT_SUFFIX=o=openam
DS_DIRMGRDN=cn=Directory Manager
DS_DIRMGRPASSWD=chang3me

# External OpenDJ based user data store
USERSTORE_TYPE=LDAPv3ForOpenDS
USERSTORE_SSL=SIMPLE
#USERSTORE_DOMAINNAME=ad.example.com
USERSTORE_HOST=opendj.example.com
USERSTORE_PORT=389
USERSTORE_SUFFIX=dc=example,dc=com
USERSTORE_MGRDN=cn=Directory Manager
USERSTORE_PASSWD=secret12

# Uncomment to specify the site for the first server in a site configuration
#LB_SITE_NAME=lb
#LB_PRIMARY_URL=http://lb.example.com:80/openam
```

The following example shows a configuration file to install the second server in a site configuration.

```
# Server properties, AM_ENC_KEY from first server
SERVER_URL=http://server2.example.com:8080
DEPLOYMENT_URI=/openam
BASE_DIR=$HOME/openam
locale=en_US
PLATFORM_LOCALE=en_US
AM_ENC_KEY=O6QWwHPO4os+zEz3Nqn/2daAYWyiFE32
ADMIN_PWD=change3me
AMLDAPUSERPASSWD=secret12
COOKIE_DOMAIN=.example.com

# Embedded configuration data store
DATA_STORE=embedded
DIRECTORY_SSL=SIMPLE
DIRECTORY_SERVER=server2.example.com
DIRECTORY_PORT=50389
DIRECTORY_ADMIN_PORT=4444
DIRECTORY_JMX_PORT=1689
ROOT_SUFFIX=o=openam
DS_DIRMGRDN=cn=Directory Manager
DS_DIRMGRPASSWD=chang3me

# External OpenDJ based user data store
USERSTORE_TYPE=LDAPv3ForOpenDS
USERSTORE_SSL=SIMPLE
#USERSTORE_DOMAINNAME=ad.example.com
USERSTORE_HOST=opendj.example.com
USERSTORE_PORT=389
USERSTORE_SUFFIX=dc=example,dc=com
```

```
USERSTORE_MGRDN=cn=Directory Manager
USERSTORE_PASSWD=secret12

# Site properties
LB_SITE_NAME=lb
LB_PRIMARY_URL=http://lb.example.com:80/openam
DS_EMB_REPL_FLAG=embReplFlag
DS_EMB_REPL_REPLPORT1=58989
DS_EMB_REPL_HOST2=server1.example.com
DS_EMB_REPL_ADMINPORT2=4444
DS_EMB_REPL_REPLPORT2=50889
existingserverid=http://server1.example.com:8080/openam
```

The following example shows a configuration file to upgrade an OpenAM server.

```
SERVER_URL=https://openam.example.com:8080
DEPLOYMENT_URI=/openam
```

Name

ssoadm — configure OpenAM core services

Synopsis

`ssoadm` [*subcommand*] [options]

Description

The **ssoadm** command provides a rich command-line interface for configuring OpenAM core services.

Also see the *Installation Guide* procedure, *To Set Up Administration Tools* in the *Installation Guide* for instructions on setting up the **ssoadm** command.

Global Options

The following global options are supported.

--debug, -d

   Run in debug mode. Results sent to the debug file.

--help, -?

   Print usage.

   This command can also be used with subcommands as in **ssoadm *subcommand* --help**.

--information, -O

   Print basic information about the tool.

--locale, -l

   Name of the locale to display the results.

--verbose, -v

   Run in verbose mode. Results sent to standard output.

--version, -V

   Print the version of this tool.

Subcommands: By Category

This section lists subcommands by category. The subsequent section lists subcommands in alphabetical order with a short description.

See **ssoadm** *subcommand* **--help** for detailed options.

Agent Configuration

- **add-agent-to-grp**

- **agent-remove-props**

- **create-agent**

- **create-agent-grp**

- **delete-agent-grps**

- **delete-agents**

- **list-agent-grp-members**

- **list-agent-grps**

- **list-agents**

- **remove-agent-from-grp**

- **show-agent**

- **show-agent-grp**

- **show-agent-membership**

- **show-agent-types**

- **update-agent**

- **update-agent-grp**

Authentication Service Management

- **add-auth-cfg-entr**

- **create-auth-cfg**

- **create-auth-instance**

- **delete-auth-cfgs**

- **delete-auth-instances**

- **get-auth-cfg-entr**

- **get-auth-instance**

- **list-auth-cfgs**

- **list-auth-instances**

- **register-auth-module**

- **unregister-auth-module**

- **update-auth-cfg-entr**

- **update-auth-cfg-props**

- **update-auth-instance**

Data Store Management

- **add-amsdk-idrepo-plugin**

- **create-datastore**

- **delete-datastores**

- **list-datastore-types**

- **list-datastores**

- **show-datastore**

- **update-datastore**

Entitlements

- **add-app-priv**

- **create-appl**

- **create-appl-type**

- **create-xacml**

- **delete-appl-types**

- **delete-appls**

- **delete-xacml**

- **list-appl-types**

- **list-appls**

- **list-xacml**

- **set-appl**

- **set-entitlement-conf**

- **show-app-priv**

- **show-appl**

- **show-entitlement-conf**

- **update-app-priv**

- **update-app-priv-resources**

- **update-app-priv-subjects**

Federation Management

- **add-cot-member**

- **create-cot**

- **create-metadata-templ**

- **delete-cot**

- **delete-entity**

- **do-bulk-federation**

- **export-entity**

- **import-bulk-fed-data**

- **import-entity**

- **list-cot-members**

- **list-cots**

- **list-entities**

- **remove-cot-member**

- **update-entity-keyinfo**

Identity Management

- **add-member**

- **add-privileges**

- **add-svc-identity**

- **create-identity**

- **delete-identities**

- **get-identity**

- **get-identity-svcs**

- **list-identities**

- **list-identity-assignable-svcs**

- **remove-member**

- **remove-privileges**

- **remove-svc-identity**

- **set-identity-attrs**

- **set-identity-svc-attrs**

- **show-identity-ops**

- **show-identity-svc-attrs**

- **show-identity-types**

- **show-members**

- **show-memberships**

- **show-privileges**

Policy Management

- **create-policies**

- **delete-policies**

- **list-policies**

- **update-policies**

Realm Management

- **add-svc-attrs**

- **add-svc-realm**

- **create-realm**

- **delete-realm**

- **delete-realm-attr**

- **get-realm**

- **get-realm-svc-attrs**

- **list-realm-assignable-svcs**

- **list-realms**

- **remove-svc-attrs**

- **remove-svc-realm**

- **set-realm-attrs**

- **set-svc-attrs**

- **set-realm-svc-attrs**

- **show-auth-modules**

- **show-data-types**

- **show-realm-svcs**

Server Configuration

- **add-site-members**

- **add-site-sec-urls**

- **clone-server**

- **create-server**

- **create-site**

- **delete-server**

- **delete-site**

- **export-server**

- **get-svrcfg-xml**

- **import-server**

- **list-server-cfg**

- **list-servers**

- **list-sites**

- **remove-server-cfg**

- **remove-site-members**

- **remove-site-sec-urls**

- **set-site-pri-url**

- **set-site-sec-urls**

- **set-svrcfg-xml**

- **show-site**

- **show-site-members**

- **update-server-cfg**

Service Management

To translate settings applied in OpenAM console to service attributes for use with **ssoadm**, login to the OpenAM console as as `amadmin` and access the services page, such as `http://openam.example.com:8080/openam/services.jsp`.

- **add-attr-defs**

- **add-attrs**

- **add-plugin-interface**

- **add-sub-schema**

- **create-sub-cfg**

- **create-svc**

- **create-svrcfg-xml**

- **delete-attr**

- **delete-sub-cfg**

- **delete-svc**

- **export-svc-cfg**

- **get-attr-defs**

- **get-revision-number**

- **import-svc-cfg**

- **remove-attr-choicevals**

- **remove-attr-defs**

- **remove-sub-schema**

- **set-attr-any**

- **set-attr-bool-values**

- **set-attr-choicevals**

- **set-attr-defs**

- **set-attr-end-range**

- **set-attr-i18n-key**

- **set-attr-start-range**

- **set-attr-syntax**

- **set-attr-type**

- **set-attr-ui-type**

- **set-attr-validator**

- **set-attr-view-bean-url**

- **set-inheritance**

- **set-plugin-viewbean-url**

- **set-revision-number**

- **set-sub-cfg**

- **set-svc-i18n-key**

- **set-svc-view-bean-url**

- **update-svc**

Other

- **add-res-bundle**

- **do-batch**

- **do-migration70**

- **list-res-bundle**

- **list-sessions**

- **remove-res-bundle**

Subcommands: Alphabetical Order

The following subcommands are supported.

See also **ssoadm** *subcommand* **--help**.

ssoadm add-agent-to-grp

Add agents to a agent group.

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

Options

--adminid, -u

Administrator ID of running the command.

--agentgroupname, -b

Name of agent group.

--agentnames, -s

Names of agents.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm add-amsdk-idrepo-plugin

Create AMSDK IdRepo Plug-in

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

Options

--adminid, -u

Administrator ID of running the command.

--basedn, -b

Directory Server base distinguished name.

--bind-password-file, -m

File that contains password of bind password.

--binddn, -e

Directory Server bind distinguished name.

--directory-servers, -s

directory servers <protocol>://<hostname>:<port>. Can have multiple entries.

--dsame-password-file, -x

File that contains password of the dsameuser

--password-file, -f

File name that contains password of administrator.

--puser-password-file, -p

File that contains password of the puser

[--org, -o]

Organization objects naming attribute (defaults to 'o')

FORGEROCK

[--user, -a]

　　User objects naming attribute (defaults to 'uid')

ssoadm add-app-priv

Add an application privilege to delegate resources of a given application.

Usage: `ssoadm add-app-priv --options [--global-options]`

Options

--actions, -a

　　Possible values are READ, MODIFY, DELEGATE, ALL

--adminid, -u

　　Administrator ID of running the command.

--application, -t

　　Application name

--name, -m

　　Name for the this delegation

--password-file, -f

　　File name that contains password of administrator.

--realm, -e

　　Realm name

--subjects, -s

　　Subject name

--subjecttype, -b

　　Possible values are User or Group

[--description, -p]

　　Description for the this delegation.

[--resources, -r]

　　Resources to delegate, All resources in the applications will be delegated if this option is absent.

ssoadm add-attr-defs

Add default attribute values in schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

[--subschemaname, -c]

Name of sub schema.

ssoadm add-attrs

Add attribute schema to an existing service.

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

Options

--adminid, -u

Administrator ID of running the command.

--attributeschemafile, -F

XML file containing attribute schema definition.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Schema Type.

--servicename, -s

Service Name.

[--subschemaname, -c]

Name of sub schema.

ssoadm add-auth-cfg-entr

Add authentication configuration entry

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

Options

--adminid, -u

Administrator ID of running the command.

--criteria, -c

Criteria for this entry. Possible values are REQUIRED, OPTIONAL, SUFFICIENT, REQUISITE

--modulename, -o

Module Name.

--name, -m

Name of authentication configuration.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--options, -t]

> Options for this entry.

[--position, -p]

> Position where the new entry is to be added. This is option is not set, entry shall be added to the end of the list. If value of this option is 0, it will be inserted to the front of the list. If value is greater of the length of the list, entry shall be added to the end of the list.

ssoadm add-cot-member

Add a member to a circle of trust.

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

Options

--adminid, -u

> Administrator ID of running the command.

--cot, -t

> Circle of Trust

--entityid, -y

> Entity ID

--password-file, -f

> File name that contains password of administrator.

[--realm, -e]

> Realm where circle of trust resides

[--spec, -c]

> Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm add-member

Add an identity as member of another identity

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity

--memberidname, -m

Name of identity that is member.

--memberidtype, -y

Type of Identity of member such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm add-plugin-interface

Add Plug-in interface to service.

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

Options

--adminid, -u

Administrator ID of running the command.

--i18nkey, -k

Plug-in I18n Key.

--interfacename, -i

Name of interface.

--password-file, -f

File name that contains password of administrator.

--pluginname, -g

Name of Plug-in.

--servicename, -s

Name of service.

ssoadm add-plugin-schema

Add Plug-in schema to service.

Usage: ssoadm add-plugin-schema --options [--global-options]

Options

--adminid, -u

Administrator ID of running the command.

--classname, -c

Name of the Plugin Schema class implementation

--i18nkey, -k

Plug-in I18n Key.

--i18nname, -n

Plug-in I18n Name.

--interfacename, -i

Name of interface.

--password-file, -f

File name that contains password of administrator.

--pluginname, -g

Name of Plug-in.

--servicename, -s

Name of service.

ssoadm add-privileges

Add privileges to an identity. To add a privilege to all authenticated users, use the "All Authenticated Users" idname with "role" idtype.

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

Options

`--adminid, -u`

Administrator ID of running the command.

`--idname, -i`

Name of identity.

`--idtype, -t`

Type of Identity such as Role and Group.

`--password-file, -f`

File name that contains password of administrator.

`--privileges, -g`

Name of privileges to be added. Privilege names are AgentAdmin, EntitlementRestAccess, FederationAdmin, LogAdmin, LogRead, LogWrite, PolicyAdmin, PrivilegeRestAccess, PrivilegeRestReadAccess, RealmAdmin.

`--realm, -e`

Name of realm.

ssoadm add-res-bundle

Add resource bundle to data store.

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

Options

`--adminid, -u`

Administrator ID of running the command.

`--bundlefilename, -B`

Resource bundle physical file name.

FORGEROCK

--bundlename, -b

Resource Bundle Name.

--password-file, -f

File name that contains password of administrator.

[--bundlelocale, -o]

Locale of the resource bundle.

ssoadm add-site-members

Add members to a site.

Usage: ssoadm add-site-members --options [--global-options]

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servernames, -e

Server names, e.g. http://www.example.com:8080/fam

--sitename, -s

Site name, e.g. mysite

ssoadm add-site-sec-urls

Add Site Secondary URLs.

Usage: ssoadm add-site-sec-urls --options [--global-options]

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

--secondaryurls, -a

> Secondary URLs

--sitename, -s

> Site name, e.g. mysite

ssoadm add-sub-schema

Add sub schema.

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

Options

--adminid, -u

> Administrator ID of running the command.

--filename, -F

> Name of file that contains the schema

--password-file, -f

> File name that contains password of administrator.

--schematype, -t

> Type of schema.

--servicename, -s

> Name of service.

[--subschemaname, -c]

> Name of sub schema.

ssoadm add-svc-attrs

Add service attribute values in a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values to be added e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values to be added.

ssoadm add-svc-identity

Add Service to an identity

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

> Name of realm.

--servicename, -s

> Name of service.

[--attributevalues, -a]

> Attribute values e.g. homeaddress=here.

[--datafile, -D]

> Name of file that contains attribute values data.

ssoadm add-svc-realm

Add service to a realm.

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

Options

--adminid, -u

> Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Name of realm.

--servicename, -s

> Service Name.

[--attributevalues, -a]

> Attribute values e.g. homeaddress=here.

[--datafile, -D]

> Name of file that contains attribute values data.

ssoadm agent-remove-props

Remove agent's properties.

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

Options

--adminid, -u

Administrator ID of running the command.

--agentname, -b

Name of agent.

--attributenames, -a

properties name(s).

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm clone-server

Clone a server instance.

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

Options

--adminid, -u

Administrator ID of running the command.

--cloneservername, -o

Clone server name

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name

ssoadm create-agent

Create a new agent configuration.

FORGEROCK

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

Options

--adminid, -u

Administrator ID of running the command.

--agentname, -b

Name of agent.

--agenttype, -t

Type of agent. Possible values: J2EEAgent, WebAgent, WSCAgent, WSPAgent, STSAgent, DiscoveryAgent, 2.2_Agent, SharedAgent, OAuth2Client

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--agenturl, -g]

Agent URL. e.g. http://www.agent.example:8080/agent. WebAgent does not take URL with path. e.g. http://www.agent.example:8080. This option is valid for J2EEAgent and WebAgent. This parameter is required if the agent is created without datafile/attributes.

[--attributevalues, -a]

Properties e.g. sunIdentityServerDeviceKeyValue=https://agent.example.com:443/

[--datafile, -D]

Name of file that contains properties.

[--serverurl, -s]

Server URL. e.g. http://www.example.com:58080/openam. This option is valid for J2EEAgent and WebAgent. This parameter is required if the agent is created without datafile/attributes.

ssoadm create-agent-grp

Create a new agent group.

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

Options

--adminid, -u

Administrator ID of running the command.

--agentgroupname, -b

Name of agent group.

--agenttype, -t

Type of agent group. e.g. J2EEAgent, WebAgent

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Properties e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains properties.

[--serverurl, -s]

Server URL. e.g. http://www.example.com:58080/openam. This option is valid for J2EEAgent and WebAgent.

ssoadm create-appl

Create application.

Usage: `ssoadm create-appl --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--applicationtype, -t

Application type name

FORGEROCK

--name, -m

> Application name

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Realm name

[--attributevalues, -a]

> Attribute values e.g. applicationType=iPlanetAMWebAgentService.

[--datafile, -D]

> Name of file that contains attribute values data. Mandatory attributes are resources, subjects, conditions and entitlementCombiner. Optional ones are actions, searchIndexImpl, saveIndexImpl, resourceComparator, subjectAttributeNames.

ssoadm create-appl-type

Create application type.

Usage: `ssoadm create-appl-type --options [--global-options]`

Options

--adminid, -u

> Administrator ID of running the command.

--name, -m

> Application Type name

--password-file, -f

> File name that contains password of administrator.

[--attributevalues, -a]

> Application Type attribute values e.g. actions=enabled=true.

[--datafile, -D]

> Name of file that contains attribute type values data. Mandatory attributes are actions, searchIndexImpl and saveIndexImpl. Optional are resourceComparator.

ssoadm create-auth-cfg

Create authentication configuration

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

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name of authentication configuration.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm create-auth-instance

Create authentication instance

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

Options

--adminid, -u

Administrator ID of running the command.

--authtype, -t

Type of authentication instance e.g. LDAP, DataStore.

--name, -m

Name of authentication instance.

--password-file, -f

File name that contains password of administrator.

--realm, -e

> Name of realm.

ssoadm create-cot

Create circle of trust.

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

Options

--adminid, -u

> Administrator ID of running the command.

--cot, -t

> Circle of Trust

--password-file, -f

> File name that contains password of administrator.

[--prefix, -p]

> Prefix URL for idp discovery reader and writer URL.

[--realm, -e]

> Realm where circle of trust resides

[--trustedproviders, -k]

> Trusted Providers

ssoadm create-datastore

Create data store under a realm

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

Options

--adminid, -u

> Administrator ID of running the command.

--datatype, -t

Type of datastore. Use the list-datastore-types subcommand to get a list of supported datastore types.

--name, -m

Name of datastore.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Attribute values e.g. sunIdRepoClass=com.sun.identity.idm.plugins.files.FilesRepo.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm create-identity

Create identity in a realm

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Attribute values e.g. sunIdentityServerDeviceStatus=Active.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm create-metadata-templ

Create new metadata template.

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

Options

--adminid, -u

Administrator ID of running the command.

--entityid, -y

Entity ID

--password-file, -f

File name that contains password of administrator.

[--affiecertalias, -K]

Affiliation encryption certificate alias

[--affiliation, -F]

Specify metaAlias for hosted affiliation. to be created. The format must be <realm name>/<identifier>

[--affimembers, -M]

Affiliation members

[--affiownerid, -N]

Affiliation Owner ID

FORGEROCK

[--affiscertalias, -J]

Affiliation signing certificate alias

[--attraecertalias, -G]

Attribute authority encryption certificate alias.

[--attrascertalias, -B]

Attribute authority signing certificate alias

[--attrauthority, -I]

Specify metaAlias for hosted attribute authority to be created. The format must be <realm name>/<identifier>.

[--attrqecertalias, -R]

Attribute query provider encryption certificate alias

[--attrqscertalias, -A]

Attribute query provider signing certificate alias

[--attrqueryprovider, -S]

Specify metaAlias for hosted attribute query provider to be created. The format must be <realm name>/<identifier>.

[--authnaecertalias, -E]

Authentication authority encryption certificate alias.

[--authnascertalias, -D]

Authentication authority signing certificate alias

[--authnauthority, -C]

Specify metaAlias for hosted authentication authority to be created. The format must be <realm name>/<identifier>.

[--extended-data-file, -x]

Specify file name for the extended metadata to be created. XML will be displayed on terminal if this file name is not provided.

[--identityprovider, -i]

Specify metaAlias for hosted identity provider to be created. The format must be <realm name>/<identifier>.

[--idpecertalias, -g]

Identity provider encryption certificate alias.

[--idpscertalias, -b]

Identity provider signing certificate alias

[--meta-data-file, -m]

Specify file name for the standard metadata to be created. XML will be displayed on terminal if this file name is not provided.

[--serviceprovider, -s]

Specify metaAlias for hosted service provider to be created. The format must be <realm name>/<identifier>.

[--specertalias, -r]

Service provider encryption certificate alias

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

[--spscertalias, -a]

Service provider signing certificate alias

[--xacmlpdpecertalias, -j]

Policy decision point encryption certificate alias

[--xacmlpdpscertalias, -t]

Policy decision point signing certificate alias

[--xacmlpdp, -p]

Specify metaAlias for policy decision point to be created. The format must be <realm name>/<identifier>.

[--xacmlpepecertalias, -z]

Policy enforcement point encryption certificate alias

[--xacmlpepscertalias, -k]

Policy enforcement point signing certificate alias

FORGEROCK

[--xacmlpep, -e]

Specify metaAlias for policy enforcement point to be created. The format must be <realm name>/ <identifier>.

ssoadm create-policies

Create policies in a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--xmlfile, -X

Name of file that contains policy XML definition.

ssoadm create-realm

Create realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm to be created.

ssoadm create-server

Create a server instance.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--serverconfigxml, -X

Server Configuration XML file name.

--servername, -s

Server name, e.g. http://www.example.com:8080/fam

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm create-site

Create a site.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--sitename, -s

Site name, e.g. mysite

FORGEROCK

--siteurl, -i

Site's primary URL, e.g. http://www.example.com:8080

[--secondaryurls, -a]

Secondary URLs

ssoadm create-sub-cfg

Create a new sub configuration.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

--subconfigname, -g

Name of sub configuration.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

[--priority, -p]

Priority of the sub configuration.

[--realm, -e]

Name of realm (Sub Configuration shall be added to global configuration if this option is not provided).

[--subconfigid, -b]

> ID of parent configuration(Sub Configuration shall be added to root configuration if this option is not provided).

ssoadm create-svc

Create a new service in server.

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

Options

--adminid, -u

> Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

--xmlfile, -X

> XML file(s) that contains schema.

[--continue, -c]

> Continue adding service if one or more previous service cannot be added.

ssoadm create-svrcfg-xml

Create serverconfig.xml file. No options are required for flat file configuration data store.

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

Options

--adminid, -u

> Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

[--basedn, -b]

> Directory Server base distinguished name.

[--dsadmin, -a]

> Directory Server administrator distinguished name

[--dshost, -t]

> Directory Server host name

[--dspassword-file, -x]

> File that contains Directory Server administrator password

[--dsport, -p]

> Directory Server port number

[--outfile, -o]

> File name where serverconfig XML is written.

ssoadm create-xacml

Create policies in a realm with XACML input.

Usage: `ssoadm create-xacml --options [--global-options]`

Options

--adminid, -u

> Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Name of realm.

--xmlfile, -X

> Name of file that contains policy XACML definition.

ssoadm delete-agent-grps

Delete agent groups.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--agentgroupnames, -s]

Separate multiple agent group names with spaces.

[--file, -D]

File containing agent group names, with multiple group names separated by spaces.

ssoadm delete-agents

Delete agent configurations.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--agentnames, -s]

Separate multiple agent names with spaces.

[--file, -D]

File containing agent names, with multiple agent names separated by spaces.

ssoadm delete-appl-types

Delete application types.

Usage: `ssoadm delete-appl-types --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--names, -m`

Application Type names

`--password-file, -f`

File name that contains password of administrator.

ssoadm delete-appls

Delete applications.

Usage: `ssoadm delete-appls --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--names, -m`

Application names

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Realm name

ssoadm delete-attr

Delete attribute schemas from a service

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

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema to be removed.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm delete-attr-def-values

Delete attribute schema default values.

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

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--defaultvalues, -e

Default value(s) to be deleted

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm delete-auth-cfgs

Delete authentication configurations

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

Options

--adminid, -u

Administrator ID of running the command.

--names, -m

Name of authentication configurations.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm delete-auth-instances

Delete authentication instances

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

Options

--adminid, -u

Administrator ID of running the command.

--names, -m

    Name of authentication instances.

--password-file, -f

    File name that contains password of administrator.

--realm, -e

    Name of realm.

ssoadm delete-cot

Delete circle of trust.

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

Options

--adminid, -u

    Administrator ID of running the command.

--cot, -t

    Circle of Trust

--password-file, -f

    File name that contains password of administrator.

[--realm, -e]

    Realm where circle of trust resides

ssoadm delete-datastores

Delete data stores under a realm

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

Options

--adminid, -u

    Administrator ID of running the command.

FORGEROCK

--names, -m

> Names of datastore.

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Name of realm.

ssoadm delete-entity

Delete entity.

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

Options

--adminid, -u

> Administrator ID of running the command.

--entityid, -y

> Entity ID

--password-file, -f

> File name that contains password of administrator.

[--extendedonly, -x]

> Set to flag to delete only extended data.

[--realm, -e]

> Realm where data resides

[--spec, -c]

> Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm delete-identities

Delete identities in a realm

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

Options

--adminid, -u

Administrator ID of running the command.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--file, -D]

Name of file that contains the identity names to be deleted.

[--idnames, -i]

Names of identites.

ssoadm delete-policies

Delete policies from a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--file, -D]

Name of file that contains the policy names to be deleted.

[--policynames, -p]

Names of policy to be deleted.

ssoadm delete-realm

Delete realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm to be deleted.

[--recursive, -r]

Delete descendent realms recursively.

ssoadm delete-realm-attr

Delete attribute from a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--attributename, -a

Name of attribute to be removed.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

ssoadm delete-server

Delete a server instance.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name, e.g. http://www.example.com:8080/fam

ssoadm delete-site

Delete a site.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--sitename, -s

Site name, e.g. mysite

ssoadm delete-sub-cfg

Remove Sub Configuration.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

--subconfigname, -g

Name of sub configuration.

[--realm, -e]

Name of realm (Sub Configuration shall be added to global configuration if this option is not provided).

ssoadm delete-svc

Delete service from the server.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Service Name(s).

[--continue, -c]

Continue deleting service if one or more previous services cannot be deleted.

[--deletepolicyrule, -r]

Delete policy rule.

ssoadm delete-xacml

Delete XACML policies from a realm.

Usage: `ssoadm delete-xacml --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--file, -D]

Name of file that contains the policy names to be deleted.

[--policynames, -p]

Names of policy to be deleted.

ssoadm do-batch

Do multiple requests in one command.

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

Options

--adminid, -u

Administrator ID of running the command.

--batchfile, -Z

Name of file that contains commands and options.

--password-file, -f

File name that contains password of administrator.

[--batchstatus, -b]

Name of status file.

[--continue, -c]

Continue processing the rest of the request when preceeding request was erroneous.

ssoadm do-bulk-federation

Perform bulk federation.

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

Options

--adminid, -u

Administrator ID of running the command.

--metaalias, -m

Specify metaAlias for local provider.

--nameidmapping, -e

Name of file that will be created by this sub command. It contains remote user Id to name identifier. It shall be used by remote provider to update user profile.

--password-file, -f

File name that contains password of administrator.

--remoteentityid, -r

Remote entity Id

--useridmapping, -g

File name of local to remote user Id mapping. Format <local-user-id>|<remote-user-id>

[--spec, -c]

Specify metadata specification, either idff or saml2, defaults to saml2

ssoadm do-migration70

Migrate organization to realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--entrydn, -e

Distinguished name of organization to be migrated.

--password-file, -f

File name that contains password of administrator.

ssoadm embedded-status

Status of embedded store.

Usage: `ssoadm embedded-status --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--port, -p

Embedded store port

[--password, -w]

Embedded store password

ssoadm export-entity

Export entity.

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

Options

--adminid, -u

Administrator ID of running the command.

--entityid, -y

Entity ID

--password-file, -f

File name that contains password of administrator.

[--extended-data-file, -x]

Extended data

[--meta-data-file, -m]

Metadata

[--realm, -e]

Realm where data resides

[--sign, -g]

Set this flag to sign the metadata

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm export-server

Export a server instance.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

--servername, -s

> Server name

[--outfile, -o]

> Filename where configuration was written.

ssoadm export-svc-cfg

Export service configuration.

Usage: ssoadm export-svc-cfg --options [--global-options]

Options

--adminid, -u

> Administrator ID of running the command.

--encryptsecret, -e

> Secret key for encrypting password.

--password-file, -f

> File name that contains password of administrator.

[--outfile, -o]

> Filename where configuration was written.

ssoadm get-attr-choicevals

Get choice values of attribute schema.

Usage: ssoadm get-attr-choicevals --options [--global-options]

Options

--adminid, -u

> Administrator ID of running the command.

--attributename, -a

Name of attribute.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm get-attr-defs

Get default attribute values in schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema. One of dynamic, global, or organization (meaning realm).

--servicename, -s

Name of service.

[--attributenames, -a]

Attribute name(s).

[--subschemaname, -c]

Name of sub schema.

ssoadm get-auth-cfg-entr

Get authentication configuration entries

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

Options

--adminid, -u

> Administrator ID of running the command.

--name, -m

> Name of authentication configuration.

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Name of realm.

ssoadm get-auth-instance

Get authentication instance values

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

Options

--adminid, -u

> Administrator ID of running the command.

--name, -m

> Name of authentication instance.

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Name of realm.

ssoadm get-identity

Get identity property values

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributenames, -a]

Attribute name(s). All attribute values shall be returned if the option is not provided.

ssoadm get-identity-svcs

Get the service in an identity

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

FORGEROCK

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm get-realm

Get realm property values.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

ssoadm get-realm-svc-attrs

Get realm's service attribute values.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

ssoadm get-revision-number

Get service schema revision number.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

ssoadm get-sub-cfg

Get sub configuration.

Usage: `ssoadm get-sub-cfg --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

--subconfigname, -g

    Name of sub configuration.

[--realm, -e]

    Name of realm (Sub Configuration shall be added to global configuration if this option is not provided).

ssoadm get-svrcfg-xml

Get server configuration XML from centralized data store

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

Options

--adminid, -u

    Administrator ID of running the command.

--password-file, -f

    File name that contains password of administrator.

--servername, -s

    Server name, e.g. http://www.example.com:8080/fam

[--outfile, -o]

    File name where serverconfig XML is written.

ssoadm import-bulk-fed-data

Import bulk federation data which is generated by 'do-bulk-federation' sub command.

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

Options

--adminid, -u

    Administrator ID of running the command.

--bulk-data-file, -g

    File name of bulk federation data which is generated by 'do-bulk-federation' sub command.

--metaalias, -m

Specify metaAlias for local provider.

--password-file, -f

File name that contains password of administrator.

[--spec, -c]

Specify metadata specification, either idff or saml2, defaults to saml2

ssoadm import-entity

Import entity.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

[--cot, -t]

Specify name of the Circle of Trust this entity belongs.

[--extended-data-file, -x]

Specify file name for the extended entity configuration to be imported.<web>Extended entity configuration to be imported.

[--meta-data-file, -m]

Specify file name for the standard metadata to be imported.<web>Standard metadata to be imported.

[--realm, -e]

Realm where entity resides.

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm import-server

Import a server instance.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name

--xmlfile, -X

XML file that contains configuration.

ssoadm import-svc-cfg

Import service configuration.

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

Options

--adminid, -u

Administrator ID of running the command.

--encryptsecret, -e

Secret key for decrypting password.

--password-file, -f

File name that contains password of administrator.

--xmlfile, -X

XML file that contains configuration data.

ssoadm list-agent-grp-members

List agents in agent group.

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

Options

--adminid, -u

Administrator ID of running the command.

--agentgroupname, -b

Name of agent group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--filter, -x]

Filter (Pattern).

ssoadm list-agent-grps

List agent groups.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--agenttype, -t]

Type of agent. e.g. J2EEAgent, WebAgent

[--filter, -x]

Filter (Pattern).

ssoadm list-agents

List agent configurations.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--agenttype, -t]

Type of agent. e.g. J2EEAgent, WebAgent

[--filter, -x]

Filter (Pattern).

ssoadm list-app-privs

List application privileges in a realm.

Usage: `ssoadm list-app-privs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

  File name that contains password of administrator.

--realm, -e

  Realm name

ssoadm list-appl-types

List application types.

Usage: `ssoadm list-appl-types --options [--global-options]`

Options

--adminid, -u

  Administrator ID of running the command.

--password-file, -f

  File name that contains password of administrator.

ssoadm list-appls

List applications in a realm.

Usage: `ssoadm list-appls --options [--global-options]`

Options

--adminid, -u

  Administrator ID of running the command.

--password-file, -f

  File name that contains password of administrator.

--realm, -e

  Realm name

ssoadm list-auth-cfgs

List authentication configurations

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

Options

--adminid, -u

    Administrator ID of running the command.

--password-file, -f

    File name that contains password of administrator.

--realm, -e

    Name of realm.

ssoadm list-auth-instances

List authentication instances

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

Options

--adminid, -u

    Administrator ID of running the command.

--password-file, -f

    File name that contains password of administrator.

--realm, -e

    Name of realm.

ssoadm list-cot-members

List the members in a circle of trust.

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

Options

--adminid, -u

    Administrator ID of running the command.

--cot, -t

    Circle of Trust

--password-file, -f

    File name that contains password of administrator.

[--realm, -e]

    Realm where circle of trust resides

[--spec, -c]

    Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm list-cots

List circles of trust.

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

Options

--adminid, -u

    Administrator ID of running the command.

--password-file, -f

    File name that contains password of administrator.

[--realm, -e]

    Realm where circle of trusts reside

ssoadm list-datastore-types

List the supported data store types

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

Options

--adminid, -u

    Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

ssoadm list-datastores

List data stores under a realm

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

Options

--adminid, -u

> Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Name of realm.

ssoadm list-entities

List entities under a realm.

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

Options

--adminid, -u

> Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

[--realm, -e]

> Realm where entities reside.

[--spec, -c]

> Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm list-identities

List identities in a realm

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

Options

--adminid, -u

Administrator ID of running the command.

--filter, -x

Filter (Pattern).

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm list-identity-assignable-svcs

List the assignable service to an identity

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm list-policies

List policy definitions in a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--namesonly, -n]

Returns only names of matching policies. Policies are not returned.

[--outfile, -o]

Filename where policy definition will be printed to. Definition will be printed in standard output if this option is not provided.

[--policynames, -p]

Names of policy. This can be an wildcard. All policy definition in the realm will be returned if this option is not provided.

ssoadm list-realm-assignable-svcs

List the assignable services to a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

FORGEROCK

--password-file, -f

    File name that contains password of administrator.

--realm, -e

    Name of realm.

ssoadm list-realms

List realms by name.

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

Options

--adminid, -u

    Administrator ID of running the command.

--password-file, -f

    File name that contains password of administrator.

--realm, -e

    Name of realm where search begins.

[--filter, -x]

    Filter (Pattern).

[--recursive, -r]

    Search recursively

ssoadm list-res-bundle

List resource bundle in data store.

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

Options

--adminid, -u

    Administrator ID of running the command.

--bundlename, -b

Resource Bundle Name.

--password-file, -f

File name that contains password of administrator.

[--bundlelocale, -o]

Locale of the resource bundle.

ssoadm list-server-cfg

List server configuration.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name, e.g. http://www.example.com:8080/fam or enter default to list default server configuration.

[--withdefaults, -w]

Set this flag to get default configuration.

ssoadm list-servers

List all server instances.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

ssoadm list-sessions

List Sessions.

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

Options

--adminid, -u

> Administrator ID of running the command.

--host, -t

> Host Name.

--password-file, -f

> File name that contains password of administrator.

[--filter, -x]

> Filter (Pattern).

[--quiet, -q]

> Do not prompt for session invalidation.

ssoadm list-sites

List all sites.

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

Options

--adminid, -u

> Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

ssoadm list-xacml

export policies in realm as XACML.

Usage: `ssoadm list-xacml --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--namesonly, -n]

Returns only names of matching policies. Policies are not returned.

[--outfile, -o]

Filename where policy definition will be printed to. Definition will be printed in standard output if this option is not provided.

[--policynames, -p]

Names of policy. This can be a wildcard. All policy definition in the realm will be returned if this option is not provided.

ssoadm register-auth-module

Registers authentication module.

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

Options

--adminid, -u

Administrator ID of running the command.

--authmodule, -a

Java class name of authentication module.

--password-file, -f

> File name that contains password of administrator.

ssoadm remove-agent-from-grp

Remove agents from a agent group.

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

Options

--adminid, -u

> Administrator ID of running the command.

--agentgroupname, -b

> Name of agent group.

--agentnames, -s

> Names of agents.

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Name of realm.

ssoadm remove-app-priv-resources

Remove application privilege resources.

Usage: `ssoadm remove-app-priv-resources --options [--global-options]`

Options

--adminid, -u

> Administrator ID of running the command.

--application, -t

> Application name

--name, -m

Name for the this delegation

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

[--resources, -r]

Resources to removed, All resources in the applications will be removed if this option is absent.

ssoadm remove-app-priv-subjects

Remove application privilege subjects.

Usage: `ssoadm remove-app-priv-subjects --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name for the this delegation

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

--subjects, -s

Subject name

--subjecttype, -b

Possible values are User or Group

ssoadm remove-app-privs

Remove an application privileges.

Usage: `ssoadm remove-app-privs --options [--global-options]`

Options

--adminid, -u

   Administrator ID of running the command.

--names, -m

   Names of application privilege to be removed

--password-file, -f

   File name that contains password of administrator.

--realm, -e

   Realm name

ssoadm remove-attr-choicevals

Remove choice values from attribute schema.

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

Options

--adminid, -u

   Administrator ID of running the command.

--attributename, -a

   Name of attribute.

--choicevalues, -k

   Choice values e.g. Inactive

--password-file, -f

   File name that contains password of administrator.

--schematype, -t

   Type of schema.

--servicename, -s

   Name of service.

[--subschemaname, -c]

    Name of sub schema.

ssoadm remove-attr-defs

Remove default attribute values in schema.

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

Options

--adminid, -u

    Administrator ID of running the command.

--attributenames, -a

    Attribute name(s).

--password-file, -f

    File name that contains password of administrator.

--schematype, -t

    Type of schema.

--servicename, -s

    Name of service.

[--subschemaname, -c]

    Name of sub schema.

ssoadm remove-cot-member

Remove a member from a circle of trust.

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

Options

--adminid, -u

    Administrator ID of running the command.

--cot, -t

    Circle of Trust

--entityid, -y

    Entity ID

--password-file, -f

    File name that contains password of administrator.

[--realm, -e]

    Realm where circle of trust resides

[--spec, -c]

    Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm remove-member

Remove membership of identity from another identity

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

Options

--adminid, -u

    Administrator ID of running the command.

--idname, -i

    Name of identity.

--idtype, -t

    Type of Identity

--memberidname, -m

    Name of identity that is member.

--memberidtype, -y

    Type of Identity of member such as User, Role and Group.

--password-file, -f

    File name that contains password of administrator.

--realm, -e

> Name of realm.

ssoadm remove-plugin-schema

Add Plug-in interface to service.

Usage: ssoadm remove-plugin-schema --options [--global-options]

Options

--adminid, -u

> Administrator ID of running the command.

--interfacename, -i

> Name of interface.

--password-file, -f

> File name that contains password of administrator.

--pluginname, -g

> Name of Plug-in.

--servicename, -s

> Name of service.

ssoadm remove-privileges

Remove privileges from an identity

Usage: ssoadm remove-privileges --options [--global-options]

Options

--adminid, -u

> Administrator ID of running the command.

--idname, -i

> Name of identity.

--idtype, -t

Type of Identity such as Role and Group.

--password-file, -f

File name that contains password of administrator.

--privileges, -g

Name of privileges to be removed. Privilege names are AgentAdmin, EntitlementRestAccess, FederationAdmin, LogAdmin, LogRead, LogWrite, PolicyAdmin, PrivilegeRestAccess, PrivilegeRestReadAccess, RealmAdmin.

--realm, -e

Name of realm.

ssoadm remove-res-bundle

Remove resource bundle from data store.

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

Options

--adminid, -u

Administrator ID of running the command.

--bundlename, -b

Resource Bundle Name.

--password-file, -f

File name that contains password of administrator.

[--bundlelocale, -o]

Locale of the resource bundle.

ssoadm remove-server-cfg

Remove server configuration.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--propertynames, -a

Name of properties to be removed.

--servername, -s

Server name, e.g. http://www.example.com:8080/fam or enter default to remove default server configuration.

ssoadm remove-site-members

Remove members from a site.

Usage: ssoadm remove-site-members --options [--global-options]

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servernames, -e

Server names, e.g. http://www.example.com:8080/fam

--sitename, -s

Site name, e.g. mysite

ssoadm remove-site-sec-urls

Remove Site Secondary URLs.

Usage: ssoadm remove-site-sec-urls --options [--global-options]

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--secondaryurls, -a

Secondary URLs

--sitename, -s

Site name, e.g. mysite

ssoadm remove-sub-schema

Remove sub schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--subschemanames, -a

Name(s) of sub schema to be removed.

[--subschemaname, -c]

Name of parent sub schema.

ssoadm remove-svc-attrs

Remove service attribute values in a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values to be removed e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values to be removed.

ssoadm remove-svc-identity

Remove Service from an identity

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

ssoadm remove-svc-realm

Remove service from a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service to be removed.

ssoadm set-appl

Set application attributes.

Usage: `ssoadm set-appl --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

`--name, -m`

Application name

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Realm name

`[--attributevalues, -a]`

Attribute values e.g. applicationType=iPlanetAMWebAgentService.

`[--datafile, -D]`

Name of file that contains attribute values data. Possible attributes are resources, subjects, conditions, actions, searchIndexImpl, saveIndexImpl, resourceComparator, subjectAttributeNames and entitlementCombiner.

ssoadm set-attr-any

Set any member of attribute schema.

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

Options

`--adminid, -u`

Administrator ID of running the command.

`--any, -y`

Attribute Schema Any value

`--attributeschema, -a`

Name of attribute schema

`--password-file, -f`

File name that contains password of administrator.

`--schematype, -t`

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-bool-values

Set boolean values of attribute schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--attributename, -a

Name of attribute.

--falsei18nkey, -j

Internationalization key for false value.

--falsevalue, -z

Value for false.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--truei18nkey, -k

Internationalization key for true value.

--truevalue, -e

Value for true.

[--subschemaname, -c]

> Name of sub schema.

ssoadm set-attr-choicevals

Set choice values of attribute schema.

Usage: ssoadm set-attr-choicevals --options [--global-options]

Options

--adminid, -u

> Administrator ID of running the command.

--attributename, -a

> Name of attribute.

--password-file, -f

> File name that contains password of administrator.

--schematype, -t

> Type of schema.

--servicename, -s

> Name of service.

[--add, -p]

> Set this flag to append the choice values to existing ones.

[--choicevalues, -k]

> Choice value e.g. o102=Inactive.

[--datafile, -D]

> Name of file that contains attribute values data.

[--subschemaname, -c]

> Name of sub schema.

ssoadm set-attr-defs

Set default attribute values in schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-end-range

Set attribute schema end range.

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

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--range, -r

End range

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-i18n-key

Set i18nKey member of attribute schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--i18nkey, -k

Attribute Schema I18n Key

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-start-range

Set attribute schema start range.

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

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--range, -r

Start range

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-syntax

Set syntax member of attribute schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--syntax, -x

Attribute Schema Syntax

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-type

Set type member of attribute schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

`--type, -p`

Attribute Schema Type

`[--subschemaname, -c]`

Name of sub schema.

ssoadm set-attr-ui-type

Set UI type member of attribute schema.

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

Options

`--adminid, -u`

Administrator ID of running the command.

`--attributeschema, -a`

Name of attribute schema

`--password-file, -f`

File name that contains password of administrator.

`--schematype, -t`

Type of schema.

`--servicename, -s`

Name of service.

`--uitype, -p`

Attribute Schema UI Type

`[--subschemaname, -c]`

Name of sub schema.

ssoadm set-attr-validator

Set attribute schema validator.

FORGEROCK

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

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--validator, -r

validator class name

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-view-bean-url

Set properties view bean URL member of attribute schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--url, -r

Attribute Schema Properties View Bean URL

[--subschemaname, -c]

Name of sub schema.

ssoadm set-entitlement-conf

Set entitlements service configuration

Usage: `ssoadm set-entitlement-conf --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

[--attributevalues, -a]

Attribute values e.g. evalThreadSize=4.

[--datafile, -D]

Name of file that contains attribute values data. Possible attributes are evalThreadSize, searchThreadSize, policyCacheSize and indexCacheSize.

ssoadm set-identity-attrs

Set attribute values of an identity

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm set-identity-svc-attrs

Set service attribute values of an identity

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm set-inheritance

Set Inheritance value of Sub Schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--inheritance, -r

Value of Inheritance.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--subschemaname, -c

Name of sub schema.

ssoadm set-plugin-viewbean-url

Set properties view bean URL of plug-in schema.

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

Options

--adminid, -u

Administrator ID of running the command.

--interfacename, -i

Name of interface.

--password-file, -f

File name that contains password of administrator.

--pluginname, -g

Name of Plug-in.

--servicename, -s

Name of service.

--url, -r

Properties view bean URL.

ssoadm set-realm-attrs

Set attribute values of a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--append, -p]

Set this flag to append the values to existing ones.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm set-realm-svc-attrs

Set attribute values of a service that is assigned to a realm.

Usage: `ssoadm set-realm-svc-attrs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--append, -p]

Set this flag to append the values to existing ones.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

  Name of file that contains attribute values data.

ssoadm set-revision-number

Set service schema revision number.

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

Options

--adminid, -u

  Administrator ID of running the command.

--password-file, -f

  File name that contains password of administrator.

--revisionnumber, -r

  Revision Number

--servicename, -s

  Name of service.

ssoadm set-site-id

Set the ID of a site.

Usage: `ssoadm set-site-id --options [--global-options]`

Options

--adminid, -u

  Administrator ID of running the command.

--password-file, -f

  File name that contains password of administrator.

--siteid, -i

  Site's ID, e.g. 10

--sitename, -s

  Site name, e.g. mysite

ssoadm set-site-pri-url

Set the primary URL of a site.

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

Options

--adminid, -u

  Administrator ID of running the command.

--password-file, -f

  File name that contains password of administrator.

--sitename, -s

  Site name, e.g. mysite

--siteurl, -i

  Site's primary URL, e.g. http://site.www.example.com:8080

ssoadm set-site-sec-urls

Set Site Secondary URLs.

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

Options

--adminid, -u

  Administrator ID of running the command.

--password-file, -f

  File name that contains password of administrator.

--secondaryurls, -a

  Secondary URLs

FORGEROCK

--sitename, -s

Site name, e.g. mysite

ssoadm set-sub-cfg

Set sub configuration.

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

Options

--adminid, -u

Administrator ID of running the command.

--operation, -o

Operation (either add/set/modify) to be performed on the sub configuration.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

--subconfigname, -g

Name of sub configuration.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

[--realm, -e]

Name of realm (Sub Configuration shall be added to global configuration if this option is not provided).

ssoadm set-svc-attrs

Set service attribute values in a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm set-svc-i18n-key

Set service schema i18n key.

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

Options

--adminid, -u

Administrator ID of running the command.

--i18nkey, -k

I18n Key.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

ssoadm set-svc-view-bean-url

Set service schema properties view bean URL.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

--url, -r

Service Schema Properties View Bean URL

ssoadm set-svrcfg-xml

Set server configuration XML to centralized data store

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name, e.g. http://www.example.com:8080/fam

--xmlfile, -X

XML file that contains configuration.

ssoadm show-agent

Show agent profile.

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

Options

--adminid, -u

Administrator ID of running the command.

--agentname, -b

Name of agent.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--inherit, -i]

Set this to inherit properties from parent group.

[--outfile, -o]

Filename where configuration is written to.

ssoadm show-agent-grp

Show agent group profile.

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

Options

--adminid, -u

Administrator ID of running the command.

--agentgroupname, -b

Name of agent group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

> Name of realm.

[--outfile, -o]

> Filename where configuration is written to.

ssoadm show-agent-membership

List agent's membership.

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

Options

--adminid, -u

> Administrator ID of running the command.

--agentname, -b

> Name of agent.

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Name of realm.

ssoadm show-agent-types

Show agent types.

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

Options

--adminid, -u

> Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

ssoadm show-app-priv

Show application privilege.

Usage: `ssoadm show-app-priv --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name of application privilege

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

ssoadm show-appl

Show application attributes.

Usage: `ssoadm show-appl --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Application name

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

ssoadm show-appl-type

Show application type details.

Usage: `ssoadm show-appl-type --options [--global-options]`

Options

--adminid, -u

> Administrator ID of running the command.

--name, -m

> Application Type name

--password-file, -f

> File name that contains password of administrator.

ssoadm show-auth-modules

Show the supported authentication modules in the system.

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

Options

--adminid, -u

> Administrator ID of running the command.

--password-file, -f

> File name that contains password of administrator.

ssoadm show-data-types

Show the supported data type in the system.

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

Options

--adminid, -u

> Administrator ID of running the command.

--password-file, -f

>   File name that contains password of administrator.

ssoadm show-datastore

Show data store profile.

Usage: ssoadm show-datastore --options [--global-options]

Options

--adminid, -u

>   Administrator ID of running the command.

--name, -m

>   Name of datastore.

--password-file, -f

>   File name that contains password of administrator.

--realm, -e

>   Name of realm.

ssoadm show-entitlement-conf

Display entitlements service configuration

Usage: ssoadm show-entitlement-conf --options [--global-options]

Options

--adminid, -u

>   Administrator ID of running the command.

--password-file, -f

>   File name that contains password of administrator.

ssoadm show-identity-ops

Show the allowed operations of an identity a realm

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

Options

--adminid, -u

> Administrator ID of running the command.

--idtype, -t

> Type of Identity such as User, Role and Group.

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Name of realm.

ssoadm show-identity-svc-attrs

Show the service attribute values of an identity

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

Options

--adminid, -u

> Administrator ID of running the command.

--idname, -i

> Name of identity.

--idtype, -t

> Type of Identity such as User, Role and Group.

--password-file, -f

> File name that contains password of administrator.

--realm, -e

> Name of realm.

--servicename, -s

> Name of service.

ssoadm show-identity-types

Show the supported identity type in a realm

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm show-members

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

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--membershipidtype, -m

Membership identity type.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm show-memberships

Show the memberships of an identity. For sample show the memberships of an user.

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--membershipidtype, -m

Membership identity type.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm show-privileges

Show privileges assigned to an identity

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

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm show-realm-svcs

Show services in a realm.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--mandatory, -y]

Include Mandatory services.

ssoadm show-site

Show site profile.

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

Options

--adminid, -u

Administrator ID of running the command.

FORGEROCK

--password-file, -f

    File name that contains password of administrator.

--sitename, -s

    Site name, e.g. mysite

ssoadm show-site-members

Display members of a site.

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

Options

--adminid, -u

    Administrator ID of running the command.

--password-file, -f

    File name that contains password of administrator.

--sitename, -s

    Site name, e.g. mysite

ssoadm unregister-auth-module

Unregisters authentication module.

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

Options

--adminid, -u

    Administrator ID of running the command.

--authmodule, -a

    Java class name of authentication module.

--password-file, -f

    File name that contains password of administrator.

ssoadm update-agent

Update agent configuration.

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

Options

--adminid, -u

Administrator ID of running the command.

--agentname, -b

Name of agent.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Properties e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains properties.

[--set, -s]

Set this flag to overwrite properties values.

ssoadm update-agent-grp

Update agent group configuration.

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

Options

--adminid, -u

Administrator ID of running the command.

--agentgroupname, -b

Name of agent group.

`--password-file, -f`

    File name that contains password of administrator.

`--realm, -e`

    Name of realm.

`[--attributevalues, -a]`

    Properties e.g. homeaddress=here.

`[--datafile, -D]`

    Name of file that contains properties.

`[--set, -s]`

    Set this flag to overwrite properties values.

ssoadm update-app-priv

Update an application privilege.

Usage: `ssoadm update-app-priv --options [--global-options]`

Options

`--adminid, -u`

    Administrator ID of running the command.

`--name, -m`

    Name for the this delegation

`--password-file, -f`

    File name that contains password of administrator.

`--realm, -e`

    Realm name

`[--actions, -a]`

    Possible values are READ, MODIFY, DELEGATE, ALL

`[--description, -p]`

    Description for the this delegation.

ssoadm update-app-priv-resources

Set application privilege resources.

Usage: `ssoadm update-app-priv-resources --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--application, -t`

Application name

`--name, -m`

Name for the this delegation

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Realm name

`[--add, -p]`

Resources are added to this application if this option is set. Otherwise, resources in the current application privilege will be overwritten.

`[--resources, -r]`

Resources to delegate, All resources in the applications will be delegated if this option is absent.

ssoadm update-app-priv-subjects

Set application privilege subjects.

Usage: `ssoadm update-app-priv-subjects --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

--name, -m

Name for the this delegation

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

--subjects, -s

Subject name

--subjecttype, -b

Possible values are User or Group

[--add, -p]

Subjects are added to this application if this option is set. Otherwise, subjects in the current application privilege will be overwritten.

ssoadm update-auth-cfg-entr

Set authentication configuration entries

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

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name of authentication configuration.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--datafile, -D]

Name of file that contains formatted authentication configuration entries in this format name|flag|options. option can be REQUIRED, OPTIONAL, SUFFICIENT, REQUISITE. e.g. myauthmodule|REQUIRED|my options.

[--entries, -a]

formatted authentication configuration entries in this format name|flag|options. option can be REQUIRED, OPTIONAL, SUFFICIENT, REQUISITE. e.g. myauthmodule|REQUIRED|my options.

ssoadm update-auth-cfg-props

Set authentication configuration properties

Usage: ssoadm update-auth-cfg-props --options [--global-options]

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name of authentication configuration.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

authentication configuration properties, valid configuration keys are: iplanet-am-auth-login-failure-url, iplanet-am-auth-login-success-url and iplanet-am-auth-post-login-process-class.

[--datafile, -D]

Name of file that contains authentication configuration properties.

ssoadm update-auth-instance

Update authentication instance values

Usage: ssoadm update-auth-instance --options [--global-options]

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name of authentication instance.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm update-datastore

Update data store profile.

Usage: ssoadm update-datastore --options [--global-options]

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name of datastore.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Attribute values e.g. sunIdRepoClass=com.sun.identity.idm.plugins.files.FilesRepo.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm update-entity-keyinfo

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

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

Options

--adminid, -u

Administrator ID of running the command.

--entityid, -y

Entity ID

--password-file, -f

File name that contains password of administrator.

[--idpecertalias, -g]

Identity provider encryption certificate alias.

[--idpscertalias, -b]

Identity provider signing certificate alias

[--realm, -e]

Realm where entity resides.

[--specertalias, -r]

Service provider encryption certificate alias

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

[--spscertalias, -a]

Service provider signing certificate alias

ssoadm update-policies

Update policies in a realm.

Usage: `ssoadm update-policies --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--xmlfile, -X

Name of file that contains policy XML definition.

ssoadm update-server-cfg

Update server configuration.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name, e.g. http://www.example.com:8080/fam or enter default to update default server configuration.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm update-svc

Update service.

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

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--xmlfile, -X

XML file(s) that contains schema.

[--continue, -c]

Continue updating service if one or more previous services cannot be updated.

FORGEROCK

Chapter 1
Configuration Reference

This chapter covers OpenAM configuration properties accessible through the Configuration tab of the console, most of which can be set by using the **ssoadm** command. The chapter is organized to follow the OpenAM console layout.

1.1. Authentication Configuration

Under Configuration > Authentication you can configure authentication services globally using the same attributes you use to configure authentication modules per realm under Access Control > *Realm Name* > Authentication > Module Instances, and described in the *Administration Guide* chapter on *Defining Authentication Services* in the *Administration Guide*.

The primary difference is that when configuring services globally, you set the default values to be used when a module is configured further for a specific realm.

The Core Authentication module includes some fields under this tab that are not available through the realm changes under the `Access Control` tab. Because attributes set under the `Configuration` tab apply on a server level, the changes you make here will apply to all realms. Attributes set under the `Access Control` tab only apply to the realms that you specify. The Authentication table under the `Configuration` tab lists all existing types of modules available for configuration, including any customized modules you have added.

The following are the global fields you can configure for the Core Authentication module under the `Configuration` tab.

Pluggable Authentication Module Classes

Add class names for custom authentication modules to this list.

ssoadm attribute: `iplanet-am-auth-authenticators`

LDAP Connection Pool Size, Default LDAP Connection Pool Size

Sets a minimum and maximum number of LDAP connections in the pool for connecting to a directory server. When tuning for production, start with `10:65` (10 minimum, 65 maximum). Explicit settings for specific servers override the default.

This attribute is for LDAP and Membership authentication services only.

This connection pool is different than the SDK connection pool configured in `serverconfig.xml`.

ssoadm attributes: `iplanet-am-auth-ldap-connection-pool-size`, and `iplanet-am-auth-ldap-connection-pool-default-size`

LDAP Connection Pool Size, Default LDAP Connection Pool Size

Sets a minimum and maximum number of LDAP connections in the pool for connecting to a directory server. When tuning for production, start with `10:65` (10 minimum, 65 maximum). Explicit settings for specific servers override the default.

This attribute is for LDAP and Membership authentication services only.

This connection pool is different than the SDK connection pool configured in `serverconfig.xml`.

ssoadm attributes: `iplanet-am-auth-ldap-connection-pool-size`, and `iplanet-am-auth-ldap-connection-pool-default-size`

Remote Auth Security

Require the authenticating application to send its SSOToken. This allows the Authentication Service to obtain the username and password associated with the application.

ssoadm attribute: `sunRemoteAuthSecurityEnabled`

Keep Post Process Objects for Logout Processing, Keep Authentication Module Objects for Logout Processing

When enabled, retain objects used to process authentication or post authentication operations in the user session until the user logs out.

ssoadm attributes: `sunAMAuthKeepPostProcessInstances`, and `sunAMAuthKeepAuthModuleIntances`

XUI Interface

When enabled, the initial login screen uses the XUI.

ssoadm attribute: `openam-xui-interface-enabled`

1.2. Console Configuration

Under Configuration > Console you can customize how the OpenAM console appears, and what character sets are used.

Administration

Administration includes both global and realm attributes.

ssoadm service name: `iPlanetAMAdminConsoleService`

Federation Management

Clear Enabled to disable federation functionality in OpenAM.

ssoadm attribute: `iplanet-am-admin-console-liberty-enabled`

Maximum Results Returned from Search

Use this attribute to restrict the maximum number of results found in a search, such as a search for user profiles. Increasing the value can negatively impact performance. On the other hand, the default maximum of 100 can explain why administrators unaware of this setting can be surprised not to see all the users they expect in search results.

ssoadm attribute: `iplanet-am-admin-console-search-limit`

Timeout for Search

Timeout in seconds for a console search. OpenAM returns an error if the search is not completed by the timeout.

ssoadm attribute: `iplanet-am-admin-console-search-timeout`

Search Return Attribute

List of LDAP attribute types to return in search results. OpenAM sorts users by the first attribute you specify. Use attributes that are actually present in user profiles.

ssoadm attribute: `iplanet-am-admin-console-user-return-attribute`

Maximum Items Displayed per Page

OpenAM shows a maximum of this many items in a console page before separating the page into multiple screens.

ssoadm attribute: `iplanet-am-admin-console-paging-size`

Prompt user for old password

If enabled, when the user edits her password in the user view, then OpenAM prompts her for the old password.

ssoadm attribute: `iplanet-am-admin-console-password-reset-enabled`

Globalization Settings

Globalization settings affect character sets and common name formats. See *Localization* for a list of supported locales.

ssoadm service name: `iPlanetG11NSettings`

Charsets Supported by Each Locale

This table lets you configure the order of supported character sets used for each supported locale. Change the settings only if the defaults are not appropriate.

ssoadm attribute: `sun-identity-g11n-settings-locale-charset-mapping`

Charsets Aliases

Use this list to map between different character set names used in Java and in MIME.

ssoadm attribute: `sun-identity-g11n-settings-charset-alias-mapping`

Auto Generated Common Name Format

Use this list to configure how OpenAM formats names shown in the console banner.

ssoadm attribute: `sun-identity-g11n-settings-common-name-format`

1.3. System Configuration

Under Configuration > System, you can change OpenAM settings for server logging, monitoring, service URL naming, locale, cookie domain, and how OpenAM detects specific clients.

Client Detection

OpenAM can detect client user agents by their HTTP requests.

ssoadm service name: `iPlanetAMClientDetection`

Default Client Type

If no specific match is found for the client type, then this type is used. The default is `genericHTML`, suitable for supported browsers.

ssoadm attribute: `iplanet-am-client-detection-default-client-type`

Client Detection Class

The client detection plugin must implement the `com.iplanet.services.cdm.ClientDetectionInterface`. Client type is a name that uniquely identifies the client to OpenAM. The plugin scans HTTP requests to determine the client type.

ssoadm attribute: `iplanet-am-client-detection-class`

Enable Client Detection

If this is enabled, then OpenAM needs an appropriate client detection class implementation, and the authentication user interface must be appropriate for the clients detected.

ssoadm attribute: `iplanet-am-client-detection-enabled`

Logging

You configure global OpenAM logging settings on this page.

ssoadm service name: `iPlanetAMLoggingService`

Maximum Log Size

Sets the maximum log file size in bytes.

ssoadm attribute: `iplanet-am-logging-max-file-size`

Number of History Files

Sets the number of history files for each log that OpenAM keeps, including time-based histories. The previously live file is moved to be included in the history count, and a new log is created to serve as the live log file. Any log file in the history count that goes over the number specified here will be deleted. For time-based logs, a new set of logs will be created when OpenAM is started because of the time-based file names that are used.

ssoadm attribute: `iplanet-am-logging-num-hist-file`

Logfile Rotation Prefix

Set this if you want to add a prefix to log files governed by time-based log rotation.

ssoadm attribute: `openam-logging-file-prefix`

Logfile Rotation Suffix

Changing this if you want to change the suffix for log files governed by time-based log rotation. You can use `SimpleDateFormat` patterns. The default is `-MM.dd.yy-kk.mm`.

ssoadm attribute: `openam-logging-file-suffix`

Log File Location

This property is interpreted to determine the location of log files, taking either a file system location or a JDBC URL. The default is `%BASE_DIR%/%SERVER_URI%/log/`.

ssoadm attribute: `iplanet-am-logging-location`

Log Status

Set this to `INACTIVE` to disable the logging system.

ssoadm attribute: `logstatus`

FORGEROCK

Log Record Resolve Host Name

Enable this to have OpenAM perform a DNS host lookup to populate the host name field for log records. OpenAM requires DNS on the host where it runs. Enabling this feature increases the load on the logging system.

ssoadm attribute: `resolveHostName`

Logging Type

Set this to `DB` to log to a database. Default: `File`. If you choose `DB` then be sure to set the connection attributes correctly, including the JDBC driver to use.

ssoadm attribute: `iplanet-am-logging-type`

Database User Name

When logging to a database, set this to the user name used to connect to the database. If this attribute is incorrectly set, OpenAM performance suffers.

ssoadm attribute: `iplanet-am-logging-db-user`

Database User Password

When logging to a database, set this to the password used to connect to the database. If this attribute is incorrectly set, OpenAM performance suffers.

ssoadm attribute: `iplanet-am-logging-db-password`

Database Driver Name

When logging to a database, set this to the class name of the JDBC driver used to connect to the database. The default is for Oracle. OpenAM also works with the MySQL database driver.

ssoadm attribute: `iplanet-am-logging-db-driver`

Configurable Log Fields

Select the fields OpenAM includes in log messages using this attribute. By default all fields are included in log messages.

ssoadm attribute: `iplanet-am-logging-logfields`

Log Verification Frequency

When secure logging is enabled, set this to how often OpenAM verifies log file content (in seconds).

ssoadm attribute: `iplanet-am-logging-verify-period-in-seconds`

Log Signature Time

When secure logging is enabled, set this to how often OpenAM signs log file content (in seconds).

ssoadm attribute: `iplanet-am-logging-signature-period-in-seconds`

Secure Logging

Set this to `ON` to enable the secure logging system whereby OpenAM digitally signs and verifies log files. You must also set up the Logging Certificate Store for this feature to function.

ssoadm attribute: `iplanet-am-logging-security-status`

Secure Logging Signing Algorithm

Set this to the algorithm used for digitally signing log records.

ssoadm attribute: `iplanet-am-logging-secure-signing-algorithm`

Logging Certificate Store Location

The secure logging system uses the certificate with alias `Logger` that it finds in the key store specified by this path. The default is `%BASE_DIR%/%SERVER_URI%/Logger.jks`.

ssoadm attribute: `iplanet-am-logging-secure-certificate-store`

Maximum Number of Records

Set this to the maximum number of records read from the logs through the Logging API.

ssoadm attribute: `iplanet-am-logging-max-records`

Number of Files per Archive

Set this to the number of files to be archived by the secure logging system.

ssoadm attribute: `iplanet-am-logging-files-per-keystore`

Buffer Size

The number of log messages buffered in memory before OpenAM flushes them to the log file or the database.

ssoadm attribute: `iplanet-am-logging-buffer-size`

DB Failure Memory Buffer Size

Set this to the maximum number of log records to hold in memory if the database to which records are logged is unavailable. If the value is less than Buffer Size, that value takes precedence.

ssoadm attribute: `sun-am-logging-db-max-in-mem`

Buffer Time

Set the time in seconds that OpenAM buffers log messages in memory before flushing the buffer when Time Buffering is ON. The default is 60 seconds.

ssoadm attribute: `iplanet-am-logging-buffer-time-in-seconds`

Time Buffering

Set this to OFF to cause OpenAM to write each log message separately rather than the default of holding messages in a memory buffer that OpenAM flushes periodically, as specified using the Buffer Time attribute.

ssoadm attribute: `iplanet-am-logging-time-buffering-status`

Logging Level

Set the log level for OpenAM. `OFF` is equivalent to setting the status to `INACTIVE`.

ssoadm attribute: `sun-am-log-level`

Monitoring

You enable OpenAM monitoring by using these attributes.

ssoadm service name: `iPlanetAMMonitoringService`

Monitoring Status

Enable monitoring using this attribute.

ssoadm attribute: `iplanet-am-monitoring-enabled`

Monitoring HTTP Port

Set the port number for the HTML monitoring interface.

ssoadm attribute: `iplanet-am-monitoring-http-port`

Monitoring HTTP interface status

Enable the HTML monitoring interface using this attribute.

ssoadm attribute: `iplanet-am-monitoring-http-enabled`

Monitoring HTTP interface authentication file path

Set this to path to indicate the file indicating the user name and password used to protect access to monitoring information. The default user name password combination is `demo` and `changeit`. You can encode a new password using the **ampassword**command.

ssoadm attribute: `iplanet-am-monitoring-authfile-path`

Monitoring RMI Port

Set the port number for the JMX monitoring interface.

ssoadm attribute: `iplanet-am-monitoring-rmi-port`

Monitoring RMI interface status

Enable the JMX monitoring interface using this attribute.

ssoadm attribute: `iplanet-am-monitoring-rmi-enabled`

Monitoring SNMP Port

Set the port number for the SNMP monitoring interface.

ssoadm attribute: `iplanet-am-monitoring-snmp-port`

Monitoring SNMP interface status

Enable the SNMP monitoring interface using this attribute.

ssoadm attribute: `iplanet-am-monitoring-snmp-enabled`

Naming

You can configure URLs for service endpoints.

ssoadm service name: `iPlanetAMNamingService`

Profile Service URL

Set the endpoint used by the profile service.

This attribute is deprecated.

ssoadm attribute: `iplanet-am-naming-profile-url`

Session Service URL

Set the endpoint used by the session service.

ssoadm attribute: `iplanet-am-naming-session-url`

Logging Service URL

Set the endpoint used by the logging service.

ssoadm attribute: `iplanet-am-naming-logging-url`

Policy Service URL

Set the endpoint used by the policy service.

ssoadm attribute: `iplanet-am-naming-policy-url`

Authentication Service URL

Set the endpoint used by the authentication service.

ssoadm attribute: `iplanet-am-naming-auth-url`

SAML Web Profile/Artifact Service URL

Set the SAML v1 endpoint.

ssoadm attribute: `iplanet-am-naming-samlawareservlet-url`

SAML SOAP Service URL

Set the endpoint used by the SAML v1 SOAP service.

ssoadm attribute: `iplanet-am-naming-samlsoapreceiver-url`

SAML Web Profile/POST Service URL

Set the SAML v1 Web Profile endpoint.

ssoadm attribute: `iplanet-am-naming-samlpostservlet-url`

SAML Assertion Manager Service URL

Set the endpoint used by the SAML v1 assertion service.

ssoadm attribute: `iplanet-am-naming-samlassertionmanager-url`

Federation Assertion Manager Service URL

Set the endpoint used by the ID-FF assertion manager service.

ssoadm attribute: `iplanet-am-naming-fsassertionmanager-url`

Security Token Manager URL

Set the STS endpoint.

ssoadm attribute: `iplanet-am-naming-securitytokenmanager-url`

JAXRPC Endpoint URL

Set the JAXRPC endpoint used by remote IDM/SMS APIs.

FORGEROCK

ssoadm attribute: `iplanet-am-naming-jaxrpc-url`

Identity Web Services Endpoint URL

Set the endpoint for Identity WSDL services.

ssoadm attribute: `sun-naming-idsvcs-jaxws-url`

Identity REST Services Endpoint URL

Set the endpoint used for Identity REST services.

ssoadm attribute: `sun-naming-idsvcs-rest-url`

Security Token Service Endpoint URL

Set the STS endpoint.

ssoadm attribute: `sun-naming-sts-url`

Security Token Service MEX Endpoint URL

Set the STS MEX endpoint.

ssoadm attribute: `sun-naming-sts-mex-url`

Platform

You can configure the default locale and list of cookie domains.

ssoadm service name: `iPlanetAMPlatformService`

Platform Locale

Set the fallback locale used when the user locale cannot be determined.

ssoadm attribute: `iplanet-am-platform-locale`

Cookie Domains

Set the list of domains into which OpenAM writes cookies. If you set multiple cookie domains, OpenAM still only sets the cookie in the domain the client uses to access OpenAM. You can also configure cross domain single sign on (CDSSO) to allow single sign on across multiple domains managed by your organization. See the *Administration Guide* chapter on *Configuring Cross-Domain Single Sign On* in the *Administration Guide* for details.

ssoadm attribute: `iplanet-am-platform-cookie-domains`

1.4. Global Configuration

Under Configuration > Global you can set defaults for a range of federation services, for password reset, for policy configuration, for session management, and for dynamic user attributes.

Common Federation Configuration

ssoadm service name: `sunFAMFederationCommon`

Datastore SPI implementation class

Used by the Federation system to access user profile attributes

ssoadm attribute: `DatastoreClass`

ConfigurationInstance SPI implementation class

Used by the Federation system to access service configuration

ssoadm attribute: `ConfigurationClass`

Logger SPI implementation class

Used by the Federation system to record log messages

ssoadm attribute: `LoggerClass`

SessionProvider SPI implementation class

Used by the Federation system to access the session service

ssoadm attribute: `SessionProviderClass`

Maximum allowed content length

Maximum number of bytes for Federation communications

ssoadm attribute: `MaxContentLength`

PasswordDecoder SPI implementation class

Used by the Federation system to decode passwords encoded by OpenAM

ssoadm attribute: `PasswordDecoderClass`

SignatureProvider SPI implementation class

Used by the Federation system digitally to sign SAML documents

ssoadm attribute: `SignatureProviderClass`

KeyProvider SPI implementation class

Used by the Federation system to access the Java key store

ssoadm attribute: `KeyProviderClass`

Check presence of certificates

If enabled, OpenAM checks that the partner's signing certificate presented in the XML matches the certificate from the partner's metadata

ssoadm attribute: `CheckCert`

XML canonicalization algorithm

Algorithm used to render the canonical versions of XML documents

ssoadm attribute: `CannonicalizationAlgorithm`

XML signature algorithm

Algorithm used to sign XML documents

ssoadm attribute: `SignatureAlgorithm`

XML transformation algorithm

Algorithm used for XML transformations

ssoadm attribute: `TransformationAlgorithm`

SAML Error Page URL

OpenAM redirects users here when an error occurs in the SAML2 engine. Users are redirected to absolute URLs, whereas releative URLs are displayed within the request.

ssoadm attribute: `SAMLErrorPageURL`

SAML Error Page HTTP Binding

Set this either to `HTTP-Redirect` or to `HTTP-POST`.

ssoadm attribute: `SAMLErrorPageHTTPBinding`

Monitoring Agent Provider Class

Used by the Federation system to access the monitoring system

ssoadm attribute: `MonAgentClass`

Monitoring Provider Class for SAML1

Used by the SAMLv1 engine to access the monitoring system

ssoadm attribute: `MonSAML1Class`

Monitoring Provider Class for SAML2

Used by the SAML2 engine to access the monitoring system

ssoadm attribute: `MonSAML2Class`

Monitoring Provider Class for ID-FF

Used by the ID-FF engine to access the monitoring system

ssoadm attribute: `MonIDFFClass`

Dashboard Configuration

ssoadm service name: `dashboardService`

Dashboard Class Name

Identifies how to access the application, for example `SAML2ApplicationClass` for a SAML 2.0 application

ssoadm attribute: `dashboardClassName`

Dashboard Name

The application name as it will appear to the administrator for configuring the dashboard

ssoadm attribute: `dashboardName`

Dashboard Display Name

The application name that displays on the dashboard client

ssoadm attribute: `dashboardDisplayName`

Dashboard Icon

The icon name that will be displayed on the dashboard client identifying the application

ssoadm attribute: `dashboardIcon`

Dashboard Login

The URL that takes the user to the application

ssoadm attribute: `dashboardLogin`

Available Dashboard Apps

List of application dashboard names available by default for realms with the Dashboard configured

ssoadm attribute: `assignedDashboard`

Email Service

ssoadm service name: `ForgeRockSendEmailService`

Email Message Implementation Class

Specifies the class that sends email notifications, such as those sent for user registration and forgotten passwords.

Default: `org.forgerock.openam.services.email.MailServerImpl`

ssoadm attribute: `forgerockMailServerImplClassName`

Mail Server Host Name

Specifies the fully qualified domain name of the SMTP mail server through which to send email notifications.

Default: `smtp.gmail.com`

ssoadm attribute: `forgerockEmailServiceSMTPHostName`

Mail Server Host Port

Specifies the port number for the SMTP mail server.

Default: 465

ssoadm attribute: `forgerockEmailServiceSMTPHostPort`

Mail Server Authentication Username

Specifies the user name for the SMTP mail server.

Default: `forgerocksmtp`

ssoadm attribute: `forgerockEmailServiceSMTPUserName`

Mail Server Authentication Password

Specifies the password for the SMTP user name.

ssoadm attribute: `forgerockEmailServiceSMTPUserPassword`

Mail Server Secure Connection

Specifies whether to connect to the SMTP mail server using SSL.

Default: use SSL (`true`)

ssoadm attribute: `forgerockEmailServiceSMTPSSLEnabled`

Email From Address

Specifies the address from which to send email notifications.

Default: `no-reply@openam.org`

ssoadm attribute: `forgerockEmailServiceSMTPFromAddress`

Email Attribute Name

Specifies the profile attribute from which to retrieve the end user's email address.

Default: `mail`

ssoadm attribute: `openamEmailAttribute`

Email Subject

Specifies a subject for notification messages. If you do not set this OpenAM does not set the subject for notification messages.

ssoadm attribute: `forgerockEmailServiceSMTPSubject`

Email Content

Specifies content for notification messages. If you do not set this OpenAM includes only the confirmation URL in the mail body.

ssoadm attribute: `forgerockEmailServiceSMTPMessage`

Liberty ID-FF Service Configuration

ssoadm service name: `sunFAMIDFFConfiguration`

Federation Cookie Name

Cookie name for Liberty ID-FF

ssoadm attribute: `FedCookieName`

IDP Proxy Finder SPI implementation class

Used by the ID-FF engine to find the IDP proxy

ssoadm attribute: `IDPProxyFinderClass`

Request cache cleanup interval

Seconds between times OpenAM cleans up the request cache

ssoadm attribute: `RequestCacheCleanupInterval`

Request cache timeout

Seconds cached requests remain valid

ssoadm attribute: `RequestCacheTimeout`

IDP Login URL

Login URL for the ID-FF IDP

ssoadm attribute: `IDPLoginURL`

XML signing on

If yes, require XML signing.

ssoadm attribute: `XMLSigningOn`

Liberty Interaction Service

ssoadm service name: `sunFAMLibertyInteractionService`

WSP to redirect user for interaction

    ssoadm attribute: `WSPWillRedirect`

WSP to redirect user for interaction for data

    ssoadm attribute: `WSPWillRedirectForData`

WSP's expected duration for interaction

    ssoadm attribute: `WSPRedirectTime`

WSP to enforce that returnToURL must be SSL

    ssoadm attribute: `WSPWillEnforceHttpsCheck`

WSP to enforce return to host be the same as request host

    ssoadm attribute: `WSPWillEnforceReturnToHostEqualsRequestHost`

HTML style sheet location

    ssoadm attribute: `HTMLStyleSheetLocation`

WML style sheet location

    ssoadm attribute: `WMLStyleSheetLocation`

WSP interaction URL

> **ssoadm** attribute: `WSPRedirectHandlerURL`

WSP interaction URL if behind load balancer

> **ssoadm** attribute: `LBWSPRedirectHandler`

List of interaction URLs of WSP cluster (site) behind the load balancer

> **ssoadm** attribute: `TrustedWspRedirectHandlers`

Interaction Configuration Class

> **ssoadm** attribute: `InteractionConfigClass`

Options for WSC to participate in interaction

> **ssoadm** attribute: `WSCSpecifiedInteractionChoice`

WSC to include userInteractionHeader

> **ssoadm** attribute: `WSCWillIncludeUserInteractionHeader`

WSC to redirect user for interaction

> **ssoadm** attribute: `WSCWillRedirect`

WSC's expected duration for interaction

> **ssoadm** attribute: `WSCSpecifiedMaxInteractionTime`

WSC to enforce that redirection URL must be SSL

> **ssoadm** attribute: `WSCWillEnforceHttpsCheck`

Multi-Federation Protocol

ssoadm service name: `sunMultiFederationProtocol`

Single Logout Handler List

> List of logout handlers used for each different federation protocol

> **ssoadm** attribute: `SingleLogoutHandlerList`

OAuth2 Provider Configuration

ssoadm service name: `OAuth2Provider`

Authorization Code Lifetime

Lifetime of OAuth 2.0 authorization code in seconds.

ssoadm attribute: `forgerock-oauth2-provider-authorization-code-lifetime`

Refresh Token Lifetime

Lifetime of OAuth 2.0 refresh token in seconds.

ssoadm attribute: `forgerock-oauth2-provider-refresh-token-lifetime`

Access Token Lifetime

Lifetime of OAuth 2.0 access token in seconds.

ssoadm attribute: `forgerock-oauth2-provider-access-token-lifetime`

Issue Refresh Tokens

Whether to issue a refresh token when returning an access token.

ssoadm attribute: `forgerock-oauth2-provider-issue-refresh-token`

Scope Implementation Class

Name of class on OpenAM classpath implementing scopes.

ssoadm attribute: `forgerock-oauth2-provider-scope-implementation-class`

Response Type Plugins

List of plugins that handle the valid `response_type` values. OAuth 2.0 clients pass response types as parameters to the OAuth 2.0 Authorization end point (`/oauth2/authorize`) to indicate which grant type is requested from the provider. For example, the client passes `code` when requesting an authorization code, and `token` when requesting an access token.

Values in this list take the form *response-type|plugin-class-name*.

Defaults: `code|org.forgerock.restlet.ext.oauth2.flow.responseTypes.CodeResponseType`, `id_token|org.forgerock.restlet.ext.oauth2.flow.responseTypes`, `token|org.forgerock.restlet.ext.oauth2.flow.responseTypes.TokenResponseType`

ssoadm attribute: `forgerock-oauth2-provider-response-type-map-class`

User Profile Attribute(s) the Resource Owner is Authenticated On

Names of profile attributes that resource owners use to log in. The default is `uid`, and you can add others such as `mail`.

ssoadm attribute: `forgerock-oauth2-provider-authentication-attributes`

Shared Consent Attribute Name

Name of a multi-valued attribute on resource owner profiles where OpenAM can save authorization consent decisions. When the resource owner chooses to save the decision to authorize access for a client application, then OpenAM updates the resource owner's profile to avoid having to prompt the resource owner to grant authorization when the client issues subsequent authorization requests.

ssoadm attribute: `forgerock-oauth2-provider-saved-consent-attribute`

JSON Web Key URL

The URL where the OpenID Connect provider's JSON Web Key can be retrieved.

ssoadm attribute: `forgerock-oauth2-provider-jkws-uri`

ID Token Signing Algorithms supported

Algorithms supported to sign OpenID Connect `id_tokens`.

ssoadm attribute: `forgerock-oauth2-provider-id-token-signing-algorithms-supported`

Supported Claims

List of claims supported by the OpenID Connect `/oauth2/userinfo` endpoint.

ssoadm attribute: `forgerock-oauth2-provider-supported-claims`

Password Reset

Realm Attributes

See the *Administration Guide* chapter on *Configuring Password Reset* in the *Administration Guide* for details.

Policy Configuration

You can change global policy configuration, and the defaults per realm.

ssoadm service name: `iPlanetAMPolicyConfigService`

Resource Comparator

OpenAM uses resource comparators to match resources specified in policy rules. When setting comparators on the command line, separate fields with `|` characters.

ssoadm attribute: `iplanet-am-policy-config-resource-comparator`

Continue Evaluation on Deny Decision

If no, then OpenAM stops evaluating policy as soon as it reaches a deny decision.

ssoadm attribute: `iplanet-am-policy-config-continue-evaluation-on-deny-decision`

Advices Handleable by OpenAM

Lists advice names for which policy agents redirect users to OpenAM for further authentication and authorization

ssoadm attribute: `sun-am-policy-config-advices-handleable-by-am`

Realm Alias Referrals

If yes, then OpenAM allows creation of policies for HTTP and HTTPS resources whose FQDN matches the DNS alias for the realm even when no referral policy exists.

ssoadm attribute: `sun-am-policy-config-org-alias-mapped-resources-enabled`

Primary LDAP Server

Configuration directory server host:port that OpenAM searches for policy information

ssoadm attribute: `iplanet-am-policy-config-ldap-server`

LDAP Base DN

Base DN for policy searches

ssoadm attribute: `iplanet-am-policy-config-ldap-base-dn`

LDAP Users Base DN

Base DN for LDAP Users subject searches

ssoadm attribute: `iplanet-am-policy-config-ldap-users-base-dn`

OpenAM Roles Base DN

Base DN for OpenAM Roles searches

ssoadm attribute: `iplanet-am-policy-config-is-roles-base-dn`

LDAP Bind DN

Bind DN to connect to the directory server for policy information

ssoadm attribute: `iplanet-am-policy-config-ldap-bind-dn`

LDAP Bind Password

Bind password to connect to the directory server for policy information

ssoadm attribute: `iplanet-am-policy-config-ldap-bind-password`

LDAP Organization Search Filter

Search filter to match organization entries

ssoadm attribute: `iplanet-am-policy-config-ldap-organizations-search-filter`

LDAP Organization Search Scope

Search scope to find organization entries

ssoadm attribute: `iplanet-am-policy-config-ldap-organizations-search-scope`

LDAP Groups Search Filter

Search filter to match group entries

ssoadm attribute: `iplanet-am-policy-config-ldap-groups-search-filter`

LDAP Groups Search Scope

Search scope to find group entries

ssoadm attribute: `iplanet-am-policy-config-ldap-groups-search-scope`

LDAP Users Search Filter

Search filter to match user entries

ssoadm attribute: `iplanet-am-policy-config-ldap-users-search-filter`

LDAP Users Search Scope

Search scope to find user entries

ssoadm attribute: `iplanet-am-policy-config-ldap-users-search-scope`

LDAP Roles Search Filter

Search filter to match nsRole definition entries

ssoadm attribute: `iplanet-am-policy-config-ldap-roles-search-filter`

LDAP Roles Search Scope

Search scope to find nsRole definition entries

ssoadm attribute: `iplanet-am-policy-config-ldap-roles-search-scope`

OpenAM Roles Search Scope

Search scope to find OpenAM roles entries

ssoadm attribute: `iplanet-am-policy-config-is-roles-search-scope`

LDAP Organization Search Attribute

Naming attribute for organization entries

ssoadm attribute: `iplanet-am-policy-config-ldap-organizations-search-attribute`

LDAP Groups Search Attribute

Naming attribute for group entries

ssoadm attribute: `iplanet-am-policy-config-ldap-groups-search-attribute`

LDAP Users Search Attribute

Naming attribute for user entries

ssoadm attribute: `iplanet-am-policy-config-ldap-users-search-attribute`

LDAP Roles Search Attribute

Naming attribute for nsRole definition entries

ssoadm attribute: `iplanet-am-policy-config-ldap-roles-search-attribute`

Maximum Results Returned from Search

Search limit for LDAP searches

ssoadm attribute: `iplanet-am-policy-config-search-limit`

Search Timeout

Seconds after which OpenAM returns an error for an incomplete search

ssoadm attribute: `iplanet-am-policy-config-search-timeout`

LDAP SSL/TLS

If enabled, OpenAM connects securely to the directory server. This requires that you install the directory server certificate.

ssoadm attribute: `iplanet-am-policy-config-ldap-ssl-enabled`

LDAP Connection Pool Minimum Size

Minimum number of connections in the pool

ssoadm attribute: `iplanet-am-policy-config-connection_pool_min_size`

LDAP Connection Pool Maximum Size

Maximum number of connections in the pool

ssoadm attribute: `iplanet-am-policy-config-connection_pool_max_size`

Selected Policy Subjects

Lists subjects available for policy definition in realms

ssoadm attribute: `iplanet-am-policy-selected-subjects`

Selected Policy Conditions

Lists conditions available for policy definition in realms

ssoadm attribute: `iplanet-am-policy-selected-conditions`

Selected Policy Referrals

Lists referral types available for policy definition in realms

ssoadm attribute: `iplanet-am-policy-selected-referrals`

Subjects Result Time to Live

Maximum minutes OpenAM caches a subject result for evaluating policy requests. A value of 0 prevents OpenAM from caching subject evaluations for policy decisions.

Default: 10

ssoadm attribute: `iplanet-am-policy-config-subjects-result-ttl`

User Alias

If enabled, OpenAM can evaluate policy for remote users aliased to local users.

ssoadm attribute: `iplanet-am-policy-config-user-alias-enabled`

Selected Response Providers

Lists available response providers available for policy definition

ssoadm attribute: `sun-am-policy-selected-responseproviders`

Selected Dynamic Response Attributes

Lists dynamic response attributes available for policy definition

ssoadm attribute: `sun-am-policy-dynamic-response-attributes`

REST Security

ssoadm service name: `RestSecurity`

The order of options that appear in the console may vary depending on whether you are running from a new installation or an upgrade of OpenAM.

Self-Registration for Users

If enabled, new users can sign up using a REST API client.

Default: not enabled

ssoadm attribute: `forgerockRESTSecuritySelfRegistrationEnabled`

Self-Registration Token LifeTime (seconds)

Maximum life time for the token allowing user self-registration using the REST API.

Default: 900 (seconds)

ssoadm attribute: `forgerockRESTSecuritySelfRegTokenTTL`

Self-Registration Confirmation Email URL

This page handles the HTTP GET request when the user clicks the link sent by email in the confirmation request.

Default: *deployment-base-url*`/XUI/confirm.html` where *deployment-base-url* is something like `https://openam.example.com:8443/openam`

ssoadm attribute: `forgerockRESTSecuritySelfRegConfirmationUrl`

Forgot Password for Users

If enabled, users can assign themselves a new password using a REST API client.

Default: not enabled

ssoadm attribute: `forgerockRESTSecurityForgotPasswordEnabled`

Forgot Password Token LifeTime (seconds)

Maximum life time for the token allowing user to process a forgotten password using the REST API.

Default: 900 (seconds)

ssoadm attribute: `forgerockRestSecurityForgotPassTokenTTL`

Forgot Password Confirmation Email URL

This page handles the HTTP GET request when the user clicks the link sent by email in the confirmation request.

Default: `deployment-base-url/XUI/confirm.html` where *deployment-base-url* is something like `https://openam.example.com:8443/openam`

ssoadm attribute: `forgerockRESTSecurityForgotPassConfirmationUrl`

SAMLv2 Service Configuration

ssoadm service name: `sunFAMSAML2Configuration`

Cache cleanup interval

Seconds between cache cleanup operations

ssoadm attribute: `CacheCleanupInterval`

Attribute name for Name ID information

User entry attribute to store name identifier information

ssoadm attribute: `NameIDInfoAttribute`

Attribute name for NAME ID information key

User entry attribute to store the name identifier key

ssoadm attribute: `NameIDInfoKeyAttribute`

Cookie domain for IDP Discovery Service

Specifies the cookie domain for the IDP discovery service

ssoadm attribute: `IDPDiscoveryCookieDomain`

Cookie type for IDP Discovery Service

Indicates whether to use PERSISTENT or SESSION cookies

ssoadm attribute: `IDPDiscoveryCookieType`

URL scheme for IDP Discovery Service

Indicates whether to use HTTP or HTTPS

ssoadm attribute: `IDPDiscoveryURLScheme`

XML Encryption SPI implementation class

Used by the SAML2 engine to encrypt and decrypt documents

ssoadm attribute: `XMLEncryptionClass`

Include xenc:EncryptedKey Inside ds:KeyInfo Element

ssoadm attribute: `EncryptedKeyInKeyInfo`

XML Signing SPI implementation class

Used by the SAML2 engine to sign documents

ssoadm attribute: `XMLSigningClass`

XML Signing Certificate Validation

If enabled, then validate certificates used to sign documents.

ssoadm attribute: `SigningCertValidation`

CA Certificate Validation

If enabled, then validate CA certificates.

ssoadm attribute: `CACertValidation`

Enable SAMLv2 failover

If enabled, the OpenAM can failover requests to another instance.

ssoadm attribute: `failOverEnabled`

Buffer length to decompress request

The size is specified in bytes.

ssoadm attribute: `bufferLength`

SAMLv2 SOAP Binding

ssoadm service name: `sunfmSAML2SOAPBindingService`

Request Handler List

List of handlers to deal with SAML2 requests bound to SOAP. The key for a request handler is the meta alias, whereas the class indicates the name of the class that implements the handler.

ssoadm attribute: `sunSAML2RequestHandlerList`

Security Token Service

ssoadm service name: `sunFAMSTSService`

Issuer

Specifies the name of the security token service

ssoadm attribute: `stsIssuer`

End Point

Specifies the STS service endpoint

ssoadm attribute: `stsEndPoint`

Lifetime for Security Token

Milliseconds the security token remains valid

ssoadm attribute: `stsLifetime`

Certificate Alias Name

Specifies the alias for the signing certificate

ssoadm attribute: `stsCertAlias`

STS End User Token Plugin class

Specifies the class that converts end user tokens

ssoadm attribute: `com.sun.identity.wss.sts.clientusertoken`

Security Mechanism

Lists credentials used to secure the token, and credentials OpenAM accepts in the incoming request

ssoadm attribute: `SecurityMech`

Authentication Chain

Specifies the authentication chain OpenAM applies for incoming requests for authenticated security tokens

ssoadm attribute: `AuthenticationChain`

User Credential

User name and password shared secrets to validate UserName tokens in incoming requests

ssoadm attribute: `UserCredential`

Detect Message Replay

If yes, then OpenAM checks for and rejects replayed messages.

ssoadm attribute: `DetectMessageReplay`

Detect User Token Replay

If yes, then OpenAM checks for and rejects replayed user tokens.

ssoadm attribute: `DetectUserTokenReplay`

Is Request Signature Verified

If yes, then OpenAM verifies signatures on incoming requests.

ssoadm attribute: `isRequestSign`

Is Response Signed Enabled

If yes, then OpenAM signs the selected parts of the response.

ssoadm attribute: `isResponseSign`

Signing Reference Type

Specifies the reference type used to sign the response. One of `DirectReference`, `KeyIdentifierRef`, or `X509IssuerSerialRef`.

ssoadm attribute: `SigningRefType`

Is Request Decrypted

If yes, then OpenAM decrypts the selected parts of the request.

ssoadm attribute: `isRequestEncrypt`

Is Response Encrypted

If yes, then OpenAM encrypts responses.

ssoadm attribute: `isResponseEncrypt`

Encryption Algorithm

Specifies the algorithm used to encrypt responses

ssoadm attribute: `EncryptionAlgorithm`

Private Key Alias

Alias for the private key used to sign responses and decrypt requests

ssoadm attribute: `privateKeyAlias`

Private Key Type

Type of private key. One of `publicKey`, `symmetricKey`, or `noProofKey`.

ssoadm attribute: `privateKeyType`

Public Key Alias of Web Service Client

Alias for the certificate used to verify request signatures and encrypt responses

ssoadm attribute: `publicKeyAlias`

Kerberos Domain Server

Specifies the FQDN of the KDC

ssoadm attribute: `KerberosDomainServer`

Kerberos Domain

Specifies the domain name of the KDC

ssoadm attribute: `KerberosDomain`

Kerberos Service Principal

Specifies the Kerberos principal who owns the generated token. Use the format `HTTP/`*`host.domain@kdc-domain`*.

ssoadm attribute: `KerberosServicePrincipal`

Kerberos Key Tab File

Specifies the key tab file used to issue the token

ssoadm attribute: `KerberosKeyTabFile`

Is Verify Kerberos Signature

If yes, then OpenAM requires signed Kerberos tokens.

ssoadm attribute: `isVerifyKrbSignature`

SAML Attribute Mapping

Lists attribute mappings for generated assertions

This attribute applies when OpenAM acts as a WSP, receiving a SAML token or assertion generated by another STS.

ssoadm attribute: `SAMLAttributeMapping`

NameID Mapper

Specifies the NameID mapper for generated assertions

This attribute applies when OpenAM acts as a WSP, receiving a SAML token or assertion generated by another STS.

ssoadm attribute: `NameIDMapper`

Should Include Memberships

If yes, then OpenAM requires generated assertions include user memberships.

This attribute applies when OpenAM acts as a WSP, receiving a SAML token or assertion generated by another STS.

ssoadm attribute: `includeMemberships`

Attribute Namespace

Specifies the namespace for generated assertions

This attribute applies when OpenAM acts as a WSP, receiving a SAML token or assertion generated by another STS.

ssoadm attribute: `AttributeNamespace`

Trusted Issuers

Lists issuers OpenAM can trust to send security tokens

ssoadm attribute: `trustedIssuers`

Trusted IP Addresses

Lists issuer IP address that OpenAM can trust to send security tokens

ssoadm attribute: `trustedIPAddresses`

Session

ssoadm service name: `iPlanetAMSessionService`

Secondary Configuration Instance

When session failover is configured, you can set up additional configurations for connecting to the session repository here.

Maximum Number of Search Results

Maximum number of results from a session search

ssoadm attribute: `iplanet-am-session-max-session-list-size`

Timeout for Search

Seconds after which OpenAM sees an incomplete search as having failed

ssoadm attribute: `iplanet-am-session-session-list-retrieval-timeout`

Enable Property Change Notifications

If on, then OpenAM notifies other applications participating in SSO when a session property in the Notification Properties list changes.

ssoadm attribute: `iplanet-am-session-property-change-notification`

Enable Quota Constraints

If on, then OpenAM allows you to set constraints on user sessions.

ssoadm attribute: `iplanet-am-session-enable-session-constraint`

Read Timeout for Quota Constraint

Milliseconds after which OpenAM considers a search for live session count as having failed if quota constraints are enabled

ssoadm attribute: `iplanet-am-session-constraint-max-wait-time`

Resulting behavior if session quota exhausted

You can either set the next expiring session to be destroyed, `DESTROY_NEXT_EXPIRING`, the oldest session to be destroyed, `DESTROY_OLDEST_SESSION`, all previous sessions to be destroyed, `DESTROY_OLD_SESSIONS`, or deny the new session creation request, `DENY_ACCESS`.

ssoadm attribute: `iplanet-am-session-constraint-resulting-behavior`

Deny user login when session repository is down

This attribute takes effect when quota constraints are enabled.

ssoadm attribute: `iplanet-am-session-deny-login-if-db-is-down`

Notification Properties

Lists session properties for which OpenAM can send notifications upon modification

ssoadm attribute: `iplanet-am-session-notification-property-list`

DN Restriction Only Enabled

If enabled, OpenAM does not perform DNS lookups when checking restrictions in cookie hijacking mode.

ssoadm attribute: `iplanet-am-session-dnrestrictiononly`

Enable Session Trimming

If yes, then OpenAM stores only a limited set of session properties after session timeout and before session purging.

ssoadm attribute: `iplanet-am-session-enable-session-trimming`

Session Timeout Handler implementations

Lists plugin classes implementing session timeout handlers

ssoadm attribute: `openam-session-timeout-handler-list`

Maximum Session Time

Maximum minutes a session can remain valid before OpenAM requires the user to authenticate again

ssoadm attribute: `iplanet-am-session-max-session-time`

Maximum Idle Time

Maximum minutes a session can remain idle before OpenAM requires the user to authenticate again

ssoadm attribute: `iplanet-am-session-max-idle-time`

Maximum Caching Time

Maximum minutes before OpenAM refreshes a session that has been cached

ssoadm attribute: `iplanet-am-session-max-caching-time`

Active User Sessions

Maximum number of concurrent sessions OpenAM allows a user to have

ssoadm attribute: `iplanet-am-session-quota-limit`

User

ssoadm service name: `iPlanetAMUserService`

User Preferred Timezone

Time zone for accessing OpenAM console

ssoadm attribute: `preferredtimezone`

Administrator DN Starting View

Specifies the DN for the initial screen when the OpenAM administrator successfully logs in to the OpenAM console

ssoadm attribute: `iplanet-am-user-admin-start-dn`

Default User Status

Inactive users cannot authenticate, though OpenAM stores their profiles. Default: `Active`

ssoadm attribute: `iplanet-am-user-login-status`

1.5. Servers and Sites Configuration

Under Configuration > Servers and Sites you can manage server defaults, configuration for OpenAM server instances, and site configurations when using multiple OpenAM server instances.

To change inherited settings that appear read only for a server, click Default Server Settings on the Servers and Sites tab page to access and adjust the defaults, or change the Inheritance Settings for a specific server.

After changing server configurations, restart OpenAM or the web application container where OpenAM runs for the changes to take effect.

Servers > General

The General tab lets you access the settings to inherit, set the site for the server, and also set system, debug, and mail server attributes.

Parent Site

Select the site from the list. You must first create at least one site.

Base installation directory

OpenAM writes the configuration data and logs here.

property: `com.iplanet.services.configpath`

Default Locale

The locale used when none is requested.

property: `com.iplanet.am.locale`

Notification URL

The notification service endpoint.

property: `com.sun.identity.client.notification.url`

XML Validation

If on, then OpenAM validates XML documents that it parses.

property: `com.iplanet.am.util.xml.validating`

Debug Level

Set the log level shared across components for debug logging.

property: `com.iplanet.services.debug.level`

Merge Debug Files

If on, then OpenAM writes all debug log messages to a single file, `debug.out`. By default, OpenAM writes a debug log per component.

property: `com.iplanet.services.debug.mergeall`

Debug Directory

File system directory where OpenAM writes debug logs.

property: `com.iplanet.services.debug.directory`

Mail Server Host Name

SMTP host name for email sent by OpenAM.

property: `com.iplanet.am.smtphost`

Mail Server Port Number

SMTP port number for email sent by OpenAM.

property: `com.iplanet.am.smtpport`

Servers > Security

Most security settings are inherited by default.

Password Encryption Key

Encryption key for decrypting stored passwords.

The value of the `am.encryption.pwd` property must be the same for all deployed servers in a site. You can set this property on the OpenAM console at Servers and Sites > Server > Security > Password Encryption Key. Verify that all servers have the same setting for this property.

Example: `TF1Aue9c63bWTTY4mmZJeFYubJbNiSE3`

property: `am.encryption.pwd`

Authentication Service Shared Secret

Shared secret for application authentication

Example: `AQICQ7QMKN5TSt1fpyFZBMZ8hRwkYkkrUaFk`

property: `com.iplanet.am.service.secret`

Encryption class

Default class used to handle encryption

Default: `com.iplanet.services.util.JCEEncryption`

property: `com.iplanet.security.encryptor`

Secure Random Factory Class

The default implementation uses pure Java, rather than JSS.

Default: `com.iplanet.am.util.SecureRandomFactoryImpl`

property: `com.iplanet.security.SecureRandomFactorImpl`

Platform Low Level Comm. Max. Content Length

Maximum content length for an HTTP request

Default: 16384

property: `com.iplanet.services.comm.server.pllrequest.maxContentLength`

Client IP Address Check

If yes, then OpenAM checks client IP addresses when creating and validating SSO tokens.

Default: No

property: `com.iplanet.am.clientIPCheckEnabled`

Cookie Name

Cookie name OpenAM uses to set a session handler ID during authentication.

Default: `iPlanetDirectoryPro`

property: `com.iplanet.am.cookie.name`

Secure Cookie

If yes, then OpenAM sets the cookie in secure mode such that the browser only returns the cookie if a secure protocol such as HTTPS is used.

Default: No

property: `com.iplanet.am.cookie.secure`

Encode Cookie Value

If yes, then OpenAM URL encodes cookie values.

Default: No

property: `com.iplanet.am.cookie.encode`

Keystore File

Path to OpenAM key store file

Default: Path to `keystore.jks`, located in the directory that holds the OpenAM configuration.

Example: `~/openam/openam/keystore.jks`

property: `com.sun.identity.saml.xmlsig.keystore`

Keystore Password File

Path to password file for key store

Default: Path to `.storepass`, located in the directory that holds the OpenAM configuration.

Example: `~/openam/openam/.storepass`

property: `com.sun.identity.saml.xmlsig.storepass`

Private Key Password File

Path to password file for OpenAM private key

Default: Path to `.keypass`, located in the directory that holds the OpenAM configuration.

Example: `~/openam/openam/.keypass`

property: `com.sun.identity.saml.xmlsig.keypass`

Certificate Alias

Alias for OpenAM certificate stored in key store

Not set by default

property: `com.sun.identity.saml.xmlsig.certalias`

CRL: LDAP server host name

Directory server host name where the certificate revocation list (CRL) is cached

Not set by default

property: `com.sun.identity.crl.cache.directory.host`

CRL: LDAP server port number

Directory server port number where the certificate revocation list is cached

Not set by default

property: `com.sun.identity.crl.cache.directory.port`

CRL: SSL/TLS Enabled

If yes, then connect securely when accessing the CRL cache directory server

Default: No

property: `com.sun.identity.crl.cache.directory.ssl`

CRL: LDAP server bind user name

Bind DN to access CRL cache directory server

Not set by default

property: `com.sun.identity.crl.cache.directory.user`

CRL: LDAP server bind password

Bind password to access CRL cache directory server

Not set by default

property: `com.sun.identity.crl.cache.directory.password`

CRL: LDAP search base DN

Base DN under which to search for CRL

Not set by default

property: `com.sun.identity.crl.cache.directory.searchlocs`

CRL: Search Attributes

DN component of issuer's subject DN used to retrieve the CRL

Not set by default

property: `com.sun.identity.crl.cache.directory.searchattr`

OCSP: Check Enabled

If yes, then OpenAM runs Online Certificate Status Protocol (OCSP) checks.

Default: Yes

property: `com.sun.identity.authentication.ocspCheck`

Responder URL

URL for OCSP responder

Not set by default

property: `com.sun.identity.authentication.ocsp.responder.url`

Certificate Nickname

Nickname for OCSP responder certificate

Not set by default

property: `com.sun.identity.authentication.ocsp.responder.nickname`

FIPS Mode

If yes, then OpenAM runs in Federal Information Processing Standards mode.

Default: No

property: `com.sun.identity.security.fipsmode`

Servers > Session

Session settings are inherited by default.

Maximum Sessions

Maximum concurrent sessions OpenAM permits

property: `com.iplanet.am.session.maxSessions`

Invalidate Session Max Time

Minutes after which invalid sessions are removed from the session table

property: `com.iplanet.am.session.invalidsessionmaxtime`

Sessions Purge Delay

Minutes OpenAM delays session purging

property: `com.iplanet.am.session.purgedelay`

Logging Interval

Seconds OpenAM delays between logging sessions statistics

property: `com.iplanet.am.stats.interval`

State

Whether to write statistics to a `file`, to the `console`, or to turn recording `off`

property: `com.iplanet.services.stats.state`

Directory

Path to statistics logs directory

property: `com.iplanet.services.stats.directory`

Enable Host Lookup

If yes, then OpenAM performs host lookup during session logging.

property: `com.sun.am.session.enableHostLookUp`

Notification Pool Size

Number of threads in the notification pool

property: `com.iplanet.am.notification.threadpool.size`

Notification Thread Pool Threshold

Maximum number of tasks in the queue for serving notification threads

property: `com.iplanet.am.notification.threadpool.threshold`

Case Insensitive client DN comparison

If yes, then OpenAM distinguished name comparison is case insensitive.

property: `com.sun.am.session.caseInsensitiveDN`

Servers > SDK

Most SDK settings are inherited.

Enable Datastore Notification

If yes, then OpenAM uses datastore notification. Otherwise, OpenAM uses in-memory notification.

property: `com.sun.identity.sm.enableDataStoreNotification`

Enable Directory Proxy

If yes, then OpenAM accounts for the use of a directory proxy to access the directory server.

property: `com.sun.identity.sm.ldap.enableProxy`

Notification Pool Size

Service management notification thread pool size

property: `com.sun.identity.sm.notification.threadpool.size`

Number of retries for Event Service connections

Maximum number of attempts to reestablish Event Service connections

property: `com.iplanet.am.event.connection.num.retries`

Delay between Event Service connection retries

Milliseconds between attempts to reestablish Entry Service connections

property: `com.iplanet.am.event.connection.delay.between.retries`

Error codes for Event Service connection retries

LDAP error codes for which OpenAM retries rather than returning failure

property: `com.iplanet.am.event.connection.ldap.error.codes.retries`

Idle Time Out

Minutes after which OpenAM reestablishes idle persistent search connections

property: `com.sun.am.event.connection.idle.timeout`

Disabled Event Service Connection

Persistent search connections OpenAM can disable

property: `com.sun.am.event.connection.disable.list`

Number of retries for LDAP Connection

Maximum number of attempts to reestablish LDAP connections

property: `com.iplanet.am.ldap.connection.num.retries`

Delay between LDAP connection retries

Milliseconds between attempts to reestablish LDAP connections

property: `com.iplanet.am.ldap.connection.delay.between.retries`

Error Codes for LDAP connection retries

LDAP error codes for which OpenAM retries rather than returning failure

property: `com.iplanet.am.ldap.connection.ldap.error.codes.retries`

SDK Caching Max. Size

Cache size used if SDK caching is enabled

property: `com.iplanet.am.sdk.cache.maxSize`

SDK Replica Retries

Maximum number of attempts to retrieve entries returned as not found

property: `com.iplanet.am.replica.num.retries`

Delay between SDK Replica Retries

Milliseconds between attempts to retrieve entries through the SDK

property: `com.iplanet.am.replica.delay.between.retries`

Cache Entry Expiration Enabled

If no, then cache entries expire based on User Entry Expiration Time

property: `com.iplanet.am.sdk.cache.entry.expire.enabled`

User Entry Expiration Time

Minutes user entries remain valid after modification. When OpenAM accesses a user entry that has expired, it rereads the entry from the directory server.

property: `com.iplanet.am.sdk.cache.entry.user.expire.time`

Default Entry Expiration Time

Minutes non-user entries remain valid after modification

property: `com.iplanet.am.sdk.cache.entry.default.expire.time`

Servers > Directory Configuration

Use this tab to change connection settings and add additional LDAP configuration directory server instances.

Minimum Connection Pool

Set the minimum number of connections in the pool.

Maximum Connection Pool

Set the maximum number of connections in the pool.

Bind DN

Set the bind DN to connect to the configuration directory servers.

Bind Password

Set the bind password to connect to the configuration directory servers.

Servers > CTS

The Core Token Service (CTS) does not need to be configured in the same LDAP storage as the external or embedded user store. The CTS can instead be configured on its own external directory server. There are some specific requirements for indexing and replication which need to be accounted for. In particular, WAN replication is an important consideration which needs to be handled carefully for optimum performance.

You may also choose to set advanced properties related to token size, including `com.sun.identity.session.repository.enableEncryption`, `com.sun.identity.session.repository.enableCompression`, and `com.sun.identity.session.repository.enableAttributeCompression`. For more information, identify these variables in the following section: Servers > Advanced.

Default Token Store

If selected, CTS tokens are stored in the same external or embedded datastore as is used on an OpenAM configuration store. If you use the default token store, you can only configure the `Root Suffix`. Associated with the `Directory Configuration` tab associated with individual servers.

External Token Store

If you use OpenDJ, you can separate the CTS from the configuration on different external servers. On the external CTS server, you can also configure token schema and indexes.

Root Suffix

For either the default or external token stores, enter the base DN for CTS storage information in LDAP format, such as `dc=cts,dc=forgerock,dc=com`. The `Root Suffix` would be a database that can be maintained and replicated separately from tha standard user datastore.

SSL/TLS Enabled

Access the directory service using StartTLS or LDAPS.

Directory Name

The hostname of the external server.

Port

Specifies the TCP/IP port number used for communication to to external datastore, such as 389 for LDAP.

Login Id

Specifies the user, in DN format, needed to authenticate. The user needs sufficient privileges to read and write to the root suffix of the external datastore.

Password

Specifies the password associated with the Login Id.

Max Connections

Notes the maximum number of remote connections to the external datastore.

Heartbeat

Specifies how often OpenAM should send a heartbeat request to the directory server to ensure that the connection does not remain idle, in seconds. Default: 10.

Servers > Advanced

Use this page to set advanced properties directly. A partial list of advanced properties follows.

For a list of inherited advanced properties, see the table under the Advanced tab for Default Server Settings.

`com.iplanet.am.cookie.c66Encode`

Properly URL encode session tokens.

Default: `true`

com.iplanet.am.cookie.timeToLive

`iplanetDirectoryPro` cookie lifetime if persistent, in hours

Default: 24

com.iplanet.am.daemons

Modules for which to open daemons at OpenAM startup.

Default: `securid`

com.iplanet.am.directory.ssl.enabled

Whether to connect to the configuration directory server over LDAPS.

Default: `false`

com.iplanet.am.installdir

OpenAM Configuration and log file location.

Default: `~/openam/`*`server-uri`*, such as `~/openam/openam`

com.iplanet.am.jssproxy.checkSubjectAltName

When using JSS, check whether the name values in the `SubjectAltName` certificate match the server FQDN.

Default: `false`

com.iplanet.am.jssproxy.resolveIPAddress

When using JSS, check that the IP address of the server resolves to the host name.

Default: `false`

com.iplanet.am.jssproxy.SSLTrustHostList

When using JSS, comma-separated list of server FQDNs to trust if they match the certificate CN, even if the domain name is not correct.

com.iplanet.am.jssproxy.trustAllServerCerts

When using JSS, set to `true` to trust whatever certificate is presented without checking.

Default: `true`

com.iplanet.am.lbcookie.name

Used with sticky load balancers that can inspect the cookie value.

Default: `amlbcookie`

com.iplanet.am.lbcookie.value

Used with sticky load balancers that can inspect the cookie value. Set this property to a unique value if your load balancer requires it. Restart OpenAM for the change to take effect.

Default: 01

com.iplanet.am.pcookie.name

Persistent cookie name.

Default: `DProPCookie`

com.iplanet.am.profile.host

Not used

Default: *server-host*, such as `openam.example.com`

com.iplanet.am.profile.port

Not used

Default: *server-port*, such as 8080 or 8443

com.iplanet.am.session.agentSessionIdleTime

Time in minutes after which a policy agent session expires.

Default: 0, meaning never time out. Range is 0-30 (minutes).

com.iplanet.am.session.client.polling.enable

Whether client applications such as policy agents poll for configuration changes. If `false`, then OpenAM notifies clients about changes.

Default: false

com.iplanet.am.session.client.polling.period

If client applications poll for changes, number of seconds between polls.

Default: 180

com.iplanet.am.session.failover.cluster.stateCheck.period

Time in milliseconds between health checks of other servers in the same site.

Default: 1000

com.iplanet.am.session.failover.cluster.stateCheck.timeout

Socket timeout in milliseconds for health checks of other servers in the same site.

Default: 1000

com.iplanet.am.session.httpSession.enabled

Create an `HttpSession` for users on successful authentication.

Default: `true`

com.iplanet.security.SSLSocketFactoryImpl

SSL socket factory implementation used by OpenAM.

Default: `com.sun.identity.shared.ldap.factory.JSSESocketFactory`, uses a pure Java provider

com.iplanet.services.cdc.invalidGotoStrings;

Strings that OpenAM rejects as values in `goto` query string parameters.

Default: `<,>javascript:,javascript%3a,%3c,%3e`

com.sun.embedded.replicationport

Replication port for embedded OpenDJ directory server.

Default: 8989

com.sun.embedded.sync.servers

Whether to replicate data between embedded directory servers.

Default: `on`

com.sun.identity.am.cookie.check

Whether to check for cookie support in the user agent, and if not to return an error.

Default: `false`

com.sun.identity.appendSessionCookieInURL

Whether to append the session cookie to URL for a zero page session.

Default: `true`

com.sun.identity.auth.cookieName

Cookie used by the OpenAM authentication service to handle the authentication process.

Default: `AMAuthCookie`

com.sun.identity.authentication.client.ipAddressHeader

Set the name of the HTTP header that OpenAM can examine to learn the client IP address when requests go through a proxy or load balancer. (When requests go through an HTTP proxy or load balancer, checking the IP address on the request alone returns the address of the proxy or load balancer rather than that of the client.) OpenAM must be able to trust the proxy or load balancer to set the client IP address correctly in the header specified.

Example: `com.sun.identity.authentication.client.ipAddressHeader=X-Forwarded-For`

com.sun.identity.authentication.multiple.tabs.used

Whether to allow users to open many browser tabs to the login page at the same time without encountering an error.

Default: `false`

com.sun.identity.authentication.setCookieToAllDomains

Whether to allow multiple cookie domains.

Default: `true`

com.sun.identity.authentication.special.users

List of special users always authenticated against the local directory server.

Default: `cn=dsameuser,ou=DSAME Users,dc=openam,dc=forgerock,dc=org|cn=amService-UrlAccessAgent,ou=DSAME Users,dc=openam,dc=forgerock,dc=org`

com.sun.identity.authentication.super.user

OpenAM privileged administrator user.

Default: `uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org`

com.sun.identity.authentication.uniqueCookieName

When cookie hijacking protection is configured, name of the cookie holding the URL to the OpenAM server that authenticated the user.

Default: `sunIdentityServerAuthNServer`

com.sun.identity.client.notification.url

Notification service endpoint for clients such as policy agents.

Default: *server-protocol*://*server-host*:*server-port*/*server-uri*/notificationservice, such as `https://openam.example.com:8443/openam/notificationservice`

`com.sun.identity.common.systemtimerpool.size`

Number of threads in the shared system timer pool used to schedule operations such as session timeout.

Default: 3

`com.sun.identity.cookie.httponly`

When set to `true`, mark cookies as HTTPOnly to prevent scripts and third-party programs from accessing the cookies.

Default: `false`

`com.sun.identity.enableUniqueSSOTokenCookie`

If `true`, then OpenAM is using protection against cookie hijacking.

Default: `false`

`com.sun.identity.jss.donotInstallAtHighestPriority`

Whether JSS should take priority over other providers.

Default: `true`

`com.sun.identity.monitoring`

Whether monitoring is active for OpenAM.

Default: `off`

`com.sun.identity.monitoring.local.conn.server.url`

URL for local connection to the monitoring service.

Default: `service:jmx:rmi://`

`com.sun.identity.password.deploymentDescriptor`

Internal property used by OpenAM.

Default: *server-uri*, such as `openam`

`com.sun.identity.policy.Policy.policy_evaluation_weights`

Weights of the cost of evaluating policy subjects, rules, and conditions. Evaluation is in order of heaviest weight to lightest weight.

Default: `10:10:10`, meaning evaluation of rules, then conditions, then subjects

com.sun.identity.policy.resultsCacheMaxSize

Maximum number of policy decisions OpenAM caches.

Default: 10000

com.sun.identity.server.fqdnMap

Enables virtual hosts, partial hostname and IP address. Maps invalid or virtual name keys to valid FQDN values for proper redirection.

To map `myserver` to `myserver.example.com`, set `com.sun.identity.server.fqdnMap[myserver]=myserver.example.com`.

com.sun.identity.session.repository.enableEncryption

Enables tokens to be encrypted when stored.

Multi-instance deployments require consistent use of this property, which should be done under the Servers and Sites > Default Server Settings > Advanced.

The `am.encryption.pwd` property must also be the same for all deployed instances. The `am.encryption.pwd` is under Servers and Sites > Server > Security > Password Encryption Key. You will need to verify that all servers have the same setting for this property as the default server.

Default: `false`

com.sun.identity.urlchecker.dorequest

Whether to perform an HTTP GET on `com.sun.identity.urlchecker.targeturl` as a health check against another server in the same site. If `false`, then OpenAM only checks the Socket connection, and does not perform an HTTP GET.

If each OpenAM server runs behind a reverse proxy, then setting this property to `true` means the health check actually runs against the OpenAM instance, rather than checking only the Socket to the reverse proxy.

Default: `false`

com.sun.identity.urlchecker.targeturl

URL to monitor when `com.sun.identity.urlchecker.dorequest` is set to `true`.

Default: URL to the `/openam/namingservice` endpoint on the remote server

com.sun.identity.security.checkcaller

Whether to perform a Java security permissions check for OpenAM.

Default: `false`

com.sun.identity.session.repository.enableEncryption

For CTS token encryption, if desired.

Default: false

com.sun.identity.session.repository.enableCompression

For GZip-based compression of CTS tokens, if desired.

Default: false

com.sun.identity.session.repository.enableAttributeCompression

For additional compression of CTS token JSON binaries, beyond GZip, if desired.

Default: false

com.sun.identity.sm.cache.ttl

When service configuration caching time-to-live is enabled, this sets the time to live in minutes.

Default: 30

com.sun.identity.sm.cache.ttl.enable

If service configuration caching is enabled, whether to enable a time-to-live for cached configuration.

Default: `false`

com.sun.identity.sm.flatfile.root_dir

File system directory to hold file-based representation of OpenAM configuration.

Default: `~/openam/`*`server-uri`*`/sms` such as `~/openam/openam/sms`

com.sun.identity.sm.sms_object_class_name

Class used to read and write OpenAM service configuration entries in the directory.

Default: `com.sun.identity.sm.ldap.SMSEmbeddedLdapObject`

com.sun.identity.url.readTimeout

Used to set the read timeout in milliseconds for HTTP and HTTPS connections to other servers.

Default: 30000

com.sun.identity.urlchecker.dorequest

Allows the OpenAM ClusterStateService to work with HTTPS endpoints.

Default: `true`

com.sun.identity.urlconnection.useCache

Whether to cache documents for HTTP and HTTPS connections to other servers.

Default: `false`

com.sun.identity.webcontainer

Name of the web container to correctly set character encoding, if necessary.

Default: `WEB_CONTAINER`

console.privileged.users

Used to assigned privileged console access to particular users. Set to a `|` separated list of users' Universal IDs, such as `console.privileged.users=uid=demo,ou=user,dc=openam,dc=forgerock,dc=org|uid=demo2,ou=user,dc=openam,dc=forgerock,dc=org`.

openam.auth.destroy_session_after_upgrade

Where to destroy the old session after a session is successfully upgraded.

Default: `true`

openam.auth.distAuthCookieName

Cookie used by the OpenAM distributed authentication service to handle the authentication process.

Default: `AMDistAuthCookie`

openam.auth.session_property_upgrader

Class that controls which session properties are copied during session upgrade, where default is to copy all properties to the upgraded session.

Default: `org.forgerock.openam.authentication.service.DefaultSessionPropertyUpgrader`

openam.auth.version.header.enabled

The X-DSAMEVersion http header provides detailed information about the version of OpenAM currently running on the system, including the build and date/time of the build. OpenAM will need to be restarted once this property is enabled.

Default: false

openam.authentication.ignore_goto_during_logout

Whether to ignore the `goto` query string parameter on logout, instead displaying the logout page.

Default: `false`

openam.cdm.default.charset

Character set used for globalization.

Default: `UTF-8`

openam.forbidden.to.copy.headers

Comma-separated list of HTTP headers not to copy when the distributed authentication server forwards a request to another distributed authentication server.

Default: `connection`

openam.forbidden.to.copy.request.headers

Comma-separated list of HTTP headers not to copy when the distributed authentication server forwards a request to another distributed authentication server.

Default: `connection`

openam.retained.http.headers

Comma-separated list of HTTP headers to copy to the forwarded response when the server forwards a request to another server.

Requests are forwarded when the server receiving the request is not the server that originally initiated authentication. The server that originally initiated authentication is identified by a cookie.

When the distributed authentication service (DAS) is in use, then the cookie is the `AMDistAuthCookie` that identifies the DAS server by its URL.

When authentication is done directly on OpenAM, then the cookie is the `AMAuthCookie` that holds a session ID that identifies the OpenAM server.

On subsequent requests the server receiving the request checks the cookie. If the cookie identifies another server, the current server forwards the request to that server.

If a header such as `Cache-Control` has been included in the list of values for the property `openam .retained.http.request.headers` and the header must also be copied to the response, then add it to the list of values for this property.

Example: `openam.retained.http.headers=X-DSAMEVersion,Cache-Control`

Default: `X-DSAMEVersion`

openam.retained.http.request.headers

Comma-separated list of HTTP headers to copy to the forwarded request when the server forwards a request to another server.

Requests are forwarded when the server receiving the request is not the server that originally initiated authentication. The server that originally initiated authentication is identified by a cookie.

When the distributed authentication service (DAS) is in use, then the cookie is the `AMDistAuthCookie` that identifies the DAS server by its URL.

When authentication is done directly on OpenAM, then the cookie is the `AMAuthCookie` that holds a session ID that identifies the OpenAM server.

On subsequent requests the server receiving the request checks the cookie. If the cookie identifies another server, the current server forwards the request to that server.

When configuring the distributed authentication service, or when a reverse proxy is set up to provide the client IP address in the `X-Forwarded-For` header, if your deployment includes multiple OpenAM servers, then this property must be set to include the header.

Example: `openam.retained.http.request.headers=X-DSAMEVersion,X-Forwarded-For`

OpenAM copies the header when forwarding a request to the authoritative server where the client originally began the authentication process, so that the authoritative OpenAM server receiving the forwarded request can determine the real client IP address.

In order to retain headers to return in the response to the OpenAM server that forwarded the request, use the property `openam.retained.http.headers`.

Default: `X-DSAMEVersion`

openam.session.allow_persist_am_cookie

If `true` users can extend the lifetime of the `iplanetDirectoryPro` cookie to `com.iplanet.am.cookie.timeToLive` on a per-session basis, by using the query string parameter `openam.session.persist_am_cookie=Yes`.

openam.session.case.sensitive.uuid

Whether universal user IDs are considered case sensitive when matching them.

Default: `false`

openam.session.persist_am_cookie

If `true` extend the lifetime of the `iplanetDirectoryPro` cookie to `com.iplanet.am.cookie.timeToLive`.

Default: false

openam.session.useLocalSessionsInMultiServerMode

This property is for use in multi-server deployments where session failover is not available. If `true`, calculate session quotas per server. In other words, if the session quota is 5 sessions and users can access up to 4 servers, they can have a maximum of 20 (5 * 4) sessions.

Default: `false`

opensso.protocol.handler.pkgs

If the web application containers sets `java.protocol.handler.pkgs`, then set this property to `com.sun.identity.protocol`.

org.forgerock.embedded.dsadminport

Administration port for embedded OpenDJ directory server.

Default: 4444

org.forgerock.openam.authentication.accountExpire.days

Days until account expiration set after successful authentication by the account expiration post authentication plugin.

Default: 30

securidHelper.ports

Port on which SecurID daemon listens.

Default: 58943

ssoadm.disabled

Set to `false` to enable `ssoadm.jsp`.

Default: `true`

Sites

Sites involve multiple OpenAM servers working together to provide services. You can use sites with load balancers and session failover to configure pools of servers capable of responding to client requests in highly available fashion.

Primary URL

Set the primary entry point to the site, such as the URL to the load balancer for the site configuration.

Secondary URLs

Set alternate entry points to the site. Used when session failover is configured.

Assigned Servers

Shows the list of OpenAM servers in the site.

Chapter 2
Log Files and Messages

This chapter gives information about the different log files and messages for OpenAM.

2.1. Log Files

This section describes the different OpenAM log files.

Administrative Log Files

Administrative logs record information on OpenAM events. You can adjust the amount of detail in the administrative logs under Configuration > System > Logging.

amAdmin.access

Contains log data about actions conducted by users logged in as amAdmin

amAdmin.error

Contains log data about errors encountered for users logged in as amAdmin

amAuthentication.access

Contains log data for when users log into and out of OpenAM, including failed authentications

amAuthentication.error

Contains log data about errors encountered when users login and out of OpenAM

amConsole.access

Contains data about actions run as the administrator in the console, including changes to realms and policies

amConsole.error

Contains data on errors encountered during administrator sessions

amPasswordReset.access

Contains data about password resets

amPolicy.access

Contains data about authorization actions permitted by policies, including policy creation, removal, or modification

amPolicy.error

Contains data on errors encountered during actions related to the policy

amPolicyDelegation.access

Contains data about actions as part of the policy delegation, including any changes to the delegation

amRemotePolicy.access

Contains data about policies accessed remotely

amSSO.access

Contains data about user sessions, including times of access, session time outs, and session creation/termination

CoreToken.access

Contains data about actions run against the core token

CoreToken.error

Contains data on errors encountered regarding the core token

COT.access

Contains data about the circle of trust

COT.error

Contains data on errors encountered for the circle of trust

Entitlement.access

Contains data about entitlement actions or changes

Federation.access

Contains data about federation events

Federation.error

Contains data on errors encountered while executing actions for federation

IDFF.access

Contains data about federation actions, including the creation of authentication domains or the hosted providers

IDFF.error

Contains data on errors encountered during federation actions

Liberty.access

Contains data about actions run for the federation Liberty schema

Liberty.error

Contains data on errors encountered for the federation Liberty schema

OAuth2Provider.access

Contains data about actions for the OAuth 2.0 provider

OAuth2Provider.error

Contains data about errors encountered by the OAuth 2.0 provider

SAML2.access

Contains data about SAML 2 actions, including changes to assertions, artifacts, response, and requests

SAML2.error

Contains data about errors encountered during SAML 2 actions

SAML.access

Contains data about SAML actions, including changes to assertions, artifacts, response, and requests

SAML.error

Contains data about errors encountered during SAML actions

ssoadm.access

Contains data about actions completed for SSO as admin

WebServicesSecurity.access

Contains data about activity for Web Services Security

WebServicesSecurity.error

Contains data on errors encountered by Web Services Security

WSFederation.access

Contains data about activity for WS Federation, including changes and access information

WSFederation.error

Contains data on errors encountered during WS Federation

Debug Log Files

Debug logs provide information that can help you troubleshoot. You can adjust the amount of detail in the debug logs under Configuration > System > Logging.

Authentication

Contains information about problems encountered during user authentication, including authentication services, framework, modules, callbacks, JAAS, and API

Configuration

Contains information about problems with the OpenAM configuration

CoreSystem

Contains information about problems specific to your core deployment of OpenAM that are not part of the authentication process or part of your current configuration, including core infrastructure services, PLL, cookies, naming, logging, and upgrades

Entitlement

Contains information about problems specific to entitlement

Federation

Contains information about problems specific to federation, including federated SSO, the federation protocols (SAML, SAML 2.0, ID-FF, and WS-Federation), metadata, hub, and circles of trust

IdRepo

Contains information about problems specific to the identity repository, including datastores and plugins

Policy

Contains information about problems specific to the policies you have setup, including policy framework, their subjects, conditions, resource attributes, plugins, and API

Session

Contains information about problems specific to OpenAM sessions, including session framework, management SSOToken, failover, and API

WebServices

Contains information about problems specific to Web Services, including STS and Identity Services

2.2. Log Messages

This section describes OpenAM log messages.

OpenAM logs the following COT messages.

INVALID_COT_NAME

ID: COT-1

Level: INFO

Description: Invalid circle of trust name.

Data: Realm or organization name, Circle of Trust Name

Triggers: Accessing the circle of trust.

Actions: Check the name and retry accessing the circle of trust.

CONFIG_ERROR_MODIFY_COT_DESCRIPTOR

ID: COT-2

Level: INFO

Description: Configuration error modifying the circle of trust.

Data: Error message, Name of the circle of trust, Realm or organization name

Triggers: Modifying the circle of trust.

Actions: Check COT debug , fmCOT, for more detailed error message.

CONFIG_ERROR_GET_ALL_COT_DESCRIPTOR

ID: COT-3

Level: INFO

Description: Error retreiving all circle of trusts.

Data: Error message, Realm or organization name

Triggers: Getting all circle of trust.

Actions: Check configuration; check debug for more detailed error message.

NO_COT_NAME_CREATE_COT_DESCRIPTOR

ID: COT-4

Level: INFO

Description: Invalid name , error creating the circle of trust.

Data: Realm or organization name

Triggers: Creating the circle of trust.

Actions: Check the name to create circle of trust descriptor.

COT_EXISTS_CREATE_COT_DESCRIPTOR

ID: COT-5

Level: INFO

Description: Circle of Trust exists.

Data: Name of the circle of trust, Realm or organization name

Triggers: Creating the circle of trust.

Actions: Create Circle of Trust with a unique name.

INVALID_COT_TYPE

ID: COT-6

Level: INFO

Description: Circle of Trust Type is invalid

Data: Realm or organization name, Circle of Trust Type

Triggers: Creating the circle of trust.

Actions: The values for Circle of Trust type are IDFF , SAML2. Create Circle of Trust using either of these values.

CONFIG_ERROR_CREATE_COT_DESCRIPTOR

ID: COT-7

Level: INFO

Description: Configuration error while creating circle of trust.

Data: Error message, Entity ID, Realm or organization name

Triggers: Create circle of trust.

Actions: Check the fmCOT debug file for detailed errors.

COT_DESCRIPTOR_CREATED

ID: COT-8

Level: INFO

Description: Circle of trust created.

Data: Name of the circle of trust, Realm or organization name

Triggers: Creating the circle of trust.

NULL_COT_NAME_ADD_COT_DESCRIPTOR

ID: COT-9

Level: INFO

Description: Circle of Trust name is null, error adding to circle of trust.

Data: Realm or organization name

Triggers: Adding to the circle of trust.

Actions: Check the name of the circle of trust.

NULL_ENTITYID_ADD_COT_DESCRIPTOR

ID: COT-10

Level: INFO

Description: Entity Identifier is null , cannot add entity to circle of trust

Data: Realm or organization name

Triggers: Adding to the circle of trust.

Actions: Check the value of entity id.

CONFIG_ERROR_ADD_COT_MEMBER

ID: COT-11

Level: INFO

Description: Error adding entity to the circle of trust.

Data: Error message, Name of the circle of trust, Entity Id, Realm or organization name

Triggers: Adding entity to circle of trust.

Actions: Check COT debug for more detailed error message.

NO_COT_NAME_REMOVE_COT_MEMBER

ID: COT-12

Level: INFO

Description: Null circle of trust name.

Data: Realm or organization name

Triggers: Removing member from the circle of trust.

Actions: Check the name of the circle of trust.

NULL_ENTITYID_REMOVE_COT_MEMBER

ID: COT-13

Level: INFO

Description: Null entity identifier.

Data: Name of the circle of trust, Realm or organization name

Triggers: Removing member from the circle of trust.

Actions: Check the value of the entity identifier.

CONFIG_ERROR_REMOVE_COT_MEMBER

ID: COT-14

Level: INFO

Description: Error while removing entity from the circle of trust.

Data: Error message, Name of the circle of trust, Entity Id, Realm or organization name

Triggers: Removing entity identifier from the circle of trust.

Actions: Check COT debug for more detailed error message.

NULL_COT_NAME_LIST_COT

ID: COT-15

Level: INFO

Description: Null circle of trust name.

Data: Realm or organization name

Triggers: Listing entities in Circle of Trust

Actions: Check the name of the circle of trust.

CONFIG_ERROR_LIST_COT_MEMBER

ID: COT-16

Level: INFO

Description: Error listing providers in the circle of trust.

Data: Error message, Name of the circle of trust, Realm or organization name

Triggers: Listing providers in the circle of trust.

Actions: Check COT debug for more detailed error message.

CONFIG_ERROR_DELETE_COT_DESCRIPTOR

ID: COT-17

Level: INFO

Description: Error while deleting the circle of trust.

Data: Error message, Name of the circle of trust, Realm or organization name

Triggers: Deleting the circle of trust.

Actions: Check COT debug for more detailed error message.

INVALID_NAME_ERROR_DELETE_COT_DESCRIPTOR

ID: COT-18

Level: INFO

Description: Invalid name, cannot delete circle of trust.

Data: Circle of Trust Name, Realm or organization name

Triggers: Deleting the circle of trust.

Actions: Check the circle of trust name and retry deletion.

HAS_ENTITIES_DELETE_COT_DESCRIPTOR

ID: COT-19

Level: INFO

Description: Cannot delete circle of trust which has entities.

Data: Circle of Trust Name, Realm or organization name

Triggers: Deleting the circle of trust.

Actions: Remove all entities from the circle of trust and retry deletion.

INVALID_COT_TYPE_DELETE_COT_DESCRIPTOR

ID: COT-20

Level: INFO

Description: Invalid type cannot delete circle of trust.

Data: Realm or organization name, Circle of Trust Name, Circle of Trust Type

Triggers: Deleting the circle of trust.

Actions: Specify correct Circle of Trust type and retry delete.

COT_DESCRIPTOR_DELETED

ID: COT-21

Level: INFO

Description: Circle of trust deleted.

Data: Name of the circle of trust, Realm or organization name

Triggers: Deleting the circle of trust.

COT_FROM_CACHE

ID: COT-22

Level: FINE

Description: Retrieved the circle of trust from cache.

Data: Name of the circle of trust, Realm or organization name

Triggers: Retreived the circle of trust from cache.

CONFIG_ERROR_GET_COT_DESCRIPTOR

ID: COT-23

Level: INFO

Description: Error while getting the circle of trust from data store.

Data: Error message, Name of the circle of trust, Realm or organization name

Triggers: Retreiving the circle of trust

Actions: Check configuration; check debug for more detailed error message.

CONFIG_ERROR_RETREIVE_COT

ID: COT-24

Level: INFO

Description: Error determining an entity is in a circle of trust.

Data: Error message, Name of the circle of trust, ID of an entity, Realm or organization name

Triggers: Determining an entity is in a circle of trust.

Actions: Check debug for more detailed error message.

COT_DESCRIPTOR_RETRIEVED

ID: COT-25

Level: INFO

Description: Retrieved the circle of trust descriptor.

Data: Name of the circle of trust, Realm or organization name

Triggers: Retrieving the circle of trust under a realm.

OpenAM logs the following IDFF messages.

WRITE_ACCOUNT_FED_INFO

ID: IDFF-14

Level: INFO

Description: Write Account Federation Info

Data: user DN, federation info key, federation info value

Triggers: Acccount Federation Info with key was added to user

REMOVE_ACCOUNT_FED_INFO

ID: IDFF-15

Level: INFO

Description: Remove Account Federation Info

Data: user DN, provider id, existing federation info key

Triggers: Account federation info with key and provider ID was removed from user

CREATE_ASSERTION

ID: IDFF-16

Level: FINER

Description: Create Assertion

Data: assertion id or string

Triggers: Assertion Created

LOGOUT_REQUEST_PROCESSING_FAILED

ID: IDFF-18

Level: INFO

Description: Logout Request processing failed.

Data: message

Triggers: Logout Request processing failed

TERMINATION_REQUEST_PROCESSING_FAILED

ID: IDFF-19

Level: INFO

Description: Termination request processing failed

Data: message

Triggers: Termination request processing failed

FAILED_SOAP_URL_END_POINT_CREATION

ID: IDFF-20

Level: INFO

Description: Failed in creating SOAP URL End point.

Data: soap end point url

Triggers: Failed in creating SOAP URL End point

MISMATCH_AUTH_TYPE_AND_PROTOCOL

ID: IDFF-21

Level: INFO

Description: Mismatched AuthType and the protocol (based on SOAPUrl).

Data: protocol, authentication type

Triggers: AuthType and the protocol (based on SOAPUrl) do not match.

WRONG_AUTH_TYPE

ID: IDFF-22

Level: INFO

Description: Wrong Authentication type

Data: authentication type

Triggers: Wrong Authentication type

SOAP_RECEIVER_URL

ID: IDFF-23

Level: FINER

Description: SAML SOAP Receiver URL

Data: soap url

Triggers: SAML SOAP Receiver URL

INVALID_SOAP_RESPONSE

ID: IDFF-24

Level: INFO

Description: SOAP Response is Invalid

Data: message

Triggers: SOAP Response is Invalid.

INVALID_ASSERTION

ID: IDFF-25

Level: INFO

Description: Assertion is invalid

Data: message

Triggers: This Assertion is invalid

SINGLE_SIGNON_FAILED

ID: IDFF-26

Level: INFO

Description: Single SignOn Failed

Data: message

Triggers: Single SignOn Failed

ACCESS_GRANTED_REDIRECT_TO

ID: IDFF-27

Level: INFO

Description: Redirect to URL after granting access.

Data: redirect url

Triggers: Redirecting to URL after granting access.

MISSING_AUTHN_RESPONSE

ID: IDFF-28

Level: INFO

Description: Authentication Response is missing

Data: message

Triggers: Authentication Response not found

ACCOUNT_FEDERATION_FAILED

ID: IDFF-29

Level: INFO

Description: Account Federation Failed

Data: message

Triggers: Account Federation Failed

FAILED_SSO_TOKEN_GENERATION

ID: IDFF-30

Level: INFO

Description: SSOToken Generation Failed

Data: message

Triggers: Failed to generate SSOToken

INVALID_AUTHN_RESPONSE

ID: IDFF-31

Level: INFO

Description: Authentication Response is invalid

Data: invalid authentication response

Triggers: Authentication Response is invalid

AUTHN_REQUEST_PROCESSING_FAILED

ID: IDFF-32

Level: INFO

Description: Authentication Request processing failed

Data: message

Triggers: Authentication Request processing failed.

SIGNATURE_VERIFICATION_FAILED

ID: IDFF-33

Level: INFO

Description: Signature Verification Failed.

Data: message

Triggers: Signature Verification Failed.

CREATE_SAML_RESPONSE

ID: IDFF-34

Level: INFO

Description: Created SAML Response

Data: sending saml response to remote server's IP address, saml response or response ID and InResponseTo ID

Triggers: Created SAML Response

REDIRECT_TO

ID: IDFF-35

Level: FINER

Description: Redirect URL

Data: redirect url

Triggers: Redirect to :

COMMON_DOMAIN_META_DATA_NOT_FOUND

ID: IDFF-36

Level: INFO

Description: Common Domain Service Information not found

Data: message

Triggers: Common Domain Service Information not found.

PROVIDER_NOT_TRUSTED

ID: IDFF-37

Level: INFO

Description: Provider is not trusted

Data: provider id

Triggers: Provider is not trusted.

INVALID_AUTHN_REQUEST

ID: IDFF-38

Level: INFO

Description: Authentication Request is invalid

Data: message

Triggers: Authentication Request is invalid

USER_ACCOUNT_FEDERATION_INFO_NOT_FOUND

ID: IDFF-39

Level: INFO

Description: Account Federation Information not found for user

Data: user name

Triggers: Account Federation Information not found for user :

USER_NOT_FOUND

ID: IDFF-40

Level: INFO

Description: User not found.

Data: user name

Triggers: User not found.

LOGOUT_PROFILE_NOT_SUPPORTED

ID: IDFF-41

Level: INFO

Description: Logout profile not supported.

Data: logout profile

Triggers: Logout profile not supported.

Actions: Verify metadata is correct.

LOGOUT_SUCCESS

ID: IDFF-42

Level: INFO

Description: Logout is successful.

Data: user name

Triggers: Logout is successful.

LOGOUT_REDIRECT_FAILED

ID: IDFF-43

Level: INFO

Description: Logout failed to redirect due to incorrect URL.

Data: message

Triggers: Logout failed to redirect due to incorrect URL.

LOGOUT_FAILED_REQUEST_IMPROPER

ID: IDFF-44

Level: INFO

Description: Logout request not formed properly.

Data: user name

Triggers: Logout request not formed properly.

LOGOUT_FAILED_INVALID_HANDLER

ID: IDFF-45

Level: INFO

Description: Failed to get Pre/Logout handler.

Data: logout url

Triggers: Failed to get Pre/Logout handler.

LOGOUT_FAILED

ID: IDFF-46

Level: INFO

Description: Single logout failed.

Data: user name

Triggers: Single logout failed.

REGISTRATION_FAILED_SP_NAME_IDENTIFIER

ID: IDFF-47

Level: INFO

Description: Failed to create SPProvidedNameIdentifier.

Data: message

Triggers: Failed to create SPProvidedNameIdentifier.

INVALID_SIGNATURE

ID: IDFF-48

Level: INFO

Description: Invalid Signature.

Data: message

Triggers: Invalid Signature.

TERMINATION_FAILED

ID: IDFF-49

Level: INFO

Description: Federation Termination failed.

Data: user name

Triggers: Federation Termination failed. Cannot update account.

TERMINATION_SUCCESS

ID: IDFF-50

Level: INFO

Description: Federation Termination succeeded.

Data: userDN

Triggers: Federation Termination succeeded. User account updated.

INVALID_RESPONSE

ID: IDFF-51

Level: INFO

Description: Response is Invalid

Data: saml response

Triggers: SAML Response is Invalid.

INVALID_PROVIDER

ID: IDFF-52

Level: INFO

Description: Invalid Provider Registration.

Data: provider id, Realm or Organization Name

Triggers: Invalid Provider.

ERROR_GET_IDFF_META_INSTANCE

ID: IDFF-61

Level: INFO

Description: Error getting Configuration instance.

Data: message

Triggers: Trying to initialize IDFF Metadata configuration.

Actions: 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.

NULL_ENTITY_DESCRIPTOR

ID: IDFF-62

Level: INFO

Description: EntityDescriptor is null.

Data: message

Triggers: Trying to create EntityDescriptor.

Actions: Pass a valid non-null EntityDescriptorElement object to the IDFFMetaManager:createEntityDescriptor method.

NULL_ENTITY_ID

ID: IDFF-63

Level: INFO

Description: Entity Identifier in the EntityDescriptor is null.

Data: message

Triggers: Trying to create, modify, retrieve or delete EntityDescriptor or extended Entity Config.

Actions: The EntityDescriptor Element passed should have the Entity Identifier , this is the "providerID" attribute in the IDFF MetaData schema.

CREATE_ENTITY_SUCCEEDED

ID: IDFF-64

Level: INFO

Description: Creating of Entity Descriptor succeeded.

Data: Entity ID, Realm or Organization Name

Triggers: EntityDescriptor is stored in the data repository.

CREATE_ENTITY_FAILED

ID: IDFF-65

Level: INFO

Description: Storing of IDFF Meta Data in the repository failed.

Data: Entity ID, Realm or Organization Name

Triggers: Trying to create EntityDescriptor.

Actions: 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.

UNSUPPORTED_OPERATION

ID: IDFF-66

Level: INFO

Description: Unsupported operation.

Data: message

Triggers: Trying to create, modify or delete EntityDescriptor or extended EntityConfig.

Actions: Check the System Configuration Implementation to find out how IDFF Meta Data can be stored in the repository.

INVALID_ENTITY_DESCRIPTOR

ID: IDFF-67

Level: INFO

Description: The EntityDescriptor object is not valid.

Data: Entity ID, Realm or Organization Name

Triggers: Trying to retrieve or modify EntityDescriptor.

Actions: Check the EntityDescriptor Element is valid and follows the IDFF Standard Meta Data Schema Description.

GET_ENTITY_FAILED

ID: IDFF-68

Level: INFO

Description: Retrieval of Entity Configuration failed.

Data: Entity ID, Realm or Organization Name

Triggers: EntityDescriptor is retrieved.

Actions: Check if the entity identifier is correct.

GET_ENTITY_SUCCEEDED

ID: IDFF-69

Level: INFO

Description: Retrieval of Entity Descriptor succeeded.

Data: Entity ID, Realm or Organization Name

Triggers: Entity Configuration is returned to the requester.

SET_ENTITY_FAILED

ID: IDFF-70

Level: INFO

Description: Storing of Entity Configuration failed.

Data: Entity ID, Realm or Organization Name

Triggers: Trying to modify IDFF Standard Meta data.

Actions: Check if the entity identifier is correct.; Check if the data repository exists and is accessible.

SET_ENTITY_SUCCEEDED

ID: IDFF-71

Level: INFO

Description: Modifying Entity Descriptor succeeded.

Data: Entity ID, Realm or Organization Name

Triggers: Entity Descriptor is modified in the data repository.

DELETE_ENTITY_SUCCEEDED

ID: IDFF-72

Level: INFO

Description: Deleting of IDFF Standard Meta Data succeeded.

Data: Entity ID, Realm or Organization Name

Triggers: IDFF Standard Meta data for the entity is deleted in the data repository.

DELETE_ENTITY_FAILED

ID: IDFF-73

Level: INFO

Description: Deleting of Standard Metadata for entity identifier failed.

Data: Entity ID, Realm or Organization Name

Triggers: Trying to delete IDFF Standard Meta data for the entity.

Actions: Check if the entity identifier is correct.; Check if the data repository exists and is accessible

NULL_ENTITY_CONFIG

ID: IDFF-74

Level: INFO

Description: Extended Entity Configuration is null.

Data: message

Triggers: Trying to create IDFF extended Meta data.

Actions: Check the validity of the extended entity configuration.

ENTITY_CONFIG_NOT_FOUND

ID: IDFF-75

Level: INFO

Description: Entity Configuration could not be found.

Data: Entity ID, Realm or Organization Name

Triggers: Trying to create IDFF extended Meta data.

Actions: Check the validity of the entity configuration.

ENTITY_CONFIG_EXISTS

ID: IDFF-76

Level: INFO

Description: Creation of Extended Entity Configuration failed since it already exists.

Data: Entity ID, Realm or Organization Name

Triggers: Trying to create IDFF extended Meta data.

Actions: 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.

GET_ENTITY_CONFIG_FAILED

ID: IDFF-77

Level: INFO

Description: Failed to get entity configuration.

Data: Entity ID, Realm or Organization Name

Triggers: Trying to retrieve IDFF extended Meta data.

Actions: Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors.

GET_ENTITY_CONFIG_SUCCEEDED

ID: IDFF-78

Level: INFO

Description: Retrieval of Entity Configuration succeeded.

Data: Entity ID, Realm or Organization Name

Triggers: Entity Configuration is retrieved from the data repository

SET_ENTITY_CONFIG_SUCCEEDED

ID: IDFF-79

Level: INFO

Description: Extended Entity Configuration was modified.

Data: Entity ID, Realm or Organization Name

Triggers: Extended Entity Configuration is modified in the data repository

SET_ENTITY_CONFIG_FAILED

ID: IDFF-80

Level: INFO

Description: Failed to modify Extended Entity Configuration.

Data: Entity ID, Realm or Organization Name

Triggers: Extended Entity Configuration is modified in the data repository

Actions: Check the IDFF Meta Data Debug "libIDFFMeta" for specific errors.

CREATE_ENTITY_CONFIG_SUCCEEDED

ID: IDFF-81

Level: INFO

Description: Extended Entity Configuration was created.

Data: Entity ID, Realm or Organization Name

Triggers: Extended Entity Configuration is stored in the data repository

CREATE_ENTITY_CONFIG_FAILED

ID: IDFF-82

Level: INFO

Description: Storing of IDFF Extended Configuration in the repository failed.

Data: Entity ID, Realm or Organization Name

Triggers: Trying to create Extended Entity Configuration.

Actions: 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.

INVALID_ENTITY_CONFIG

ID: IDFF-83

Level: INFO

Description: The Extended Entity Configuration is invalid.

Data: Entity ID, Realm or Organization Name

Triggers: Trying to create, modify or retrieve Extended Entity Configuration.

Actions: Check the Extended Entity Configuration is valid and retry creating the entity config.

GET_ALL_ENTITIES_SUCCEEDED

ID: IDFF-84

Level: INFO

Description: Retrieve all Entity Descriptors succeeded.

Data: message

Triggers: Retrieve all Entity Descriptors

GET_ALL_ENTITIES_FAILED

ID: IDFF-85

Level: INFO

Description: Failed to get all Entity Descriptors.

Data: message

Triggers: Retrieve all Entity Descriptors

Actions: 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.

GET_ENTITY_NAMES_SUCCEEDED

ID: IDFF-86

Level: INFO

Description: Retrieve names of all Entities.

Data: message

Triggers: Retrieve names of all Entities.

GET_ENTITY_NAMES_FAILED

ID: IDFF-87

Level: INFO

Description: Failed to get names for all Entities.

Data: message

Triggers: Retrieving names of all Entities.

Actions: 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.

GET_HOSTED_ENTITIES_SUCCEEDED

ID: IDFF-88

Level: INFO

Description: Retrieve all hosted Entities succeeded.

Data: message

Triggers: Retrieving all hosted Entities.

GET_HOSTED_ENTITIES_FAILED

ID: IDFF-89

Level: INFO

Description: Failed to get all hosted Entities.

Data: message

Triggers: Retrieving all hosted Entities.

Actions: 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.

GET_REMOTE_ENTITIES_SUCCEEDED

ID: IDFF-90

Level: INFO

Description: Retrieval of all remote Entities succeeded.

Data: message

Triggers: Retrieve all remote Entities.

GET_REMOTE_ENTITIES_FAILED

ID: IDFF-91

Level: INFO

Description: Failed to get all remote Entities.

Data: message

Triggers: Retrieving all remote Entities.

Actions: 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.

GET_HOSTED_SERVICE_PROVIDERS_SUCCEEDED

ID: IDFF-92

Level: INFO

Description: Retrieval of all hosted services providers succeeded.

Data: message

Triggers: Retrieving all hosted services providers.

GET_REMOTE_SERVICE_PROVIDERS_SUCCEEDED

ID: IDFF-93

Level: INFO

Description: Retrieval of all remote services providers succeeded.

Data: message

Triggers: Retrieve all remote services providers.

GET_HOSTED_IDENTITY_PROVIDERS_SUCCEEDED

ID: IDFF-94

Level: INFO

Description: Retrieval of all hosted identity providers succeeded.

Data: message

Triggers: Retrieve all hosted identity providers.

GET_REMOTE_IDENTITY_PROVIDERS_SUCCEEDED

ID: IDFF-95

Level: INFO

Description: Retrieval of all remote identity providers succeeded.

Data: message

Triggers: Retrieve all remote identity providers.

IS_AFFILIATE_MEMBER_SUCCEEDED

ID: IDFF-96

Level: INFO

Description: Checking Affiliation member succeeded.

Data: Entity ID, Affiliation ID, Realm or Organization Name

Triggers: Checks if the provider is a member of the Affiliation.

NO_ENTITY_CONFIG_TO_DELETE

ID: IDFF-97

Level: INFO

Description: No entity configuration to delete.

Data: Entity ID, Realm or Organization Name

Triggers: Delete Entity Configuration.

Actions: Check the entityID to make sure the Entity Configuration does exist.

DELETE_ENTITY_CONFIG_FAILED

ID: IDFF-98

Level: INFO

Description: Failed to delete entity configuration.

Data: Entity ID, Realm or Organization Name

Triggers: Delete Entity Configuration.

Actions: 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.

DELETE_ENTITY_CONFIG_SUCCEEDED

ID: IDFF-99

Level: INFO

Description: Entity configuration deleted successfully.

Data: Entity ID, Realm or Organization Name

Triggers: Delete Entity Configuration.

ENTITY_DOES_NOT_EXISTS

ID: IDFF-100

Level: INFO

Description: Entity does not exist.

Data: Entity ID, Realm or Organization Name

Triggers: Delete Entity Descriptor.

Actions: 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.

CREATE_AUTHN_RESPONSE

ID: IDFF-101

Level: INFO

Description: Created Authn Response

Data: saml response or response ID and InResponseTo ID

Triggers: Created SAML Response

SENT_AUTHN_RESPONSE

ID: IDFF-102

Level: INFO

Description: Sent Authn Response

Data: Service provider's assertion consumer service URL, response ID and InResponseTo ID

Triggers: Sent Authn Response

OpenAM logs the following LIBERTY messages.

AS_Abort

ID: LIBERTY-1

Level: INFO

Description: Unable to process SASL Request

Data: message id, authentication mechanism, authorization id, advisory authentication id

Triggers: Unable to process SASL Request.

AS_OK

ID: LIBERTY-2

Level: INFO

Description: SASL Response Ok

Data: message id, authentication mechanism, authorization id, advisory authentication id

Triggers: SASL Response Ok.

AS_Continue

ID: LIBERTY-3

Level: INFO

Description: Return SASL Authenticaton Response

Data: message id, authentication mechanism, authorization id, advisory authentication id

Triggers: Returned SASL Response , continue Authentication.

DS_Lookup_Failure

ID: LIBERTY-4

Level: INFO

Description: User not found in Data store

Data: user name

Triggers: User not found in Data store

DS_Lookup_Success

ID: LIBERTY-5

Level: INFO

Description: User found in Data Store

Data: user name

Triggers: User found in Data Store

DS_Update_Failure

ID: LIBERTY-6

Level: INFO

Description: Cannot locate user from resourceID

Data: resourceID

Triggers: Cannot locate user from resourceID

DS_Update_Success

ID: LIBERTY-7

Level: INFO

Description: Successfully updated user profile

Data: user name

Triggers: Successfully updated user profile

PP_Query_Failure

ID: LIBERTY-8

Level: INFO

Description: UnAuthorized. Failed to Query Personal Profile Service

Data: resource id

Triggers: Failed to Query Personal Profile Service

PP_Interaction_Failure

ID: LIBERTY-9

Level: INFO

Description: Interaction Failed

Data: resource id

Triggers: Interaction with Personal Profile Service Failed

PP_Query_Success

ID: LIBERTY-10

Level: INFO

Description: Successfully queried PP Service

Data: resource id

Triggers: Personal Profile Service Query Succeeded

PP_Modify_Failure

ID: LIBERTY-11

Level: INFO

Description: Modify Failure

Data: resource id

Triggers: Failed to modify Personal Profile Service

PP_Modify_Success

ID: LIBERTY-12

Level: INFO

Description: Modify Success

Data: resource id

Triggers: Personal Profile Service Successfully modified.

PP_Interaction_Success

ID: LIBERTY-13

Level: INFO

Description: Interaction Successful

Data: successful interaction message

Triggers: Successful interaction with Personal Profile Service

IS_Sending_Message

ID: LIBERTY-14

Level: INFO

Description: Sending Message

Data: request message id

Triggers: Sending SOAP Request Message to WSP.

IS_Returning_Response_Message

ID: LIBERTY-15

Level: INFO

Description: Returning Response Message

Data: response message id, request message id

Triggers: Returning Response Message for SOAP Request.

IS_Resending_Message

ID: LIBERTY-16

Level: INFO

Description: Resending Message

Data: message id

Triggers: Resending SOAP Request Message to WSP

IS_Redirected_User_Agent

ID: LIBERTY-17

Level: INFO

Description: Interaction manager redirecting user agent to interaction service

Data: request message id

Triggers: Interaction manager redirecting user agent to interaction service

IS_Returning_Response_Element

ID: LIBERTY-18

Level: INFO

Description: Interaction manager returning response element

Data: message id, reference message id, cache entry status

Triggers: Interaction manager returning response element

IS_Presented_Query_To_User_Agent

ID: LIBERTY-19

Level: INFO

Description: Interaction query presented to user agent

Data: message id

Triggers: Interaction query presented to user agent

IS_Collected_Response_From_User_Agent

ID: LIBERTY-20

Level: INFO

Description: User agent responded to interaction query

Data: message id

Triggers: User agent responded to interaction query

IS_Redirected_User_Agent_Back

ID: LIBERTY-21

Level: INFO

Description: User agent redirected back to SP

Data: message id

Triggers: User agent redirected back to SP

WS_Success

ID: LIBERTY-22

Level: INFO

Description: Webservices Success

Data: message id, handler key

Triggers: Webservices success.

WS_Failure

ID: LIBERTY-23

Level: INFO

Description: Webservices Failure

Data: error message

Triggers: Webservices Failure.

OpenAM logs the following SAML2 messages.

INVALID_SP

ID: SAML2-1

Level: INFO

Description: Invalid Service Provider Identifier

Data: Service Provider Entity Identifier

Triggers: Invalid Service Provider,cannot process request

Actions: Check the Service Provider Name.

INVALID_IDP

ID: SAML2-2

Level: INFO

Description: Invalid Identity Provider Identifier

Data: Identity Provider Entity Identifier

Triggers: Invalid Identity Provider,cannot process request

Actions: Check the Identity Provider Name.

SP_METADATA_ERROR

ID: SAML2-3

Level: INFO

Description: Unable to retreive Service Provider Metadata.

Data: Service Provider Entity Identifier

Triggers: Cannot retrieve Service Provider Metadata

Actions: Check the Data Store is accessible .; Check the Realm name.; Check the Service Provider Entity Identifier.

IDP_METADATA_ERROR

ID: SAML2-4

Level: INFO

Description: Unable to retrieve Identity Provider Metadata.

Data: Identity Provider Entity Identifier

Triggers: Cannot retreive Identity Provider Metadata

Actions: Check the Data Store is accessible .; Check the Realm name.; Check the Identity Provider Entity Identifier.

SSO_NOT_FOUND

ID: SAML2-5

Level: INFO

Description: Unable to retrieve SingleSignOnService URL.

Data: Identity Provider Entity Identifier

Triggers: Error retreiving SingleSignOnService URL.

Actions: Check the Data Store is accessible .; Check the Realm name.; Check the Identity Provider Entity Identifier.

REDIRECT_TO_SP

ID: SAML2-6

Level: INFO

Description: Redirecting to SingleSignOnService

Data: SingleSignOnService URL

Triggers: Sending Authentication Request by redirecting to Single SignOn Service URL.

RESPONSE_NOT_FOUND_FROM_CACHE

ID: SAML2-7

Level: INFO

Description: Unable to retrieve Response using Response ID after local login.

Data: Response ID

Triggers: Response doesn't exist in the SP cache.

Actions: Check the SP cache clean up interval configuration.

MISSING_ARTIFACT

ID: SAML2-8

Level: INFO

Description: Unable to retrieve Artifact from HTTP Request.

Triggers: SAMLart is missing from HTTP Request

Actions: Check with sender.; Check web container server log.

RECEIVED_ARTIFACT

ID: SAML2-9

Level: INFO

Description: Received Artifact from HTTP Request.

Data: Artifact value

Triggers: Received Artifact from HTTP Request in the process of Single Sign On using Artifact Profile.

IDP_NOT_FOUND

ID: SAML2-10

Level: INFO

Description: Unable to find Identity Provider Entity ID based on the SourceID in Artifact.

Data: Artifact value, Realm or organization name

Triggers: No matching Identity Provider Entity ID found in meta data configuration.

Actions: Check if Identity Provider's meta data is loaded.

IDP_META_NOT_FOUND

ID: SAML2-11

Level: INFO

Description: Unable to load Identity Provider's meta data.

Data: Realm or organization name, Identity Provider Entity ID

Triggers: Unable to load Identity Provider's meta data.

Actions: Check Identity Provider Entity ID.; Check Realm or organization name.; Check if the identity provider's meta is loaded.

ARTIFACT_RESOLUTION_URL_NOT_FOUND

ID: SAML2-12

Level: INFO

Description: Unable to find Identity Provider's Artifact resolution service URL.

Data: Identity Provider Entity ID

Triggers: Artifact resolution service URL is not defined in Identity Provider's metadata.

Actions: Check Identity Provider's meta data.

CANNOT_CREATE_ARTIFACT_RESOLVE

ID: SAML2-13

Level: INFO

Description: Unable to create ArtifactResolve.

Data: Hosted Service Provider Entity ID, Artifact value

Triggers: Error when creating ArtifactResolve instance.

Actions: Check implementation of ArtifactResolve.

CANNOT_GET_SOAP_RESPONSE

ID: SAML2-14

Level: INFO

Description: Unable to obtain response from SOAP communication with Identity Provider's artifact resolution service.

Data: Hosted Service Provider Entity ID, Identity Provider's Artifact Resolution Service URL

Triggers: Error in SOAP communication.

Actions: Check Identity Provider's Artifact Resolution Service URL.; Check SOAP message authentication requirements for Identity Provider's Artifact Resolution Service.

GOT_RESPONSE_FROM_ARTIFACT

ID: SAML2-15

Level: INFO

Description: Obtained response using artifact profile.

Data: 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

Triggers: Single Sign On using Artifact Profile.

SOAP_ERROR

ID: SAML2-16

Level: INFO

Description: Unable to obtain Artifact Response due to SOAP error.

Data: Identity Provider Entity ID

Triggers: Error in SOAP communication.

Actions: Check configuration for Identity Provider

SOAP_FAULT

ID: SAML2-17

Level: INFO

Description: Received SOAP Fault instead of Artifact Response.

Data: Identity Provider Entity ID

Triggers: Error in Identity Provider's Artifact Resolution.

Actions: Check Identity Provider; Check debug file for detailed fault info.

TOO_MANY_ARTIFACT_RESPONSE

ID: SAML2-18

Level: INFO

Description: Received too many Artifact Response.

Data: Identity Provider Entity ID

Triggers: Identity Provider sent more than one Artifact Response in SOAPMessage.

Actions: Check Identity Provider

CANNOT_INSTANTIATE_ARTIFACT_RESPONSE

ID: SAML2-19

Level: INFO

Description: Unable to instantiate Artifact Response.

Data: Identity Provider Entity ID

Triggers: Error while instantiating Artifact Response.

Actions: Check Identity Provider; Check debug message for detailed error.

MISSING_ARTIFACT_RESPONSE

ID: SAML2-20

Level: INFO

Description: Unable to obtain Artifact Response from SOAP message.

Data: Identity Provider Entity ID

Triggers: No ArtifactResponse is included in SOAPMessage.

Actions: Check Identity Provider

ARTIFACT_RESPONSE_INVALID_SIGNATURE

ID: SAML2-21

Level: INFO

Description: Unable to verify signature on Artifact Response.

Data: Identity Provider Entity ID

Triggers: Error while trying to verify signature on ArtifactResponse.

Actions: Check configuration for Identity Provider; Check debug file for detailed info

ARTIFACT_RESPONSE_INVALID_INRESPONSETO

ID: SAML2-22

Level: INFO

Description: Invalid InResponseTo attribute in Artifact Response.

Data: Identity Provider Entity ID

Triggers: InResponseTo attribute in Artifact Response is missing or doesn't match with Artifact Resolve ID.

Actions: Check with Identity Provider

ARTIFACT_RESPONSE_INVALID_ISSUER

ID: SAML2-23

Level: INFO

Description: Invalid Issuer in Artifact Response.

Data: Identity Provider Entity ID

Triggers: Issuer in Artifact Response is missing or doesn't match with Identity Provider Entity ID.

Actions: Check with Identity Provider

ARTIFACT_RESPONSE_INVALID_STATUS_CODE

ID: SAML2-24

Level: INFO

Description: Invalid status code in Artifact Response.

Data: Identity Provider Entity ID, Status code if the log level was set to LL_FINE at runtime

Triggers: Status in Artifact Response is missing or status code is not Success.

Actions: Check with Identity Provider

CANNOT_INSTANTIATE_RESPONSE_ARTIFACT

ID: SAML2-25

Level: INFO

Description: Unable to instantiate Respones from Artifact Response.

Data: Identity Provider Entity ID

Triggers: Error occurred while instantiating Response.

Actions: Check debug file for detailed error.

MISSING_SAML_RESPONSE_FROM_POST

ID: SAML2-26

Level: INFO

Description: SAML Response is missing from http post.

Triggers: Parameter SAMLResponse is missing from http POST.

CANNOT_INSTANTIATE_RESPONSE_POST

ID: SAML2-27

Level: INFO

Description: Unable to instantiate Response from POST.

Triggers: Error occurred while instantiating Response.

Actions: Check debug file for more info

CANNOT_DECODE_RESPONSE

ID: SAML2-28

Level: INFO

Description: Unable to decode Response.

Triggers: Error occurred while decoding Response.

Actions: Check debug file for more info

GOT_RESPONSE_FROM_POST

ID: SAML2-29

Level: INFO

Description: Obtained response using POST profile.

Data: Response xml String if the log level was set to LL_FINE at runtime

Triggers: Single Sign On using POST Profile.

FED_INFO_WRITTEN

ID: SAML2-30

Level: INFO

Description: Written federation info.

Data: Username, NameIDInfo value string if the log level was set to LL_FINE at runtime

Triggers: Federation is done.

REDIRECT_TO_IDP

ID: SAML2-31

Level: INFO

Description: Redirect request to IDP.

Data: redirection url

Triggers: Single logout.

NO_ACS_URL

ID: SAML2-32

Level: INFO

Description: Unable to find Assertion Consumer Service URL.

Data: meta alias

Triggers: Single Sign On.

NO_RETURN_BINDING

ID: SAML2-33

Level: INFO

Description: Unable to find return binding.

Data: meta alias

Triggers: Single Sign On.

POST_TO_TARGET_FAILED

ID: SAML2-34

Level: INFO

Description: Unable to post the response to target.

Data: Assertion Consumer Service URL

Triggers: Single Sign On with POST binding.

CANNOT_CREATE_ARTIFACT

ID: SAML2-35

Level: INFO

Description: Unable to create an artifact.

Data: IDP entity ID

Triggers: Single Sign On with Artifact binding.

RECEIVED_AUTHN_REQUEST

ID: SAML2-36

Level: INFO

Description: Received AuthnRequest.

Data: SP entity ID, IDP meta alias, authnRequest xml string

Triggers: Single Sign On.

POST_RESPONSE

ID: SAML2-37

Level: INFO

Description: Post response to SP.

Data: SP entity ID, IDP meta alias, response xml string

Triggers: Single Sign On with POST binding.

SEND_ARTIFACT

ID: SAML2-38

Level: INFO

Description: Send an artifact to SP.

Data: IDP entity ID, IDP realm, redirect URL

Triggers: Single Sign On with Artifact binding.

INVALID_SOAP_MESSAGE

ID: SAML2-39

Level: INFO

Description: Encounter invalid SOAP message in IDP.

Data: IDP entity ID

Triggers: Single Sign On with Artifact binding.

ARTIFACT_RESPONSE

ID: SAML2-40

Level: INFO

Description: The artifact response being sent to SP.

Data: IDP entity ID, artifact string, artifact response

Triggers: Single Sign On with Artifact binding.

GOT_ENTITY_DESCRIPTOR

ID: SAML2-41

Level: FINE

Description: Entity descriptor obtained.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity descriptor.

INVALID_REALM_GET_ENTITY_DESCRIPTOR

ID: SAML2-42

Level: INFO

Description: Invaid realm while getting entity descriptor.

Data: Realm or organization name

Triggers: Obtain entity descriptor.

Actions: Check the Realm name.

GOT_INVALID_ENTITY_DESCRIPTOR

ID: SAML2-43

Level: INFO

Description: Obtained invalid entity descriptor.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity descriptor.

Actions: Delete invalid entity descriptor and import it again.

CONFIG_ERROR_GET_ENTITY_DESCRIPTOR

ID: SAML2-44

Level: INFO

Description: Configuration error while getting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Obtain entity descriptor.

Actions: Check debug message for detailed error.

NO_ENTITY_ID_SET_ENTITY_DESCRIPTOR

ID: SAML2-45

Level: INFO

Description: No entity ID while setting entity descriptor.

Data: Realm or organization name

Triggers: Set entity descriptor.

Actions: Set entity ID in entity descriptor.

INVALID_REALM_SET_ENTITY_DESCRIPTOR

ID: SAML2-46

Level: INFO

Description: Invaid realm while setting entity descriptor.

Data: Realm or organization name

Triggers: Set entity descriptor.

Actions: Check the Realm name.

NO_ENTITY_DESCRIPTOR_SET_ENTITY_DESCRIPTOR

ID: SAML2-47

Level: INFO

Description: Entity descriptor doesn't exist while setting entity descriptor.

Data: Entity ID, Realm or organization name

Triggers: Set entity descriptor.

Actions: Create entity descriptor before set.

SET_ENTITY_DESCRIPTOR

ID: SAML2-48

Level: INFO

Description: Entity descriptor was set.

Data: Entity ID, Realm or organization name

Triggers: Set entity descriptor.

CONFIG_ERROR_SET_ENTITY_DESCRIPTOR

ID: SAML2-49

Level: INFO

Description: Configuration error while setting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Set entity descriptor.

Actions: Check debug message for detailed error.

SET_INVALID_ENTITY_DESCRIPTOR

ID: SAML2-50

Level: INFO

Description: Invalid entity descriptor to set.

Data: Entity ID, Realm or organization name

Triggers: Set entity descriptor.

Actions: Check entity descriptor if it follows the schema.

NO_ENTITY_ID_CREATE_ENTITY_DESCRIPTOR

ID: SAML2-51

Level: INFO

Description: No entity ID while creating entity descriptor.

Data: Realm or organization name

Triggers: Create entity descriptor.

Actions: Set entity ID in entity descriptor.

INVALID_REALM_CREATE_ENTITY_DESCRIPTOR

ID: SAML2-52

Level: INFO

Description: Invaid realm while creating entity descriptor.

Data: Realm or organization name

Triggers: Create entity descriptor.

Actions: Check the Realm name.

ENTITY_DESCRIPTOR_EXISTS

ID: SAML2-53

Level: INFO

Description: Entity descriptor exists while creating entity descriptor.

Data: Entity ID, Realm or organization name

Triggers: Create entity descriptor.

Actions: Delete existing entity descriptor first.

ENTITY_DESCRIPTOR_CREATED

ID: SAML2-54

Level: INFO

Description: Entity descriptor was created.

Data: Entity ID, Realm or organization name

Triggers: Create entity descriptor.

CONFIG_ERROR_CREATE_ENTITY_DESCRIPTOR

ID: SAML2-55

Level: INFO

Description: Configuration error while creating entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Create entity descriptor.

Actions: Check debug message for detailed error.

CREATE_INVALID_ENTITY_DESCRIPTOR

ID: SAML2-56

Level: INFO

Description: Invalid entity descriptor to create.

Data: Entity ID, Realm or organization name

Triggers: Create entity descriptor.

Actions: Check entity descriptor if it follows the schema.

INVALID_REALM_DELETE_ENTITY_DESCRIPTOR

ID: SAML2-57

Level: INFO

Description: Invaid realm while deleting entity descriptor.

Data: Realm or organization name

Triggers: Delete entity descriptor.

Actions: Check the Realm name.

NO_ENTITY_DESCRIPTOR_DELETE_ENTITY_DESCRIPTOR

ID: SAML2-58

Level: INFO

Description: Entity descriptor doesn't exist while deleting entity descriptor.

Data: Entity ID, Realm or organization name

Triggers: Delete entity descriptor.

ENTITY_DESCRIPTOR_DELETED

ID: SAML2-59

Level: INFO

Description: Entity descriptor was deleted.

Data: Entity ID, Realm or organization name

Triggers: Delete entity descriptor.

CONFIG_ERROR_DELETE_ENTITY_DESCRIPTOR

ID: SAML2-60

Level: INFO

Description: Configuration error while deleting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Delete entity descriptor.

Actions: Check debug message for detailed error.

GOT_ENTITY_CONFIG

ID: SAML2-61

Level: FINE

Description: Entity config obtained.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity config.

INVALID_REALM_GET_ENTITY_CONFIG

ID: SAML2-62

Level: INFO

Description: Invaid realm while getting entity config.

Data: Realm or organization name

Triggers: Obtain entity config.

Actions: Check the Realm name.

GOT_INVALID_ENTITY_CONFIG

ID: SAML2-63

Level: INFO

Description: Obtained invalid entity config.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity config.

Actions: Delete invalid entity config and import it again.

CONFIG_ERROR_GET_ENTITY_CONFIG

ID: SAML2-64

Level: INFO

Description: Configuration error while getting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Obtain entity config.

Actions: Check debug message for detailed error.

NO_ENTITY_ID_SET_ENTITY_CONFIG

ID: SAML2-65

Level: INFO

Description: No entity ID while setting entity config.

Data: Realm or organization name

Triggers: Set entity config.

Actions: Set entity ID in entity config.

INVALID_REALM_SET_ENTITY_CONFIG

ID: SAML2-66

Level: INFO

Description: Invaid realm while setting entity config.

Data: Realm or organization name

Triggers: Set entity config.

Actions: Check the Realm name.

NO_ENTITY_DESCRIPTOR_SET_ENTITY_CONFIG

ID: SAML2-67

Level: INFO

Description: Entity config doesn't exist while setting entity config.

Data: Entity ID, Realm or organization name

Triggers: Set entity config.

Actions: Create entity descriptor before set entity config.

SET_ENTITY_CONFIG

ID: SAML2-68

Level: INFO

Description: Entity config was set.

Data: Entity ID, Realm or organization name

Triggers: Set entity config.

CONFIG_ERROR_SET_ENTITY_CONFIG

ID: SAML2-69

Level: INFO

Description: Configuration error while setting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Set entity config.

Actions: Check debug message for detailed error.

SET_INVALID_ENTITY_CONFIG

ID: SAML2-70

Level: INFO

Description: Invalid entity config to set.

Data: Entity ID, Realm or organization name

Triggers: Set entity config.

Actions: Check entity config if it follows the schema.

NO_ENTITY_ID_CREATE_ENTITY_CONFIG

ID: SAML2-71

Level: INFO

Description: No entity ID while creating entity config.

Data: Realm or organization name

Triggers: Create entity config.

Actions: Set entity ID in entity config.

INVALID_REALM_CREATE_ENTITY_CONFIG

ID: SAML2-72

Level: INFO

Description: Invaid realm while creating entity config.

Data: Realm or organization name

Triggers: Create entity config.

Actions: Check the Realm name.

NO_ENTITY_DESCRIPTOR_CREATE_ENTITY_CONFIG

ID: SAML2-73

Level: INFO

Description: Entity config doesn't exist while creating entity config.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Create entity descriptor before create entity config.

ENTITY_CONFIG_EXISTS

ID: SAML2-74

Level: INFO

Description: Entity config exists while creating entity config.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Delete existing entity config first.

ENTITY_CONFIG_CREATED

ID: SAML2-75

Level: INFO

Description: Entity config was created.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

CONFIG_ERROR_CREATE_ENTITY_CONFIG

ID: SAML2-76

Level: INFO

Description: Configuration error while creating entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Check debug message for detailed error.

CREATE_INVALID_ENTITY_CONFIG

ID: SAML2-77

Level: INFO

Description: Invalid entity config to create.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Check entity config if it follows the schema.

INVALID_REALM_DELETE_ENTITY_CONFIG

ID: SAML2-78

Level: INFO

Description: Invaid realm while deleting entity config.

Data: Realm or organization name

Triggers: Delete entity config.

Actions: Check the Realm name.

NO_ENTITY_CONFIG_DELETE_ENTITY_CONFIG

ID: SAML2-79

Level: INFO

Description: Entity config doesn't exist while deleting entity config.

Data: Entity ID, Realm or organization name

Triggers: Delete entity config.

Actions: Check debug message for detailed error.

ENTITY_CONFIG_DELETED

ID: SAML2-80

Level: INFO

Description: Entity config was deleted.

Data: Entity ID, Realm or organization name

Triggers: Delete entity config.

CONFIG_ERROR_DELETE_ENTITY_CONFIG

ID: SAML2-81

Level: INFO

Description: Configuration error while deleting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Delete entity config.

Actions: Check debug message for detailed error.

INVALID_REALM_GET_ALL_HOSTED_ENTITIES

ID: SAML2-82

Level: INFO

Description: Invaid realm while getting all hosted entities.

Data: Realm or organization name

Triggers: Get all hosted entities.

Actions: Check the Realm name.

CONFIG_ERROR_GET_ALL_HOSTED_ENTITIES

ID: SAML2-83

Level: INFO

Description: Configuration error while getting all hosted entities.

Data: Error message, Realm or organization name

Triggers: Get all hosted entities.

Actions: Check debug message for detailed error.

GOT_ALL_HOSTED_ENTITIES

ID: SAML2-84

Level: FINE

Description: Obtained all hosted entities.

Data: Error message, Realm or organization name

Triggers: Get all hosted entities.

INVALID_REALM_GET_ALL_REMOTE_ENTITIES

ID: SAML2-85

Level: INFO

Description: Invaid realm while getting all remote entities.

Data: Realm or organization name

Triggers: Get all remote entities.

Actions: Check the Realm name.

CONFIG_ERROR_GET_ALL_REMOTE_ENTITIES

ID: SAML2-86

Level: INFO

Description: Configuration error while getting all remote entities.

Data: Error message, Realm or organization name

Triggers: Get all remote entities.

Actions: Check debug message for detailed error.

GOT_ALL_REMOTE_ENTITIES

ID: SAML2-87

Level: FINE

Description: Obtained all remote entities.

Data: Error message, Realm or organization name

Triggers: Get all remote entities.

INVALID_INRESPONSETO_RESPONSE

ID: SAML2-88

Level: INFO

Description: InResponseTo attribute in Response is invalid.

Data: Response ID

Triggers: Service Provider received a Response for Single Sign On.

Actions: Check debug message for detailed error.

INVALID_ISSUER_RESPONSE

ID: SAML2-89

Level: INFO

Description: Issuer in Response is invalid.

Data: Hosted Entity ID, Name of Realm or organization, Response ID

Triggers: Issuer in Response is not configured or not trusted by the hosted provider

Actions: Check configuration.

WRONG_STATUS_CODE

ID: SAML2-90

Level: INFO

Description: Status code in Response was not Success.

Data: Response ID, Status code (if log level is set to LL_FINE)

Triggers: Service provider received a Response with wrong Status code. Most likely an error occurred at Identity Provider.

Actions: Check the status code. Contact Identity Provider if needed.

ASSERTION_NOT_ENCRYPTED

ID: SAML2-91

Level: INFO

Description: Assertion in Response was not encrypted.

Data: Response ID

Triggers: Service provider requested the assertion in Response to be encrypted, but it received a Response with unencrypted assertion(s).

Actions: Check configuration. Notify Identity Provider regarding the requirement.

MISSING_ASSERTION

ID: SAML2-92

Level: INFO

Description: Response had no Assertion.

Data: Response ID

Triggers: Service provider received a Response for Single Sign On, but the response contained no Assertion.

Actions: Check error code of the Response. Notify Identity Provider if needed.

INVALID_ISSUER_ASSERTION

ID: SAML2-93

Level: INFO

Description: Issuer in Assertion is not valid.

Data: Assertion ID

Triggers: Issuer in Assertion for single sign on was not configured at service provider, or not trusted by the service provider.

Actions: Check configuration

MISMATCH_ISSUER_ASSERTION

ID: SAML2-94

Level: INFO

Description: Issuer in Assertion didn't match the Issuer in Response or other Assertions in the Response.

Data: Assertion ID

Triggers: Service provider received Response which had mismatch Issuer inside the Assertion it contained.

Actions: Check debug message

INVALID_SIGNATURE_ASSERTION

ID: SAML2-95

Level: INFO

Description: Assertion is not signed or signature is not valid.

Data: Assertion ID

Triggers: Service provider requested the Assertion to be signed but the assertion received was not; or the signature on the Assertion received was not valid.

Actions: Check configuration; check debug for more detailed error message.

MISSING_SUBJECT_COMFIRMATION_DATA

ID: SAML2-96

Level: INFO

Description: SubjectConfirmationData had no Subject.

Data: Assertion ID

Triggers: Service provider received an Assertion whose SubjectConfirmationData had no Subject.

Actions: Check debug for the Assertion received. Contact Identity Provider if needed.

MISSING_RECIPIENT

ID: SAML2-97

Level: INFO

Description: SubjectConfirmationData had no Recipient.

Data: Assertion ID

Triggers: Service provider received an Assertion whose SubjectConfirmationData had no Recipient.

Actions: Check debug for the Assertion received. Contact Identity Provider if needed.

WRONG_RECIPIENT

ID: SAML2-98

Level: INFO

Description: Service Provider is not the intended recipient.

Data: Assertion ID

Triggers: Service provider received an Assertion. But the provider is not the intended recipient of the Assertion.

Actions: Check debug for the Assertion received. Check meta data. Contact Identity Provider if needed.

INVALID_TIME_SUBJECT_CONFIRMATION_DATA

ID: SAML2-99

Level: INFO

Description: Time in SubjectConfirmationData of the Assertion is invalid.

Data: Assertion ID

Triggers: The assertion service provider received had expired timewise.

Actions: Synchronize the time between service provider and identity provider. Increase the time skew attribute for the service provider in its entity config.

CONTAINED_NOT_BEFORE

ID: SAML2-100

Level: INFO

Description: SubjectConfirmationData of the Assertion had NotBefore.

Data: Assertion ID

Triggers: The assertion service provider received had NotBefore.

Actions: Check debug for the Assertion received. Contact identity provider if needed.

WRONG_INRESPONSETO_ASSERTION

ID: SAML2-101

Level: INFO

Description: Assertion contained wrong InResponseTo attribute.

Data: Assertion ID

Triggers: InResponseTo in Assertion is different from the one in Response. Or Assertion didn't contain InResponseTo, but Response did.

Actions: Check debug for the Assertion received. Contact identity provider if needed.

MISSING_CONDITIONS

ID: SAML2-102

Level: INFO

Description: Assertion contained no Conditions.

Data: Assertion ID

Triggers: Conditions is missing from the Single Sign On Assertion.

Actions: Check debug for the Assertion received. Contact identity provider if needed.

MISSING_AUDIENCE_RESTRICTION

ID: SAML2-103

Level: INFO

Description: Assertion contained no AudienceRestriction.

Data: Assertion ID

Triggers: AudienceRestriction is missing from the Single Sign On Assertion.

Actions: Check debug for the Assertion received. Contact identity provider if needed.

WRONG_AUDIENCE

ID: SAML2-104

Level: INFO

Description: Assertion contained wrong Audience.

Data: Assertion ID

Triggers: This service provider was not the intended audience of the single sign on assertion.

Actions: Check debug for the Assertion received. Check meta data. Contact identity provider if needed.

FOUND_AUTHN_ASSERTION

ID: SAML2-105

Level: INFO

Description: Found authentication assertion in the Response.

Data: Assertion ID, Subject if the log level was set to LL_FINE, SesionIndex if any

Triggers: Both the Response and Assertion(s) inside the Response are valid.

INVALID_SSOTOKEN

ID: SAML2-106

Level: INFO

Description: Invalid SSOToken found in Request.

Data: SSOToken value

Triggers: Initiate Single Logout without SSOToken.

MISSING_ENTITY

ID: SAML2-107

Level: INFO

Description: No entity ID is specified in Request.

Data: EntityID value

Triggers: Initiate Request without EntityID.

Actions: Specify EntityID parameter in request URL.

MISSING_META_ALIAS

ID: SAML2-108

Level: INFO

Description: No metaAlias is specified in Request.

Data: MetaAlias value

Triggers: Initiate Request without metaAlias.

Actions: Specify metaAlias parameter in request URL.

REDIRECT_TO_AUTH

ID: SAML2-109

Level: INFO

Description: Redirect request to authentication page.

Data: URL to Authentication page

Triggers: Initiate Request without SSOToken.

CANNOT_DECODE_REQUEST

ID: SAML2-110

Level: INFO

Description: Can not decode URL encoded Query parameter.

Data: URL encoded Query parameter

Triggers: Initiate to decode incorrectly URL encoded Query parameter.

CANNOT_INSTANTIATE_MNI_RESPONSE

ID: SAML2-111

Level: INFO

Description: Can not instantiate MNI Response with input xml.

Data: Input XML string for MNI Response

Triggers: Initiate parse MNI Response with incorrect XML string.

CANNOT_INSTANTIATE_MNI_REQUEST

ID: SAML2-112

Level: INFO

Description: Can not instantiate MNI Request with input XML.

Data: Input XML string for MNI Request

Triggers: Initiate parse MNI Request with incorrect XML string.

CANNOT_INSTANTIATE_SLO_RESPONSE

ID: SAML2-113

Level: INFO

Description: Can not instantiate SLO Response with input XML.

Data: Input XML string for SLO Response

Triggers: Initiate parse SLO Response with incorrect XML string.

CANNOT_INSTANTIATE_SLO_REQUEST

ID: SAML2-114

Level: INFO

Description: Can not instantiate SLO Request with input XML.

Data: Input XML string for SLO Request

Triggers: Initiate parse SLO Request with incorrect XML string.

MNI_REQUEST_INVALID_SIGNATURE

ID: SAML2-115

Level: INFO

Description: Can not varify signature in MNI Request.

Data: MNI Request with signature

Triggers: Sinature in MNI Request is incorrect.

MNI_RESPONSE_INVALID_SIGNATURE

ID: SAML2-116

Level: INFO

Description: Can not valify signature in MNI Response.

Data: MNI Response with signature

Triggers: Sinature in MNI Response is incorrect.

SLO_REQUEST_INVALID_SIGNATURE

ID: SAML2-117

Level: INFO

Description: Can not valify signature in SLO Request.

Data: SLO Request with signature

Triggers: Sinature in SLO Request is incorrect.

SLO_RESPONSE_INVALID_SIGNATURE

ID: SAML2-118

Level: INFO

Description: Can not valify signature in SLO Response.

Data: SLO Response with signature

Triggers: Sinature in SLO Response is incorrect.

NAMEID_INVALID_ENCRYPTION

ID: SAML2-119

Level: INFO

Description: Can not decrypt EncryptedID.

Data: Exception message

Triggers: Decrypt the incorrectly encrypted EncryptedID.

INVALID_MNI_RESPONSE

ID: SAML2-120

Level: INFO

Description: MNI Response has error status.

Data: Status message

Triggers: Requested MNI Request caused problem.

INVALID_SLO_RESPONSE

ID: SAML2-121

Level: INFO

Description: SLO Response has error status.

Data: Status message

Triggers: Requested SLO Request caused problem.

MISSING_ENTITY_ROLE

ID: SAML2-122

Level: INFO

Description: Entity Role is not specified in the request.

Data: Entity Role value

Triggers: Initiate request without Role value.

Actions: Specify Entity Role parameter in the request.

INVALID_ISSUER_REQUEST

ID: SAML2-123

Level: INFO

Description: Issuer in Request is invalid.

Data: Hosted Entity ID, Name of Realm or organization, Request ID

Triggers: Issuer in Request is not configured or not trusted by the hosted provider

Actions: Check configuration.

INVALID_REALM_GET_ALL_ENTITIES

ID: SAML2-124

Level: INFO

Description: Invaid realm while getting all entities.

Data: Realm or organization name

Triggers: Get all entities.

Actions: Check the Realm name.

CONFIG_ERROR_GET_ALL_ENTITIES

ID: SAML2-125

Level: INFO

Description: Configuration error while getting all entities.

Data: Error message, Realm or organization name

Triggers: Get all entities.

Actions: Check debug message for detailed error.

GOT_ALL_ENTITIES

ID: SAML2-126

Level: FINE

Description: Obtained all entities.

Data: Realm or organization name

Triggers: Get all entities.

INVALID_PEP_ID

ID: SAML2-127

Level: INFO

Description: Invalid Policy Enforcement Point (PEP) Identifier.

Data: PEP Identifier

Triggers: Cannot retrieve PEP Metadata

Actions: Provide valid PEP Identifier and retry.

INVALID_PDP_ID

ID: SAML2-128

Level: INFO

Description: Invalid Policy Decision Point (PDP) Identifier.

Data: PDP Identifier

Triggers: Cannot retrieve PDP Metadata

Actions: Provide valid PDP Identifier and retry.

NULL_PDP_SIGN_CERT_ALIAS

ID: SAML2-129

Level: INFO

Description: Certificate Alias is null, cannot sign the message.

Data: The realm from which the metadata was retreived., Entity Identifier for the Policy Decision Point.

Triggers: Cannot sign the message.

Actions: Check the entity's metadata to verify the certificate alias is correct.

NULL_PEP_SIGN_CERT_ALIAS

ID: SAML2-130

Level: INFO

Description: Certificate Alias is null,cannot retreive the certificate.

Data: The realm from which the metadata was retreived., Entity Identifier for the Policy Enforcement Point.

Triggers: Cannot validate the signature in the request message.

Actions: Check the entity's metadata to verify the certificate alias is correct.

INVALID_SIGNATURE_QUERY

ID: SAML2-131

Level: INFO

Description: Invalid Signature in Query Request.

Data: The realm from which the metadata was retreived., Entity Identifier for the Policy Decision Point., Cert Alias used to retrieve certificate from keystore.

Triggers: Cannot process the request, server will send back error to the Requester.

Actions: Check the entity's metadata to verify the certificate alias is correct.; Check the certificate in the keystore for its existance and validity.

INVALID_ISSUER_IN_PEP_REQUEST

ID: SAML2-132

Level: INFO

Description: Issuer in Request is invalid.

Data: Name of Realm or organization, Identity of the Issuer, Hosted Entity Identifier

Triggers: Issuer in Request is not configured or not trusted by the hosted provider therefore Query will fail.

Actions: Check the hosted entity configuration attribute cotlist to make sure the issuer identifier is in the list.

PEP_METADATA_ERROR

ID: SAML2-133

Level: INFO

Description: Unable to retreive Policy Enforcement Point (PEP) Metadata.

Data: PEP Provider Entity Identifier

Triggers: Cannot retrieve PEP Provider Metadata

Actions: Check the Data Store is accessible .; Check the PEP Provider Entity Identifier.

PDP_METADATA_ERROR

ID: SAML2-134

Level: INFO

Description: Unable to retrieve Policy Decision Point (PDP) Metadata.

Data: PDP Provider Entity Identifier

Triggers: Cannot retreive PDP Provider Metadata

Actions: Check the Data Store is accessible .; Check the PDP Provider Entity Identifier.

ASSERTION_FROM_PDP_NOT_ENCRYPTED

ID: SAML2-135

Level: INFO

Description: Assertion in Response not encrypted.

Data: Identity of the Issuer, Response ID

Triggers: Policy Enforcement Point (PEP) Provider requested the assertion in Response to be encrypted, but it received a Response with unencrypted assertion(s).

Actions: Check PEP metadata published to the PDP. Notify Policy Decision Point (PDP) Provider regarding the requirement.

MISSING_ASSERTION_IN_PDP_RESPONSE

ID: SAML2-136

Level: INFO

Description: Response has no Assertion.

Data: Identity of Issuer, Response ID

Triggers: Policy Enforcement Point (PEP) Provider received a Response with no Assertion.

Actions: Check error code of the Response. Notify Policy Decision Point (PDP) Provider to check for errors or possible misconfiguration.

INVALID_ISSUER_IN_ASSERTION_FROM_PDP

ID: SAML2-137

Level: INFO

Description: Issuer in Assertion is not valid.

Data: Assertion Issuer, Assertion ID

Triggers: Issuer in Assertion was not configured at Policy Enforcement Point (PEP) provider, or not trusted by the PEP provider.

Actions: Check the configuration.

MISMATCH_ISSUER_IN_ASSERTION_FROM_PDP

ID: SAML2-138

Level: INFO

Description: Issuer in Assertion doesn't match the Issuer in Response.

Data: Issuer Identifier in the Resposnse, Issuer Identity in the Assertion

Triggers: Error condition, Response will not be accepted.

Actions: Check the Policy Decision Point instance to debug the cause of the problem.

INVALID_SIGNATURE_ASSERTION_FROM_PDP

ID: SAML2-139

Level: INFO

Description: Assertion is not signed or signature is not valid.

Data: Issuer Identity in the Assertion, Assertion ID

Triggers: 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.

Actions: Check PEP metadata configuration.; Check debug for more detailed error message.

REQUEST_MESSAGE

ID: SAML2-140

Level: FINE

Description: Request message from Query Requester

Data: policy decision point entity descriptor, SAMLv2 Query Request Message

Triggers: SAMLv2 SOAP Query

VALID_SIGNATURE_QUERY

ID: SAML2-141

Level: INFO

Description: Valid Signature in Query Request.

Data: The realm from which the metadata was retreived., Entity Identifier for the Policy Decision Point., Cert Alias used to retrieve certificate from keystore.

Triggers: The Request will be processed.

SUCCESS_FED_SSO

ID: SAML2-142

Level: INFO

Description: Successful federation/Single Sign On.

Data: user id, NameID value

Triggers: Successful federation/Single Sign On.

SAE_IDP_SUCCESS

ID: SAML2-143

Level: INFO

Description: SAE_IDP succeeded.

Data: SAE attributes

Triggers: SAE_IDP succeeded.

SAE_IDP_ERROR

ID: SAML2-144

Level: INFO

Description: SAE_IDP failed.

Data: Error message, SAE attributes

Triggers: SAE_IDP failed.

SAE_IDP_ERROR_NODATA

ID: SAML2-145

Level: INFO

Description: SAE_IDP invoked without attributes.

Data: Error message

Triggers: SAE_IDP invoked without attributes.

Actions: Add SAE attributes to request.

SAE_IDP_AUTH

ID: SAML2-146

Level: INFO

Description: SAE_IDP delegated to Auth.

Data: SAE attributes

Triggers: SAE_IDP invoked but no user session.

SAE_SP_SUCCESS

ID: SAML2-147

Level: INFO

Description: SAE_SP succeeded.

Data: SAE attributes

Triggers: SAE_SP succeeded.

SAE_SP_ERROR

ID: SAML2-148

Level: INFO

Description: SAE_SP failed.

Data: Error message

Triggers: SAE_SP failed.

SEND_ECP_RESPONSE

ID: SAML2-149

Level: INFO

Description: Send a response to ECP.

Data: 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

Triggers: Received AuthnRequest.

SEND_ECP_RESPONSE_FAILED

ID: SAML2-150

Level: INFO

Description: Unable to send a response to ECP.

Data: Identity Provider Entity Identifier, Realm or organization name, Assertion Consumer Service URL

Triggers: Send a response to ECP.

CANNOT_INSTANTIATE_SOAP_MESSAGE_ECP

ID: SAML2-151

Level: INFO

Description: Unable to instantiate a SOAP message sent from ECP.

Data: Service Provider Entity Identifier

Triggers: Received a response from ECP.

RECEIVE_SOAP_FAULT_ECP

ID: SAML2-152

Level: INFO

Description: Received a SOAP fault from ECP.

Data: Service Provider Entity Identifier

Triggers: Received a response from ECP.

CANNOT_INSTANTIATE_SOAP_MESSAGE_ECP

ID: SAML2-153

Level: INFO

Description: Unable to instantiate a SAML Response sent from ECP.

Data: Service Provider Entity Identifier

Triggers: Received a response from ECP.

ECP_ASSERTION_NOT_SIGNED

ID: SAML2-154

Level: INFO

Description: Assertion received from ECP is not signed.

Data: Identity Provider Entity Identifier

Triggers: Received a response from ECP.

ECP_ASSERTION_INVALID_SIGNATURE

ID: SAML2-155

Level: INFO

Description: Assertion received from ECP has invalid signature.

Data: Identity Provider Entity Identifier

Triggers: Assertion signature verification.

RECEIVED_AUTHN_REQUEST_ECP

ID: SAML2-156

Level: INFO

Description: Received AuthnRequest from ECP.

Data: Service Provider Entity Identifier, IDP meta alias, authnRequest xml string

Triggers: Single Sign On.

RECEIVED_HTTP_REQUEST_ECP

ID: SAML2-157

Level: INFO

Description: Received HTTP request from ECP.

Data: Service Provider Entity Identifier, Realm or organization name

Triggers: ECP accessed SP Resource.

SEND_ECP_PAOS_REQUEST

ID: SAML2-158

Level: INFO

Description: Send a PAOS request to ECP.

Data: Service Provider Entity Identifier, Realm or organization name, SOAP message string if the log level was set to LL_FINE at run time

Triggers: Received HTTP request from ECP.

SEND_ECP_PAOS_REQUEST_FAILED

ID: SAML2-159

Level: INFO

Description: Unable to send a PAOS request to ECP.

Data: Service Provider Entity Identifier, Realm or organization name

Triggers: Send a PAOS request to ECP.

SUCCESS_FED_TERMINATION

ID: SAML2-160

Level: INFO

Description: Federation termination succeeded.

Data: user id

Triggers: Federation termination succeeded.

SUCCESS_NEW_NAMEID

ID: SAML2-161

Level: INFO

Description: New name identifier succeeded.

Data: user id

Triggers: New name identifier succeeded.

UNKNOWN_PRINCIPAL

ID: SAML2-162

Level: INFO

Description: Unknown princial in manage name ID request.

Data: Manage Name ID request XML

Triggers: Unable to find old name id in the management name id request.

UNABLE_TO_TERMINATE

ID: SAML2-163

Level: INFO

Description: Unable to terminate federation.

Data: user id

Triggers: Unable to terminate federation.

POST_RESPONSE_INVALID_SIGNATURE

ID: SAML2-164

Level: INFO

Description: Unable to verify signature in Single Sign-On Response using POST binding.

Data: Identity Provider Entity ID

Triggers: Error while trying to verify signature in Response.

Actions: Check Identity Provider metadata; Check debug file for detailed info

BINDING_NOT_SUPPORTED

ID: SAML2-165

Level: INFO

Description: Binding is not supported.

Data: Provider Entity ID, Name of binding that is not supported

Triggers: Hosted provider received data from unsupported binding endpoint.

Actions: Check Provider metadata; Check debug file for detailed info

SP_SSO_FAILED

ID: SAML2-166

Level: INFO

Description: Single Sign-On Failed at Service Provider.

Data: Hosted Service Provider Entity ID, Error message, Response received from IDP if the log level was set to LL_FINE at run time

Triggers: Single Sign On failed

Actions: Check debug file for detailed info

INVALID_REALM_FOR_SESSION

ID: SAML2-167

Level: INFO

Description: Invalid realm for the user trying to get an assertion from the IdP.

Data: Realm of the authenticated user, Realm where the IdP is defined, Entity Id of the SP, IP Address of the requester, SAML2 Authentication Request

Triggers: Single Sign On failed

Actions: Check debug file for detailed info

OpenAM logs the following SAML messages.

ASSERTION_CREATED

ID: SAML-1

Level: INFO

Description: New assertion created

Data: message id, Assertion ID or Assertion if log level is LL_FINER

Triggers: Browser Artifact Profile; Browser POST Profile; Create Assertion Artifact; Authentication Query; Attribute Query; Authorization Decision Query

ASSERTION_ARTIFACT_CREATED

ID: SAML-2

Level: INFO

Description: New assertion artifact created

Data: message id, Assertion Artifact, ID of the Assertion corresponding to the Artifact

Triggers: Browser Artifact Profile; Creating Assertion Artifact

ASSERTION_ARTIFACT_REMOVED

ID: SAML-3

Level: FINE

Description: Assertion artifact removed from map

Data: message id, Assertion Artifact

Triggers: SAML Artifact Query; Assertion artifact expires

ASSERTION_REMOVED

ID: SAML-4

Level: FINE

Description: Assertion removed from map

Data: message id, Assertion ID

Triggers: SAML Artifact Query; Assertion expires

ASSERTION_ARTIFACT_VERIFIED

ID: SAML-5

Level: INFO

Description: Access right by assertion artifact verified

Data: message id, Assertion Artifact

Triggers: SAML Artifact Query

AUTH_PROTOCOL_MISMATCH

ID: SAML-6

Level: INFO

Description: Authentication type configured and the actual SOAP protocol do not match.

Data: message id

Triggers: SAML SOAP Query

Actions: 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.

INVALID_AUTH_TYPE

ID: SAML-7

Level: INFO

Description: Invalid authentication type

Data: message id

Triggers: SAML SOAP Query

Actions: Login to console, go to Federation, then SAML, edit the Trusted Partners Configuration, select one of the values for Authentication Type field, then save.

SOAP_RECEIVER_URL

ID: SAML-8

Level: FINE

Description: Remote SOAP receiver URL

Data: message id, SOAP Receiver URL

Triggers: SAML SOAP Query

NO_ASSERTION_IN_RESPONSE

ID: SAML-9

Level: INFO

Description: No assertion present in saml response

Data: message id, SAML Response

Triggers: SAML Artifact Query

Actions: Contact remote partner on what's wrong

MISMATCHED_ASSERTION_AND_ARTIFACT

ID: SAML-10

Level: INFO

Description: Number of assertions in SAML response does not equal to number of artifacts in SAML request.

Data: message id, SAML Response

Triggers: SAML Artifact Query

Actions: Contact remote partner on what's wrong

ARTIFACT_TO_SEND

ID: SAML-11

Level: INFO

Description: Artifact to be sent to remote partner

Data: message id, SAML Artifact

Triggers: SAML Artifact Query

WRONG_SOAP_URL

ID: SAML-12

Level: INFO

Description: Wrong SOAP URL in trusted partner configuration

Data: message id

Triggers: SAML Artifact Query

Actions: Login to console, go to Federation, then SAML, edit the Trusted Partners Configuration, enter value for SOAP URL field, then save.

SAML_ARTIFACT_QUERY

ID: SAML-13

Level: FINE

Description: SAML Artifact Query SOAP request

Data: message id, SAML Artifact Query message

Triggers: SAML Artifact Query

NO_REPLY_FROM_SOAP_RECEIVER

ID: SAML-14

Level: INFO

Description: No reply from remote SAML SOAP Receiver

Data: message id

Triggers: SAML Artifact Query

Actions: Check remote partner on what's wrong

REPLIED_SOAP_MESSAGE

ID: SAML-15

Level: FINE

Description: SAML Artifact Query response

Data: message id, SAML Artifact Query response message

Triggers: SAML Artifact Query

NULL_SAML_RESPONSE

ID: SAML-16

Level: INFO

Description: No SAML response inside SOAP response

Data: message id

Triggers: SAML Artifact Query

Actions: Check remote partner on what's wrong

INVALID_RESPONSE_SIGNATURE

ID: SAML-17

Level: INFO

Description: XML signature for SAML response is not valid

Data: message id

Triggers: SAML Artifact Query

Actions: Check remote partner on what's wrong on XML digital signature

ERROR_RESPONSE_STATUS

ID: SAML-18

Level: INFO

Description: Error in getting SAML response status code

Data: message id

Triggers: SAML Artifact Query

Actions: Check remote partner on what's wrong on response status code

MISSING_TARGET

ID: SAML-19

Level: INFO

Description: TARGET parameter is missing from the request

Data: message id

Triggers: SAML Artifact Profile; SAML POST Profile

Actions: Add "TARGET=target_url" as query parameter in the request

REDIRECT_TO_URL

ID: SAML-20

Level: INFO

Description: Redirection URL in SAML artifact source site

Data: message id, target, redirection URL, SAML response message in case of POST profile and log level is LL_FINER

Triggers: SAML Artifact Profile source; SAML POST Profile source

TARGET_FORBIDDEN

ID: SAML-21

Level: INFO

Description: The specified target site is forbidden

Data: message id, target URL

Triggers: SAML Artifact Profile source; SAML POST Profile source

Actions: 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

FAILED_TO_CREATE_SSO_TOKEN

ID: SAML-22

Level: INFO

Description: Failed to create single-sign-on token

Data: message id

Triggers: SAML Artifact Profile destination; SAML POST Profile destination

Actions: Authentication component failed to create SSO token, please check authentication log and debug for more details

ACCESS_GRANTED

ID: SAML-23

Level: INFO

Description: Single sign on successful, access to target is granted

Data: message id, Response message in case of POST profile and log levele is LL_FINER or higher

Triggers: SAML Artifact Profile destination; SAML POST Profile destination

NULL_PARAMETER

ID: SAML-24

Level: INFO

Description: Null servlet request or response

Data: message id

Triggers: SAML Artifact Profile; SAML POST Profile

Actions: Check web container error log for details

MISSING_RESPONSE

ID: SAML-25

Level: INFO

Description: Missing SAML response in POST body

Data: message id

Triggers: SAML POST Profile destination

Actions: Check with remote SAML partner to see why SAML response object is missing from HTTP POST body

RESPONSE_MESSAGE_ERROR

ID: SAML-26

Level: INFO

Description: Error in response message

Data: message id

Triggers: SAML POST Profile destination

Actions: 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.

INVALID_RESPONSE

ID: SAML-27

Level: INFO

Description: Response is not valid

Data: message id

Triggers: SAML POST Profile destination

Actions: recipient attribute in SAML response does not match this site's POST profile URL; Response status code is not success

SOAP_MESSAGE_FACTORY_ERROR

ID: SAML-28

Level: INFO

Description: Failed to get an instance of the message factory

Data: message id

Triggers: SAML SOAP Receiver init

Actions: Check your SOAP factory property (javax.xml.soap.MessageFactory) to make sure it is using a valid SOAP factory implementation

UNTRUSTED_SITE

ID: SAML-29

Level: INFO

Description: Received Request from an untrusted site

Data: message id, Remote site Hostname or IP Address

Triggers: SAML SOAP Queries

Actions: 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.

INVALID_REQUEST

ID: SAML-30

Level: INFO

Description: Invalid request from remote partner site

Data: message id and request hostname/IP address, return response

Triggers: SAML SOAP Queries

Actions: Check with administrator of remote partner site

SOAP_REQUEST_MESSAGE

ID: SAML-31

Level: FINE

Description: Request message from partner site

Data: message id and request hostname/IP address, request xml

Triggers: SAML SOAP Queries

BUILD_RESPONSE_ERROR

ID: SAML-32

Level: INFO

Description: Failed to build response due to internal server error

Data: message id

Triggers: SAML SOAP Queries

Actions: Check debug message to see why it is failing, for example, cannot create response status, major/minor version error, etc.

SENDING_RESPONSE

ID: SAML-33

Level: INFO

Description: Sending SAML response to partner site

Data: message id, SAML response or response id

Triggers: SAML SOAP Queries

SOAP_FAULT_ERROR

ID: SAML-34

Level: INFO

Description: Failed to build SOAP fault response body

Data: message id

Triggers: SAML SOAP Queries

Actions: Check debug message to see why it is failing, for example, unable to create SOAP fault, etc.

OpenAM logs the following WSFederation messages.

INVALID_SIGNATURE_ASSERTION

ID: WSFederation-1

Level: INFO

Description: Assertion is not signed or signature is not valid.

Data: Assertion or assertion ID, Realm or organization name, Assertion issuer

Triggers: Service provider requested the Assertion to be signed but the assertion received was not; or the signature on the Assertion received was not valid.

Actions: Check configuration; check debug for more detailed error message.

MISSING_CONDITIONS_NOT_ON_OR_AFTER

ID: WSFederation-2

Level: INFO

Description: Assertion conditions are missing notOnOrAfter attribute.

Data: Assertion or assertion ID

Triggers: The Conditions element of the assertion is missing its notOnOrAfter attribute.

Actions: Check the assertion. Contact Identity Provider if needed.

ASSERTION_EXPIRED

ID: WSFederation-3

Level: INFO

Description: Assertion has expired.

Data: Assertion or assertion ID, Assertion notOnOrAfter time, Time skew in seconds, Current time

Triggers: The current time is after the assertion's notOnOrAfter time plus the time skew.

Actions: Synchronize server clocks. Contact Identity Provider if needed.

MISSING_CONDITIONS_NOT_BEFORE

ID: WSFederation-4

Level: INFO

Description: Assertion conditions are missing notBefore attribute.

Data: Assertion or assertion ID

Triggers: The Conditions element of the assertion is missing its notBefore attribute.

Actions: Check the assertion. Contact Identity Provider if needed.

ASSERTION_NOT_YET_VALID

ID: WSFederation-5

Level: INFO

Description: Assertion not yet valid.

Data: Assertion or assertion ID, Assertion notBefore time, Time skew in seconds, Current time

Triggers: The current time is before the assertion's notBefore time minus the time skew.

Actions: Synchronize server clocks. Contact Identity Provider if needed.

MISSING_WRESULT

ID: WSFederation-6

Level: INFO

Description: WS-Federation response is missing wresult.

Data: WS-Federation response

Triggers: The WS-Federation response is missing its wresult parameter.

Actions: Check the response. Contact Identity Provider if needed.

MISSING_WCTX

ID: WSFederation-7

Level: INFO

Description: WS-Federation response is missing wctx.

Data: WS-Federation response

Triggers: The WS-Federation response is missing its wctx parameter.

Actions: Check the response. Contact Identity Provider if needed.

INVALID_WRESULT

ID: WSFederation-8

Level: INFO

Description: WS-Federation response is invalid.

Data: WS-Federation response

Triggers: The WS-Federation response is not a valid RequestSecurityTokenResponse element.

Actions: Check the response. Contact Identity Provider if needed.

CONFIG_ERROR_GET_ENTITY_CONFIG

ID: WSFederation-9

Level: INFO

Description: Configuration error while getting entity config.

Data: Error message, MetaAlias, Realm or organization name

Triggers: Obtain entity config.

Actions: Check debug message for detailed error.

CANT_FIND_SP_ACCOUNT_MAPPER

ID: WSFederation-10

Level: INFO

Description: Can't find SP Account Mapper.

Data: Error message, Account mapper class name

Triggers: Cannot get class object for SP account mapper class.

Actions: Check the configuration. Ensure that SP account mapper class name is correct and that the account mapper class is on the classpath.

CANT_CREATE_SP_ACCOUNT_MAPPER

ID: WSFederation-11

Level: INFO

Description: Can't create SP Account Mapper.

Data: Error message, Account mapper class name

Triggers: Cannot create SP account mapper object.

Actions: Check the configuration. Ensure that SP account mapper class name is correct and that the account mapper class is on the classpath.

CANT_CREATE_SESSION

ID: WSFederation-12

Level: INFO

Description: Can't create session for user.

Data: Error message, Realm or organization name, User name, Auth level

Triggers: Cannot create session for user.

Actions: Check the configuration. Ensure that SP account mapper is finding a user in the local store.

SSO_SUCCESSFUL

ID: WSFederation-13

Level: INFO

Description: Single sign-on completed successfully.

Data: wctx, Assertion or assertion ID, Realm or organization name, User ID, Authentication Level, Target URL

Triggers: Successful WS-Federation RP Signin Response.

UNTRUSTED_ISSUER

ID: WSFederation-14

Level: INFO

Description: Assertion issuer is not trusted by this service provider.

Data: Assertion or assertion ID, Realm or organization name, Service provider ID, Target URL

Triggers: Cannot create session for user.

Actions: Check the configuration. Ensure that SP account mapper is finding a user in the local store.

MISSING_SUBJECT

ID: WSFederation-15

Level: INFO

Description: Assertion does not contain a subject element.

Data: Assertion or assertion ID

Triggers: Assertion does not contain a subject element.

Actions: Check the assertion. Contact Identity Provider if needed.

GOT_FEDERATION

ID: WSFederation-16

Level: FINE

Description: Federation obtained.

Data: Federation ID, Realm or organization name

Triggers: Obtain federation.

GOT_INVALID_ENTITY_DESCRIPTOR

ID: WSFederation-17

Level: INFO

Description: Obtained invalid entity descriptor.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity descriptor.

Actions: Delete invalid entity descriptor and import it again.

CONFIG_ERROR_GET_ENTITY_DESCRIPTOR

ID: WSFederation-18

Level: INFO

Description: Configuration error while getting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Obtain entity descriptor.

Actions: Check debug message for detailed error.

SET_ENTITY_DESCRIPTOR

ID: WSFederation-19

Level: INFO

Description: Entity descriptor was set.

Data: Entity ID, Realm or organization name

Triggers: Set entity descriptor.

CONFIG_ERROR_SET_ENTITY_DESCRIPTOR

ID: WSFederation-20

Level: INFO

Description: Configuration error while setting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Set entity descriptor.

Actions: Check debug message for detailed error.

SET_INVALID_ENTITY_DESCRIPTOR

ID: WSFederation-21

Level: INFO

Description: Invalid entity descriptor to set.

Data: Entity ID, Realm or organization name

Triggers: Set entity descriptor.

Actions: Check entity descriptor if it follows the schema.

ENTITY_DESCRIPTOR_CREATED

ID: WSFederation-22

Level: INFO

Description: Entity descriptor was created.

Data: Entity ID, Realm or organization name

Triggers: Create entity descriptor.

CONFIG_ERROR_CREATE_ENTITY_DESCRIPTOR

ID: WSFederation-23

Level: INFO

Description: Configuration error while creating entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Create entity descriptor.

Actions: Check debug message for detailed error.

CREATE_INVALID_ENTITY_DESCRIPTOR

ID: WSFederation-24

Level: INFO

Description: Invalid entity descriptor to create.

Data: Entity ID, Realm or organization name

Triggers: Create entity descriptor.

Actions: Check entity descriptor if it follows the schema.

ENTITY_DESCRIPTOR_DELETED

ID: WSFederation-25

Level: INFO

Description: Entity descriptor was deleted.

Data: Entity ID, Realm or organization name

Triggers: Delete entity descriptor.

CONFIG_ERROR_DELETE_ENTITY_DESCRIPTOR

ID: WSFederation-26

Level: INFO

Description: Configuration error while deleting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Delete entity descriptor.

Actions: Check debug message for detailed error.

GOT_ENTITY_CONFIG

ID: WSFederation-27

Level: FINE

Description: Entity config obtained.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity config.

GOT_INVALID_ENTITY_CONFIG

ID: WSFederation-28

Level: INFO

Description: Obtained invalid entity config.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity config.

Actions: Delete invalid entity config and import it again.

CONFIG_ERROR_GET_ENTITY_CONFIG

ID: WSFederation-29

Level: INFO

Description: Configuration error while getting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Obtain entity config.

Actions: Check debug message for detailed error.

NO_ENTITY_ID_SET_ENTITY_CONFIG

ID: WSFederation-30

Level: INFO

Description: No entity ID while setting entity config.

Data: Realm or organization name

Triggers: Set entity config.

Actions: Set entity ID in entity config.

SET_ENTITY_CONFIG

ID: WSFederation-31

Level: INFO

Description: Entity config was set.

Data: Entity ID, Realm or organization name

Triggers: Set entity config.

CONFIG_ERROR_SET_ENTITY_CONFIG

ID: WSFederation-32

Level: INFO

Description: Configuration error while setting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Set entity config.

Actions: Check debug message for detailed error.

SET_INVALID_ENTITY_CONFIG

ID: WSFederation-33

Level: INFO

Description: Invalid entity config to set.

Data: Entity ID, Realm or organization name

Triggers: Set entity config.

Actions: Check entity config if it follows the schema.

NO_ENTITY_ID_CREATE_ENTITY_CONFIG

ID: WSFederation-34

Level: INFO

Description: No entity ID while creating entity config.

Data: Realm or organization name

Triggers: Create entity config.

Actions: Set entity ID in entity config.

NO_ENTITY_DESCRIPTOR_CREATE_ENTITY_CONFIG

ID: WSFederation-35

Level: INFO

Description: Entity config doesn't exist while creating entity config.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Create entity descriptor before create entity config.

ENTITY_CONFIG_EXISTS

ID: WSFederation-36

Level: INFO

Description: Entity config exists while creating entity config.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Delete existing entity config first.

ENTITY_CONFIG_CREATED

ID: WSFederation-37

Level: INFO

Description: Entity config was created.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

CONFIG_ERROR_CREATE_ENTITY_CONFIG

ID: WSFederation-38

Level: INFO

Description: Configuration error while creating entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Check debug message for detailed error.

CREATE_INVALID_ENTITY_CONFIG

ID: WSFederation-39

Level: INFO

Description: Invalid entity config to create.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Check entity config if it follows the schema.

NO_ENTITY_CONFIG_DELETE_ENTITY_CONFIG

ID: WSFederation-40

Level: INFO

Description: Entity config doesn't exist while deleting entity config.

Data: Entity ID, Realm or organization name

Triggers: Delete entity config.

Actions: Check debug message for detailed error.

ENTITY_CONFIG_DELETED

ID: WSFederation-41

Level: INFO

Description: Entity config was deleted.

Data: Entity ID, Realm or organization name

Triggers: Delete entity config.

CONFIG_ERROR_DELETE_ENTITY_CONFIG

ID: WSFederation-42

Level: INFO

Description: Configuration error while deleting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Delete entity config.

Actions: Check debug message for detailed error.

CONFIG_ERROR_GET_ALL_HOSTED_ENTITIES

ID: WSFederation-43

Level: INFO

Description: Configuration error while getting all hosted entities.

Data: Error message, Realm or organization name

Triggers: Get all hosted entities.

Actions: Check debug message for detailed error.

GOT_ALL_HOSTED_ENTITIES

ID: WSFederation-44

Level: FINE

Description: Obtained all hosted entities.

Data: Realm or organization name

Triggers: Get all hosted entities.

CONFIG_ERROR_GET_ALL_REMOTE_ENTITIES

ID: WSFederation-45

Level: INFO

Description: Configuration error while getting all remote entities.

Data: Error message, Realm or organization name

Triggers: Get all remote entities.

Actions: Check debug message for detailed error.

GOT_ALL_REMOTE_ENTITIES

ID: WSFederation-46

Level: FINE

Description: Obtained all remote entities.

Data: Error message, Realm or organization name

Triggers: Get all remote entities.

CONFIG_ERROR_GET_ALL_ENTITIES

ID: WSFederation-47

Level: INFO

Description: Configuration error while getting all entities.

Data: Error message, Realm or organization name

Triggers: Get all entities.

Actions: Check debug message for detailed error.

GOT_ALL_ENTITIES

ID: WSFederation-48

Level: FINE

Description: Obtained all entities.

Data: Realm or organization name

Triggers: Get all entities.

ASSERTION_CREATED

ID: WSFederation-49

Level: INFO

Description: Assertion created successfully.

Data: Assertion or assertion ID

Triggers: Creation of WS-Federation IdP Signin Response.

NO_ACS_URL

ID: WSFederation-50

Level: INFO

Description: Could not find an Assertion Consumer Service URL.

Data: Realm or organization name, Service provider ID, Reply URL

Triggers: No ACS URL in configuration.; ACS URL provided in request not found in configuration.

Actions: Check configuration for service provider.

SLO_SUCCESSFUL

ID: WSFederation-51

Level: INFO

Description: Single logout completed successfully.

Data: Reply URL

Triggers: Successful single logout.

OpenAM logs the following WebServicesSecurity messages.

UNSUPPORTED_TOKEN_TYPE

ID: WebServicesSecurity-1

Level: INFO

Description: Unsupported Token Type sent to STS for Security Token creation.

Data: Token Type sent by client to STS

Triggers: Invalid or unsupported token type sent by client to STS.

Actions: Check the Token Type sent by client to STS.

CREATED_SAML11_ASSERTION

ID: WebServicesSecurity-2

Level: INFO

Description: Successfully created SAML 1.1 assertion by STS.

Data: Assertion ID, Issuer of this SAML assertion, Service Provider for which this Assertion is created or applies to, Confirmation Method, Token Type, Key Type

Triggers: Valid parameters sent by client to STS to create SAML assetion.

CREATED_SAML20_ASSERTION

ID: WebServicesSecurity-3

Level: INFO

Description: Successfully created SAML 2.0 assertion by STS.

Data: Assertion ID, Issuer of this SAML assertion, Service Provider for which this Assertion is created or applies to, Confirmation Method, Token Type, Key Type

Triggers: Valid parameters sent by client to STS to create SAML assetion.

ERROR_SIGNING_SAML_ASSERTION

ID: WebServicesSecurity-4

Level: INFO

Description: Error during signing SAML assertion by STS.

Data: Actual Error message

Triggers: Problem in STS's Certificate or Private key.

Actions: Check the certificate of STS.; Check the Private Key of STS.

ERROR_CREATING_SAML11_ASSERTION

ID: WebServicesSecurity-5

Level: INFO

Description: Error during creation of SAML 1.1 Assertion by STS.

Data: Actual Error message

Triggers: Invalid parameters sent to create SAML 1.1 Assertion.

Actions: Check all the parameters sent to create SAML 1.1 Assertion.

ERROR_CREATING_SAML20_ASSERTION

ID: WebServicesSecurity-6

Level: INFO

Description: Error during creation of SAML 2.0 Assertion by STS.

Data: Actual Error message

Triggers: Invalid parameters sent to create SAML 2.0 Assertion.

Actions: Check all the parameters sent to create SAML 2.0 Assertion.

IDENTITY_SUBJECT_NAME

ID: WebServicesSecurity-7

Level: INFO

Description: Security token being created for this Identity.

Data: Subject or Identity of the token

ATTR_MAP_FOR_SP

ID: WebServicesSecurity-8

Level: INFO

Description: Security token being created with this Attribute Map for Service Provider.

Data: Attribute Map required by Service Provider

Triggers: Service Provider needs Attributes to be populated in Security token.

SUCCESS_VALIDATE_REQUEST

ID: WebServicesSecurity-9

Level: INFO

Description: Successfully validated the incoming SOAP request.

Data: Provider name to identify the STS service or WSP profile, Security Mechanism or authentication token sent by client

REQUEST_TO_BE_VALIDATED

ID: WebServicesSecurity-10

Level: FINE

Description: Incoming SOAP request to be validated.

Data: Complete SOAP request

RESPONSE_TO_BE_SECURED

ID: WebServicesSecurity-11

Level: FINE

Description: Outgoing SOAP response to be secured.

Data: Complete SOAP response

SUCCESS_SECURE_RESPONSE

ID: WebServicesSecurity-12

Level: INFO

Description: Successfully secured the outgoing SOAP response.

Data: Provider name to identify the STS service or WSP profile

REQUEST_TO_BE_SECURED

ID: WebServicesSecurity-13

Level: FINE

Description: Outgoing SOAP request to be secured.

Data: Complete SOAP request

SUCCESS_SECURE_REQUEST

ID: WebServicesSecurity-14

Level: INFO

Description: Successfully secured the outgoing SOAP request.

Data: Provider name to identify the STS client or WSC profile, Security Mechanism or authentication token sent by client

RESPONSE_TO_BE_VALIDATED

ID: WebServicesSecurity-15

Level: FINE

Description: Incoming SOAP response to be validated.

Data: Complete SOAP response

SUCCESS_VALIDATE_RESPONSE

ID: WebServicesSecurity-16

Level: INFO

Description: Successfully validated the incoming SOAP response.

Data: Provider name to identify the STS client or WSC profile

AUTHENTICATION_FAILED

ID: WebServicesSecurity-17

Level: INFO

Description: Authentication of the incoming SOAP request failed at server or WSP.

Data: Security Mechanism or Security token sent by client

Triggers: Invalid Security Mechanism or Security token sent by client.

Actions: Check Security Mechanism or Security token sent by client.

ERROR_PARSING_SOAP_HEADERS

ID: WebServicesSecurity-18

Level: INFO

Description: Error in parsing SOAP headers from incoming SOAP request.

Data: Actual error message

Triggers: Client has sent incorrect SOAP headers.

Actions: Check SOAP headers.

ERROR_ADDING_SECURITY_HEADER

ID: WebServicesSecurity-19

Level: INFO

Description: Error in adding Security header in outgoing SOAP request.

Data: Actual error message

Triggers: Error in adding namespaces or creating Security Header element.

Actions: Check namespaces and Secuirty Header.

SIGNATURE_VALIDATION_FAILED

ID: WebServicesSecurity-20

Level: INFO

Description: Signature validation failed in incoming SOAP request / response.

Data: Actual error message

Triggers: Error in signing request / response by client / server.

Actions: Check keystore and certificate used for signing.

UNABLE_TO_SIGN

ID: WebServicesSecurity-21

Level: INFO

Description: Unable to sign SOAP request or response.

Data: Actual error message

Triggers: Error in retrieving certificate from the keystore.

Actions: Check keystore configuration and certificate used for signing.; Check debug file for detailed info.

UNABLE_TO_ENCRYPT

ID: WebServicesSecurity-22

Level: INFO

Description: Unable to encrypt SOAP request or response.

Data: Actual error message

Triggers: Error in retrieving certificate from the keystore.

Actions: Check keystore configuration and certificate used for encryption.; Check debug file for detailed info.

UNABLE_TO_DECRYPT

ID: WebServicesSecurity-23

Level: INFO

Description: Unable to decrypt SOAP request or response.

Data: Actual error message

Triggers: Error in retrieving certificate from the keystore.

Actions: Check keystore configuration and certificate used for decryption.; Check debug file for detailed info.

SUCCESS_RETRIEVING_TOKEN_FROM_STS

ID: WebServicesSecurity-24

Level: INFO

Description: Successfully retrieved Security Token from STS service.

Data: 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

Triggers: All the required input data parameters are correct.

ERROR_RETRIEVING_TOKEN_FROM_STS

ID: WebServicesSecurity-25

Level: INFO

Description: Error in retrieving Security Token from STS service.

Data: Actual error message

Triggers: Some or more required input data parameters are not correct.

Actions: Check all the required input data parameters.; Check debug file for detailed error.

ERROR_RETRIEVING_TOKEN_FROM_STS

ID: WebServicesSecurity-26

Level: SEVERE

Description: Error in retrieving Security Token from STS service.

Data: Actual error message

Triggers: Some or more required input data parameters are not correct.

Actions: Check all the required input data parameters.; Check debug file for detailed error.

ERROR_CREATING_SAML11_ASSERTION

ID: WebServicesSecurity-27

Level: SEVERE

Description: Error during creation of SAML 1.1 Assertion by STS.

Data: Actual Error message

Triggers: Invalid parameters sent to create SAML 1.1 Assertion.

Actions: Check all the parameters sent to create SAML 1.1 Assertion.; Check debug file for detailed error.

ERROR_CREATING_SAML20_ASSERTION

ID: WebServicesSecurity-28

Level: SEVERE

Description: Error during creation of SAML 2.0 Assertion by STS.

Data: Actual Error message

Triggers: Invalid parameters sent to create SAML 2.0 Assertion.

Actions: Check all the parameters sent to create SAML 2.0 Assertion.; Check debug file for detailed error.

OpenAM logs the following AUTHENTICATION messages.

LOGIN_SUCCESS

ID: AUTHENTICATION-100

Level: INFO

Description: Authentication is Successful

Data: message, no session

Triggers: User authenticated with valid credentials

LOGIN_SUCCESS_USER

ID: AUTHENTICATION-101

Level: INFO

Description: User based authentication is successful

Data: message, authentication type, user name, no session

Triggers: User authenticated with valid credentials

LOGIN_SUCCESS_ROLE

ID: AUTHENTICATION-102

Level: INFO

Description: Role based authentication is successful

Data: message, authentication type, role name, no session

Triggers: User belonging to role authenticated with valid credentials

LOGIN_SUCCESS_SERVICE

ID: AUTHENTICATION-103

Level: INFO

Description: Service based authentication is successful

Data: message, authentication type, service name, no session

Triggers: User authenticated with valid credentials to a configured service under realm

LOGIN_SUCCESS_LEVEL

ID: AUTHENTICATION-104

Level: INFO

Description: Authentication level based authentication is successful

Data: message, authentication type, authentication level value, no session

Triggers: User authenticated with valid credentials to one or more authentication modules having authentication level value greater than or equal to specified authentication level

LOGIN_SUCCESS_MODULE_INSTANCE

ID: AUTHENTICATION-105

Level: INFO

Description: Module based authentication is successful

Data: message, authentication type, module name, no session

Triggers: User authenticated with valid credentials to authentication module under realm

LOGIN_FAILED

ID: AUTHENTICATION-200

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Incorrect/invalid credentials presented; User locked out/not active

Actions: Enter correct/valid credentials to required authentication module

LOGIN_FAILED_INVALIDPASSWORD

ID: AUTHENTICATION-201

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_NOCONFIG

ID: AUTHENTICATION-202

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Named Configuration (Auth Chain) does not exist.

Actions: Create and configure a named config for this org.

LOGIN_FAILED_NOUSERPROFILE

ID: AUTHENTICATION-203

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_USERINACTIVE

ID: AUTHENTICATION-204

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: This user is not active.

Actions: Activate the user.

LOGIN_FAILED_LOCKEDOUT

ID: AUTHENTICATION-205

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_ACCOUNTEXPIRED

ID: AUTHENTICATION-206

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_LOGINTIMEOUT

ID: AUTHENTICATION-207

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Login timed out.

Actions: Try to login again.

LOGIN_FAILED_MODULEDENIED

ID: AUTHENTICATION-208

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_MAXSESSIONREACHED

ID: AUTHENTICATION-209

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_INVALIDDOMAIN

ID: AUTHENTICATION-210

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_ORGINACTIVE

ID: AUTHENTICATION-211

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_SESSIONCREATEERROR

ID: AUTHENTICATION-212

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGIN_FAILED_USER

ID: AUTHENTICATION-213

Level: INFO

Description: User based authentication failed

Data: error message, authentication type, user name

Triggers: No authentication configuration (chain of one or more authentication modules) configured for user; Incorrect/invalid credentials presented; User locked out/not active

Actions: Configure authentication configuration (chain of one or more authentication modules) for user; Enter correct/valid credentials to required authentication module

LOGIN_FAILED_USER_INVALIDPASSWORD

ID: AUTHENTICATION-214

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_USER_NOCONFIG

ID: AUTHENTICATION-215

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: Named Configuration (Auth Chain) does not exist for this user

Actions: Create and configure a named config for this user

LOGIN_FAILED_USER_NOUSERPROFILE

ID: AUTHENTICATION-216

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_USER_USERINACTIVE

ID: AUTHENTICATION-217

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. This user is not active.

Actions: Activate the user.

LOGIN_FAILED_USER_LOCKEDOUT

ID: AUTHENTICATION-218

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_USER_ACCOUNTEXPIRED

ID: AUTHENTICATION-219

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_USER_LOGINTIMEOUT

ID: AUTHENTICATION-220

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. Login timed out.

Actions: Try to login again.

LOGIN_FAILED_USER_MODULEDENIED

ID: AUTHENTICATION-221

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_USER_MAXSESSIONREACHED

ID: AUTHENTICATION-222

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based auth. Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_USER_INVALIDDOMAIN

ID: AUTHENTICATION-223

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based auth. Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_USER_ORGINACTIVE

ID: AUTHENTICATION-224

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based auth. Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_USER_SESSIONCREATEERROR

ID: AUTHENTICATION-225

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based auth. Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGIN_FAILED_ROLE

ID: AUTHENTICATION-226

Level: INFO

Description: Role based authentication failed

Data: error message, authentication type, role name

Triggers: 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

Actions: 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

LOGIN_FAILED_ROLE_INVALIDPASSWORD

ID: AUTHENTICATION-227

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_ROLE_NOCONFIG

ID: AUTHENTICATION-228

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Named Configuration (Auth Chain) does not exist for this role.

Actions: Create and configure a named config for this role.

LOGIN_FAILED_ROLE_NOUSERPROFILE

ID: AUTHENTICATION-229

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_ROLE_USERINACTIVE

ID: AUTHENTICATION-230

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. This user is not active.

Actions: Activate the user.

LOGIN_FAILED_ROLE_LOCKEDOUT

ID: AUTHENTICATION-231

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_ROLE_ACCOUNTEXPIRED

ID: AUTHENTICATION-232

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_ROLE_LOGINTIMEOUT

ID: AUTHENTICATION-233

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. Login timed out.

Actions: Try to login again.

LOGIN_FAILED_ROLE_MODULEDENIED

ID: AUTHENTICATION-234

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_ROLE_MAXSESSIONREACHED

ID: AUTHENTICATION-235

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based auth. Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_ROLE_INVALIDDOMAIN

ID: AUTHENTICATION-236

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based auth. Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_ROLE_ORGINACTIVE

ID: AUTHENTICATION-237

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based auth. Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_ROLE_SESSIONCREATEERROR

ID: AUTHENTICATION-238

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based auth. Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGIN_FAILED_ROLE_USERNOTFOUND

ID: AUTHENTICATION-239

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based auth. User does not belong to this role.

Actions: Add the user to this role.

LOGIN_FAILED_SERVICE

ID: AUTHENTICATION-240

Level: INFO

Description: Service based authentication failed

Data: error message, authentication type, service name

Triggers: No authentication configuration (chain of one or more authentication modules) configured for service; Incorrect/invalid credentials presented; User locked out/not active

Actions: Configure authentication configuration (chain of one or more authentication modules) for service; Enter correct/valid credentials to required authentication module

LOGIN_FAILED_SERVICE_INVALIDPASSWORD

ID: AUTHENTICATION-241

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_SERVICE_NOCONFIG

ID: AUTHENTICATION-242

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Named Configuration (Auth Chain) does not exist with this service name.

Actions: Create and configure a named config.

LOGIN_FAILED_SERVICE_NOUSERPROFILE

ID: AUTHENTICATION-243

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_SERVICE_USERINACTIVE

ID: AUTHENTICATION-244

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. This user is not active.

Actions: Activate the user.

LOGIN_FAILED_SERVICE_LOCKEDOUT

ID: AUTHENTICATION-245

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_SERVICE_ACCOUNTEXPIRED

ID: AUTHENTICATION-246

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_SERVICE_LOGINTIMEOUT

ID: AUTHENTICATION-247

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. Login timed out.

Actions: Try to login again.

LOGIN_FAILED_SERVICE_MODULEDENIED

ID: AUTHENTICATION-248

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_SERVICE_NOSERVICE

ID: AUTHENTICATION-249

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. Service does not exist.

Actions: Please use only valid Service.

LOGIN_FAILED_SERVICE_MAXSESSIONREACHED

ID: AUTHENTICATION-250

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based auth. Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_SERVICE_INVALIDDOMAIN

ID: AUTHENTICATION-251

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based auth. Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_SERVICE_ORGINACTIVE

ID: AUTHENTICATION-252

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based auth. Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_SERVICE_SESSIONCREATEERROR

ID: AUTHENTICATION-253

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based auth. Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGIN_FAILED_LEVEL

ID: AUTHENTICATION-254

Level: INFO

Description: Authentication level based authentication failed

Data: error message, authentication type, authentication level value

Triggers: 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

Actions: 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

LOGIN_FAILED_LEVEL_INVALIDPASSWORD

ID: AUTHENTICATION-255

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_LEVEL_NOCONFIG

ID: AUTHENTICATION-256

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. No Auth Configuration available.

Actions: Create an auth configuration.

LOGIN_FAILED_LEVEL_NOUSERPROFILE

ID: AUTHENTICATION-257

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_LEVEL_USERINACTIVE

ID: AUTHENTICATION-258

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. This user is not active.

Actions: Activate the user.

LOGIN_FAILED_LEVEL_LOCKEDOUT

ID: AUTHENTICATION-259

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_LEVEL_ACCOUNTEXPIRED

ID: AUTHENTICATION-260

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_LEVEL_LOGINTIMEOUT

ID: AUTHENTICATION-261

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. Login timed out.

Actions: Try to login again.

LOGIN_FAILED_LEVEL_MODULEDENIED

ID: AUTHENTICATION-262

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_LEVEL_INCORRECTLEVEL

ID: AUTHENTICATION-263

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. Invalid Authg Level.

Actions: Please specify valid auth level.

LOGIN_FAILED_LEVEL_MAXSESSIONREACHED

ID: AUTHENTICATION-264

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based auth. Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_LEVEL_INVALIDDOMAIN

ID: AUTHENTICATION-265

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based auth. Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_LEVEL_ORGINACTIVE

ID: AUTHENTICATION-266

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based auth. Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_LEVEL_SESSIONCREATEERROR

ID: AUTHENTICATION-267

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based auth. Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGIN_FAILED_MODULE_INSTANCE

ID: AUTHENTICATION-268

Level: INFO

Description: Module based authentication failed

Data: error message, authentication type, module name

Triggers: Module is not registered/configured under realm; Incorrect/invalid credentials presented; User locked out/not active

Actions: Register/configure authentication module under realm; Enter correct/valid credentials to authentication module

LOGIN_FAILED_MODULE_INSTANCE_INVALIDPASSWORD

ID: AUTHENTICATION-269

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_MODULE_INSTANCE_NOUSERPROFILE

ID: AUTHENTICATION-270

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_MODULE_INSTANCE_USERINACTIVE

ID: AUTHENTICATION-271

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. This user is not active.

Actions: Activate the user.

LOGIN_FAILED_MODULE_INSTANCE_LOCKEDOUT

ID: AUTHENTICATION-272

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_MODULE_INSTANCE_ACCOUNTEXPIRED

ID: AUTHENTICATION-273

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_MODULE_INSTANCE_LOGINTIMEOUT

ID: AUTHENTICATION-274

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. Login timed out.

Actions: Try to login again.

LOGIN_FAILED_MODULE_INSTANCE_MODULEDENIED

ID: AUTHENTICATION-275

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_MODULE_INSTANCE_MAXSESSIONREACHED

ID: AUTHENTICATION-276

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based auth. Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_MODULE_INSTANCE_INVALIDDOMAIN

ID: AUTHENTICATION-277

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based auth. Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_MODULE_INSTANCE_ORGINACTIVE

ID: AUTHENTICATION-278

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based auth. Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_MODULE_INSTANCE_SESSIONCREATEERROR

ID: AUTHENTICATION-279

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based auth. Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGOUT

ID: AUTHENTICATION-300

Level: INFO

Description: User logout is Successful

Data: message

Triggers: User logged out

LOGOUT_USER

ID: AUTHENTICATION-301

Level: INFO

Description: User logout is successful from user based authentication

Data: message, authentication type, user name

Triggers: User logged out

LOGOUT_ROLE

ID: AUTHENTICATION-302

Level: INFO

Description: User logout is successful from role based authentication

Data: message, authentication type, role name

Triggers: User belonging to this role logged out

LOGOUT_SERVICE

ID: AUTHENTICATION-303

Level: INFO

Description: User logout is successful from service based authentication

Data: message, authentication type, service name

Triggers: User logged out of a configured service under realm

LOGOUT_LEVEL

ID: AUTHENTICATION-304

Level: INFO

Description: User logout is successful from authentication level based authentication

Data: message, authentication type, authentication level value

Triggers: User logged out of one or more authentication modules having authentication level value greater than or equal to specified authentication level

LOGOUT_MODULE_INSTANCE

ID: AUTHENTICATION-305

Level: INFO

Description: User logout is successful from module based authentication

Data: message, authentication type, module name

Triggers: User logged out of authentication module under realm

CHANGE_USER_PASSWORD_FAILED

ID: AUTHENTICATION-306

Level: INFO

Description: Change user password failed

Data: error message, authentication type, user name

Triggers: Change user password in authentication screen due to directory server password policy.

Actions: Enter password which meets directory server password policy

CHANGE_USER_PASSWORD_SUCCEEDED

ID: AUTHENTICATION-307

Level: INFO

Description: Changing user password succeeded

Data: message

Triggers: Change user password in authentication screen due to directory server password policy.

CREATE_USER_PROFILE_FAILED

ID: AUTHENTICATION-308

Level: INFO

Description: Create user password failed

Data: error message, user name

Triggers: Create new user in Membership module

Actions: Make sure password entered meets directory server password policy

OpenAM logs the following AMCLI messages.

ATTEMPT_LOGIN

ID: AMCLI-1

Level: INFO

Description: Attempt to login to execute the commandline.

Data: user ID

Triggers: Run the Commandline tool.

SUCCEED_LOGIN

ID: AMCLI-2

Level: INFO

Description: Login to execute the commandline.

Data: user ID

Triggers: Run the Commandline tool.

FAILED_LOGIN

ID: AMCLI-3

Level: INFO

Description: Failed to login.

Data: user ID, error message

Triggers: Run the Commandline tool.

Actions: Check your user ID and password.; Look under debug file for more information.

ATTEMPT_LOAD_SCHEMA

ID: AMCLI-20

Level: INFO

Description: Attempt to load schema to data store.

Data: XML file name

Triggers: Load Schema through Commandline interface.

SUCCESS_LOAD_SCHEMA

ID: AMCLI-21

Level: INFO

Description: Schema is loaded to data store.

Data: XML file name

Triggers: Load Schema through Commandline interface.

FAILED_LOAD_SCHEMA

ID: AMCLI-22

Level: SEVERE

Description: Schema is not loaded to data store.

Data: XML file name, error message

Triggers: Load Schema through Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_SERVICE

ID: AMCLI-30

Level: INFO

Description: Attempt to delete service from data store.

Data: service name

Triggers: Delete Service through Commandline interface.

SUCCESS_DELETE_SERVICE

ID: AMCLI-31

Level: INFO

Description: Deleted service from data store.

Data: service name

Triggers: Delete Service through Commandline interface.

FAILED_DELETE_SERVICE

ID: AMCLI-32

Level: SEVERE

Description: Schema is not loaded to data store.

Data: service name, error message

Triggers: Delete Service Schema through Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_ATTRIBUTE_SCHEMA

ID: AMCLI-40

Level: INFO

Description: Attempt to attribute schema to an existing service.

Data: service name, schema type, XML file name

Triggers: Add attribute schema through Commandline interface.

SUCCESS_ADD_ATTRIBUTE_SCHEMA

ID: AMCLI-41

Level: INFO

Description: Added attribute schema to existing service.

Data: service name, schema type, XML file name

Triggers: Add attribute schema through Commandline interface.

FAILED_ADD_ATTRIBUTE_SCHEMA

ID: AMCLI-42

Level: SEVERE

Description: Attribute schema is not added to existing service.

Data: service name, schema type, XML file name, error message

Triggers: Add attribute schema through Commandline interface.

Actions: Check the service name, schema type and XML file.; Look under debug file for more information.

ATTEMPT_ADD_RESOURCE_BUNDLE

ID: AMCLI-50

Level: INFO

Description: Attempt to add resource bundle to data store.

Data: resource bundle name, file name, locale

Triggers: Add Resource Bundle through Commandline interface.

SUCCEED_ADD_RESOURCE_BUNDLE

ID: AMCLI-51

Level: INFO

Description: Resource bundle is added to data store.

Data: resource bundle name, file name, locale

Triggers: Add Resource Bundle through Commandline interface.

FAILED_ADD_RESOURCE_BUNDLE

ID: AMCLI-52

Level: SEVERE

Description: Failed to add resource bundle to data store.

Data: resource bundle name, file name, locale, error message

Triggers: SDK for adding resource bundle failed.

Actions: Look under debug file for more information.

ATTEMPT_GET_RESOURCE_BUNDLE

ID: AMCLI-60

Level: INFO

Description: Attempt to get resource bundle from data store.

Data: resource bundle name, locale

Triggers: Get Resource Bundle through Commandline interface.

SUCCEED_GET_RESOURCE_BUNDLE

ID: AMCLI-61

Level: INFO

Description: Resource bundle retrieved from data store.

Data: resource bundle name, locale

Triggers: Get Resource Bundle through Commandline interface.

FAILED_GET_RESOURCE_BUNDLE

ID: AMCLI-62

Level: SEVERE

Description: Failed to get resource bundle from data store.

Data: resource bundle name, locale, error message

Triggers: SDK for getting resource bundle failed.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_RESOURCE_BUNDLE

ID: AMCLI-70

Level: INFO

Description: Attempt to delete resource bundle from data store.

Data: resource bundle name, locale

Triggers: Delete Resource Bundle through Commandline interface.

SUCCEED_DELETE_RESOURCE_BUNDLE

ID: AMCLI-71

Level: INFO

Description: Resource bundle deleted from data store.

Data: resource bundle name, locale

Triggers: Delete Resource Bundle through Commandline interface.

FAILED_DELETE_RESOURCE_BUNDLE

ID: AMCLI-72

Level: SEVERE

Description: Failed to delete resource bundle from data store.

Data: resource bundle name, locale, error message

Triggers: SDK for deleting resource bundle failed.

Actions: Look under debug file for more information.

ATTEMPT_SESSION_DESTROY

ID: AMCLI-100

Level: INFO

Description: Attempt to destroy Session destroyed

Data: name of user

Triggers: Administrator invalidates session via Commandline interface.

SUCCEED_SESSION_DESTROY

ID: AMCLI-101

Level: INFO

Description: Session destroyed

Data: name of user

Triggers: Administrator invalidates session via Commandline interface.

FAILED_SESSION_DESTROY

ID: AMCLI-102

Level: SEVERE

Description: Failed to destroy session

Data: name of user, error message

Triggers: Session cannot be destroyed.

Actions: Look under debug file for more information.

ATTEMPT_MIGRATION_ENTRY

ID: AMCLI-1000

Level: INFO

Description: Attempt to migration organization to realm/

Data: distinguished name of organization

Triggers: Migration Commandline interface.

SUCCEED_MIGRATION_ENTRY

ID: AMCLI-1001

Level: INFO

Description: Migration completed.

Data: distinguished name of organization

Triggers: Migration Commandline interface.

ATTEMPT_DELETE_REALM

ID: AMCLI-2000

Level: INFO

Description: Attempt to delete realm/

Data: name of realm, recursive

Triggers: Delete realm command through Commandline interface.

SUCCEED_DELETE_REALM

ID: AMCLI-2001

Level: INFO

Description: Realm deleted.

Data: name of realm, recursive

Triggers: Delete realm command through Commandline interface.

FAILED_DELETE_REALM

ID: AMCLI-2002

Level: INFO

Description: Failed to delete realm.

Data: name of realm, recursive, error message

Triggers: Delete realm command through Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_REALM

ID: AMCLI-2010

Level: INFO

Description: Attempt to create realm/

Data: name of realm

Triggers: Create realm command through Commandline interface.

SUCCEED_CREATE_REALM

ID: AMCLI-2011

Level: INFO

Description: Realm created.

Data: name of realm

Triggers: Create realm command through Commandline interface.

FAILED_CREATE_REALM

ID: AMCLI-2012

Level: INFO

Description: Failed to create realm.

Data: name of realm, error message

Triggers: Create realm command through Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SEARCH_REALM

ID: AMCLI-3020

Level: INFO

Description: Attempt to search for realms by name.

Data: name of realm, search pattern, recursive

Triggers: Search realms command through Commandline interface.

SUCCEED_SEARCH_REALM

ID: AMCLI-3021

Level: INFO

Description: Completed searching for realms.

Data: name of realm, search pattern, recursive

Triggers: Search realms command through Commandline interface.

FAILED_SEARCH_REALM

ID: AMCLI-3022

Level: INFO

Description: Search for realms failed.

Data: name of realm, search pattern, recursive, error message

Triggers: Search realms command through Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ASSIGNABLE_SERVICES_OF_REALM

ID: AMCLI-2020

Level: INFO

Description: Attempt to get assignable services of realm.

Data: name of realm

Triggers: Execute get assignable services of realm Commandline interface.

SUCCEED_GET_ASSIGNABLE_SERVICES_OF_REALM

ID: AMCLI-2021

Level: INFO

Description: Assignable services command is serviced.

Data: name of realm

Triggers: Execute get assignable services of realm Commandline interface.

FAILED_GET_ASSIGNABLE_SERVICES_OF_REALM

ID: AMCLI-2022

Level: INFO

Description: Unable to get assignable services of realm.

Data: name of realm, error message

Triggers: Execute get assignable services of realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ASSIGNED_SERVICES_OF_REALM

ID: AMCLI-2030

Level: INFO

Description: Attempt to get services assigned to a realm.

Data: name of realm, include mandatory services

Triggers: Execute get services assigned to realm Commandline interface.

SUCCEED_GET_ASSIGNED_SERVICES_OF_REALM

ID: AMCLI-2031

Level: INFO

Description: Assignable services command is serviced.

Data: name of realm, include mandatory services

Triggers: Execute get services assigned to realm Commandline interface.

FAILED_GET_ASSIGNED_SERVICES_OF_REALM

ID: AMCLI-2032

Level: INFO

Description: Unable to get services assigned to realm.

Data: name of realm, include mandatory services, error message

Triggers: Execute get services assigned to realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ASSIGN_SERVICE_TO_REALM

ID: AMCLI-2040

Level: INFO

Description: Attempt to assign service to a realm.

Data: name of realm, name of service

Triggers: Execute assign service to realm Commandline interface.

SUCCEED_ASSIGN_SERVICE_TO_REALM

ID: AMCLI-2041

Level: INFO

Description: Service is assigned to realm.

Data: name of realm, name of service

Triggers: Execute assign service to realm Commandline interface.

FAILED_ASSIGN_SERVICE_TO_REALM

ID: AMCLI-2042

Level: INFO

Description: Unable to assign service to realm.

Data: name of realm, name of service, error message

Triggers: Execute assign service to realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UNASSIGN_SERVICE_FROM_REALM

ID: AMCLI-2050

Level: INFO

Description: Attempt to unassign service from a realm.

Data: name of realm, name of service

Triggers: Execute unassign service from realm Commandline interface.

SUCCEED_UNASSIGN_SERVICE_FROM_REALM

ID: AMCLI-2051

Level: INFO

Description: Service is unassigned from realm.

Data: name of realm, name of service

Triggers: Execute unassign service from realm Commandline interface.

FAILED_UNASSIGN_SERVICE_FROM_REALM

ID: AMCLI-2052

Level: INFO

Description: Unable to unassign service from realm.

Data: name of realm, name of service, error message

Triggers: Execute unassign service from realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_REALM_SERVICE_ATTR_VALUES

ID: AMCLI-2060

Level: INFO

Description: Attempt to get service attribute values from a realm.

Data: name of realm, name of service

Triggers: Execute get service attribute values from realm Commandline interface.

SUCCEED_GET_REALM_SERVICE_ATTR_VALUES

ID: AMCLI-2061

Level: INFO

Description: Service attribute values of realm is returneed.

Data: name of realm, name of service

Triggers: Execute get service attribute values from realm Commandline interface.

FAILED_GET_REALM_SERVICE_ATTR_VALUES

ID: AMCLI-2062

Level: INFO

Description: Unable to get service attribute values of realm.

Data: name of realm, name of service, error message

Triggers: Execute get service attribute values from realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_REALM_ATTRIBUTE

ID: AMCLI-2070

Level: INFO

Description: Attempt to remove attribute from a realm.

Data: name of realm, name of service, name of attribute

Triggers: Execute remove attribute from realm Commandline interface.

SUCCEED_REMOVE_REALM_ATTRIBUTE

ID: AMCLI-2071

Level: INFO

Description: Attribute of realm is removed.

Data: name of realm, name of service, name of attribute

Triggers: Execute remove attribute from realm Commandline interface.

FAILED_REMOVE_REALM_ATTRIBUTE

ID: AMCLI-2072

Level: INFO

Description: Unable to remove attribute from realm.

Data: name of realm, name of service, name of attribute, error message

Triggers: Execute remove attribute from realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_SERVICE_REALM

ID: AMCLI-2080

Level: INFO

Description: Attempt to modify service of realm.

Data: name of realm, name of service

Triggers: Execute modify service of realm Commandline interface.

SUCCEED_MODIFY_SERVICE_REALM

ID: AMCLI-2081

Level: INFO

Description: Attribute of realm is modified.

Data: name of realm, name of service

Triggers: Execute modify service of realm Commandline interface.

FAILED_MODIFY_SERVICE_REALM

ID: AMCLI-2082

Level: INFO

Description: Unable to modify service of realm.

Data: name of realm, name of service, error message

Triggers: Execute modify service of realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_ATTR_VALUES_REALM

ID: AMCLI-2090

Level: INFO

Description: Attempt to add attribute value to realm.

Data: name of realm, name of service, name of attribute

Triggers: Execute add attribute values to realm Commandline interface.

SUCCEED_ADD_ATTR_VALUES_REALM

ID: AMCLI-2091

Level: INFO

Description: Attribute values is added to realm.

Data: name of realm, name of service, name of attribute

Triggers: Execute add attribute values to realm Commandline interface.

FAILED_ADD_ATTR_VALUES_REALM

ID: AMCLI-2092

Level: INFO

Description: Unable to add attribute values to realm.

Data: name of realm, name of service, name of attribute, error message

Triggers: Execute add attribute values to realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_ATTR_VALUES_REALM

ID: AMCLI-2100

Level: INFO

Description: Attempt to set attribute value to realm.

Data: name of realm, name of service

Triggers: Execute set attribute values to realm Commandline interface.

SUCCEED_SET_ATTR_VALUES_REALM

ID: AMCLI-2101

Level: INFO

Description: Attribute values is set to realm.

Data: name of realm, name of service

Triggers: Execute set attribute values to realm Commandline interface.

FAILED_SET_ATTR_VALUES_REALM

ID: AMCLI-2102

Level: INFO

Description: Unable to set attribute values to realm.

Data: name of realm, name of service, error message

Triggers: Execute set attribute values to realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2110

Level: INFO

Description: Attempt to remove schema attribute defaults.

Data: name of service, schema type, name of sub schema, name of attribute

Triggers: Execute remove schema attribute defaults Commandline interface.

SUCCEED_REMOVE_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2111

Level: INFO

Description: Schema attribute defaults is removed.

Data: name of service, schema type, name of sub schema, name of attribute

Triggers: Execute remove schema attribute defaults Commandline interface.

FAILED_REMOVE_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2112

Level: INFO

Description: Unable to remove schema attribute defaults.

Data: name of service, schema type, name of sub schema, name of attribute, error message

Triggers: Execute remove schema attribute defaults Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2120

Level: INFO

Description: Attempt to add schema attribute defaults.

Data: name of service, schema type, name of sub schema, name of attribute

Triggers: Execute add schema attribute defaults Commandline interface.

SUCCEED_ADD_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2121

Level: INFO

Description: Schema attribute defaults is added.

Data: name of service, schema type, name of sub schema, name of attribute

Triggers: Execute add schema attribute defaults Commandline interface.

FAILED_ADD_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2122

Level: INFO

Description: Unable to add schema attribute defaults.

Data: name of service, schema type, name of sub schema, name of attribute, error message

Triggers: Execute add schema attribute defaults Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2130

Level: INFO

Description: Attempt to get schema attribute defaults.

Data: name of service, schema type, name of sub schema

Triggers: Execute get schema attribute defaults Commandline interface.

SUCCEED_GET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2131

Level: INFO

Description: Schema attribute defaults is returned.

Data: name of service, schema type, name of sub schema

Triggers: Execute get schema attribute defaults Commandline interface.

FAILED_GET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2132

Level: INFO

Description: Unable to get schema attribute defaults.

Data: name of service, schema type, name of sub schema, error message

Triggers: Execute get schema attribute defaults Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2140

Level: INFO

Description: Attempt to set schema attribute defaults.

Data: name of service, schema type, name of sub schema

Triggers: Execute set schema attribute defaults Commandline interface.

SUCCEED_SET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2141

Level: INFO

Description: Schema attribute defaults is set.

Data: name of service, schema type, name of sub schema

Triggers: Execute set schema attribute defaults Commandline interface.

FAILED_SET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2142

Level: INFO

Description: Unable to set schema attribute defaults.

Data: name of service, schema type, name of sub schema, error message

Triggers: Execute set schema attribute defaults Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2150

Level: INFO

Description: Attempt to add choice value to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute add attribute schema choice values Commandline interface.

SUCCEED_ADD_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2151

Level: INFO

Description: Choice values are added.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute add attribute schema choice values Commandline interface.

FAILED_ADD_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2152

Level: INFO

Description: Unable to add choice value to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema, error message

Triggers: Execute add attribute schema choice values Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2155

Level: INFO

Description: Attempt to get choice value to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute get attribute schema choice values Commandline interface.

SUCCEED_GET_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2156

Level: INFO

Description: Choice values are listed.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute get attribute schema choice values Commandline interface.

FAILED_GET_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2157

Level: INFO

Description: Unable to get choice value to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema, error message

Triggers: Execute get attribute schema choice values Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_ATTRIBUTE_SCHEMA_CHOICE_VALUE

ID: AMCLI-2160

Level: INFO

Description: Attempt to remove choice value from attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute remove attribute schema choice values Commandline interface.

SUCCEED_REMOVE_ATTRIBUTE_SCHEMA_CHOICE_VALUE

ID: AMCLI-2161

Level: INFO

Description: Choice value is removed.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute remove attribute schema choice values Commandline interface.

FAILED_REMOVE_ATTRIBUTE_SCHEMA_CHOICE_VALUE

ID: AMCLI-2162

Level: INFO

Description: Unable to remove choice value to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema, error message

Triggers: Execute remove attribute schema choice values Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_TYPE

ID: AMCLI-2170

Level: INFO

Description: Attempt to modify attribute schema type.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema type

Triggers: Execute modify attribute schema type Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_TYPE

ID: AMCLI-2171

Level: INFO

Description: Attribute schema type is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema type

Triggers: Execute modify attribute schema type Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_TYPE

ID: AMCLI-2172

Level: INFO

Description: Unable to modify attribute schema type.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema type, error message

Triggers: Execute modify attribute schema type Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_UI_TYPE

ID: AMCLI-2180

Level: INFO

Description: Attempt to modify attribute schema UI type.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema UI type

Triggers: Execute modify attribute schema UI type Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_UI_TYPE

ID: AMCLI-2181

Level: INFO

Description: Attribute schema UI type is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema UI type

Triggers: Execute modify attribute schema UI type Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_UI_TYPE

ID: AMCLI-2182

Level: INFO

Description: Unable to modify attribute schema UI type.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema UI type, error message

Triggers: Execute modify attribute schema UI type Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_SYNTAX

ID: AMCLI-2190

Level: INFO

Description: Attempt to modify attribute schema syntax.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema syntax

Triggers: Execute modify attribute schema syntax Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_SYNTAX

ID: AMCLI-2191

Level: INFO

Description: Attribute schema syntax is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema syntax

Triggers: Execute modify attribute schema syntax Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_SYNTAX

ID: AMCLI-2192

Level: INFO

Description: Unable to modify attribute schema syntax.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema syntax, error message

Triggers: Execute modify attribute schema syntax Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_I18N_KEY

ID: AMCLI-2200

Level: INFO

Description: Attempt to modify attribute schema i18n Key.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema i18n Key

Triggers: Execute modify attribute schema i18n Key Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_I18N_KEY

ID: AMCLI-2201

Level: INFO

Description: Attribute schema i18n Key is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema i18n Key

Triggers: Execute modify attribute schema i18n Key Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_I18N_KEY

ID: AMCLI-2202

Level: INFO

Description: Unable to modify attribute schema i18n Key.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema i18n Key, error message

Triggers: Execute modify attribute schema i18n Key Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2210

Level: INFO

Description: Attempt to modify attribute schema properties view bean URL.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema properties view bean URL

Triggers: Execute modify attribute schema properties view bean URL Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2211

Level: INFO

Description: Attribute schema properties view bean URL is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema properties view bean URL

Triggers: Execute modify attribute schema properties view bean URL Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2212

Level: INFO

Description: Unable to modify attribute schema properties view bean URL.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema properties view bean URL, error message

Triggers: Execute modify attribute schema properties view bean URL Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_ANY

ID: AMCLI-2220

Level: INFO

Description: Attempt to modify attribute schema any value.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema any

Triggers: Execute modify attribute schema any Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_ANY

ID: AMCLI-2221

Level: INFO

Description: Attribute schema any value is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema any

Triggers: Execute modify attribute schema any Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_ANY

ID: AMCLI-2222

Level: INFO

Description: Unable to modify attribute schema any value.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema any, error message

Triggers: Execute modify attribute schema any Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_ATTRIBUTE_SCHEMA_DEFAULT_VALUE

ID: AMCLI-2230

Level: INFO

Description: Attempt to remove attribute schema default value.

Data: name of service, schema type, name of sub schema, name of attribute schema, default value to be removed

Triggers: Execute remove attribute schema default values Commandline interface.

SUCCEED_REMOVE_ATTRIBUTE_SCHEMA_DEFAULT_VALUE

ID: AMCLI-2231

Level: INFO

Description: Attribute schema default value is removed.

Data: name of service, schema type, name of sub schema, name of attribute schema, default value to be removed

Triggers: Execute remove attribute schema default values Commandline interface.

FAILED_REMOVE_ATTRIBUTE_SCHEMA_DEFAULT_VALUE

ID: AMCLI-2232

Level: INFO

Description: Unable to remove attribute schema default value.

Data: name of service, schema type, name of sub schema, name of attribute schema, default value to be removed, error message

Triggers: Execute remove attribute schema default values Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_ATTRIBUTE_SCHEMA_VALIDATOR

ID: AMCLI-2240

Level: INFO

Description: Attempt to set attribute schema validator.

Data: name of service, schema type, name of sub schema, name of attribute schema, validator

Triggers: Execute set attribute schema validator Commandline interface.

SUCCEED_SET_ATTRIBUTE_SCHEMA_VALIDATOR

ID: AMCLI-2241

Level: INFO

Description: Attribute schema validator is set.

Data: name of service, schema type, name of sub schema, name of attribute schema, validator

Triggers: Execute set attribute schema validator Commandline interface.

FAILED_SET_ATTRIBUTE_SCHEMA_VALIDATOR

ID: AMCLI-2242

Level: INFO

Description: Unable to set attribute schema validator.

Data: name of service, schema type, name of sub schema, name of attribute schema, validator, error message

Triggers: Execute set attribute schema validator Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_ATTRIBUTE_SCHEMA_START_RANGE

ID: AMCLI-2250

Level: INFO

Description: Attempt to set attribute schema start range.

Data: name of service, schema type, name of sub schema, name of attribute schema, start range

Triggers: Execute set attribute schema start range Commandline interface.

SUCCEED_SET_ATTRIBUTE_SCHEMA_START_RANGE

ID: AMCLI-2251

Level: INFO

Description: Attribute schema start range is set.

Data: name of service, schema type, name of sub schema, name of attribute schema, start range

Triggers: Execute set attribute schema start range Commandline interface.

FAILED_SET_ATTRIBUTE_SCHEMA_START_RANGE

ID: AMCLI-2252

Level: INFO

Description: Unable to set attribute schema start range.

Data: name of service, schema type, name of sub schema, name of attribute schema, start range, error message

Triggers: Execute set attribute schema start range Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_ATTRIBUTE_SCHEMA_END_RANGE

ID: AMCLI-2250

Level: INFO

Description: Attempt to set attribute schema end range.

Data: name of service, schema type, name of sub schema, name of attribute schema, end range

Triggers: Execute set attribute schema end range Commandline interface.

SUCCEED_SET_ATTRIBUTE_SCHEMA_END_RANGE

ID: AMCLI-2251

Level: INFO

Description: Attribute schema end range is set.

Data: name of service, schema type, name of sub schema, name of attribute schema, end range

Triggers: Execute set attribute schema end range Commandline interface.

FAILED_SET_ATTRIBUTE_SCHEMA_END_RANGE

ID: AMCLI-2252

Level: INFO

Description: Unable to set attribute schema end range.

Data: name of service, schema type, name of sub schema, name of attribute schema, end range, error message

Triggers: Execute set attribute schema end range Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SERVICE_SCHEMA_I18N_KEY

ID: AMCLI-2260

Level: INFO

Description: Attempt to set service schema i18n key.

Data: name of service, i18n key

Triggers: Execute set service schema i18n key Commandline interface.

SUCCEED_SET_SERVICE_SCHEMA_I18N_KEY

ID: AMCLI-2261

Level: INFO

Description: Service schema i18n key is set.

Data: name of service, i18n key

Triggers: Execute set service schema i18n key Commandline interface.

FAILED_SET_SERVICE_SCHEMA_I18N_KEY

ID: AMCLI-2262

Level: INFO

Description: Unable to set service schema i18n key.

Data: name of service, i18n key, error message

Triggers: Execute set service schema i18n key Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SERVICE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2270

Level: INFO

Description: Attempt to set service schema properties view bean URL.

Data: name of service, properties view bean URL

Triggers: Execute set service schema properties view bean URL Commandline interface.

SUCCEED_SET_SERVICE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2271

Level: INFO

Description: Service schema properties view bean URL is set.

Data: name of service, properties view bean URL

Triggers: Execute set service schema properties view bean URL Commandline interface.

FAILED_SET_SERVICE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2272

Level: INFO

Description: Unable to set service schema properties view bean URL.

Data: name of service, properties view bean URL, error message

Triggers: Execute set service schema properties view bean URL Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SERVICE_REVISION_NUMBER

ID: AMCLI-2280

Level: INFO

Description: Attempt to set service revision number.

Data: name of service, revision number

Triggers: Execute set service revision number Commandline interface.

SUCCEED_SET_SERVICE_REVISION_NUMBER

ID: AMCLI-2281

Level: INFO

Description: Service revision number is set.

Data: name of service, revision number

Triggers: Execute set service revision number Commandline interface.

FAILED_SET_SERVICE_REVISION_NUMBER

ID: AMCLI-2282

Level: INFO

Description: Unable to set service revision number.

Data: name of service, revision number, error message

Triggers: Execute set service revision number Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SERVICE_REVISION_NUMBER

ID: AMCLI-2290

Level: INFO

Description: Attempt to get service revision number.

Data: name of service

Triggers: Execute get service revision number Commandline interface.

SUCCEED_GET_SERVICE_REVISION_NUMBER

ID: AMCLI-2291

Level: INFO

Description: Service revision number is returned.

Data: name of service

Triggers: Execute get service revision number Commandline interface.

FAILED_GET_SERVICE_REVISION_NUMBER

ID: AMCLI-2292

Level: INFO

Description: Unable to get service revision number.

Data: name of service, error message

Triggers: Execute get service revision number Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_ATTRIBUTE_SCHEMA

ID: AMCLI-2300

Level: INFO

Description: Attempt to remove attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute remove attribute schema Commandline interface.

SUCCEED_REMOVE_ATTRIBUTE_SCHEMA

ID: AMCLI-2301

Level: INFO

Description: Attribute schema is removed.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute remove attribute schema Commandline interface.

FAILED_REMOVE_ATTRIBUTE_SCHEMA

ID: AMCLI-2302

Level: INFO

Description: Unable to remove attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema, error message

Triggers: Execute remove attribute schema Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SUB_CONFIGURATION

ID: AMCLI-2310

Level: INFO

Description: Attempt to add sub configuration.

Data: name of sub configuration, name of service

Triggers: Execute add sub configuration Commandline interface.

SUCCEED_ADD_SUB_CONFIGURATION

ID: AMCLI-2311

Level: INFO

Description: Sub configuration is added.

Data: name of sub configuration, name of service

Triggers: Execute add sub configuration Commandline interface.

FAILED_ADD_SUB_CONFIGURATION

ID: AMCLI-2312

Level: INFO

Description: Unable to add sub configuration.

Data: name of sub configuration, name of service, error message

Triggers: Execute add sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SUB_CONFIGURATION_TO_REALM

ID: AMCLI-2320

Level: INFO

Description: Attempt to add sub configuration to realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute add sub configuration Commandline interface.

SUCCEED_ADD_SUB_CONFIGURATION_TO_REALM

ID: AMCLI-2321

Level: INFO

Description: Sub configuration is added to realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute add sub configuration Commandline interface.

FAILED_ADD_SUB_CONFIGURATION_TO_REALM

ID: AMCLI-2322

Level: INFO

Description: Unable to add sub configuration.

Data: name of realm, name of sub configuration, name of service, error message

Triggers: Execute add sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_SUB_CONFIGURATION

ID: AMCLI-2330

Level: INFO

Description: Attempt to delete sub configuration.

Data: name of sub configuration, name of service

Triggers: Execute delete sub configuration Commandline interface.

SUCCEED_DELETE_SUB_CONFIGURATION

ID: AMCLI-2331

Level: INFO

Description: Sub configuration is deleted.

Data: name of sub configuration, name of service

Triggers: Execute delete sub configuration Commandline interface.

FAILED_ADELETE_SUB_CONFIGURATION

ID: AMCLI-2332

Level: INFO

Description: Unable to delete sub configuration.

Data: name of sub configuration, name of service, error message

Triggers: Execute delete sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_SUB_CONFIGURATION_TO_REALM

ID: AMCLI-2340

Level: INFO

Description: Attempt to delete sub configuration from realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute delete sub configuration Commandline interface.

SUCCEED_DELETE_SUB_CONFIGURATION_TO_REALM

ID: AMCLI-2341

Level: INFO

Description: Sub configuration is deleted from realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute delete sub configuration Commandline interface.

FAILED_DELETE_SUB_CONFIGURATIONT_TO_REALM

ID: AMCLI-2342

Level: INFO

Description: Unable to delete sub configuration.

Data: name of realm, name of sub configuration, name of service, error message

Triggers: Execute delete sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SUB_SCHEMA

ID: AMCLI-2350

Level: INFO

Description: Attempt to add sub schema.

Data: name of service, schema type, name of sub schema

Triggers: Execute add sub schema Commandline interface.

SUCCEED_ADD_SUB_SCHEMA

ID: AMCLI-2351

Level: INFO

Description: Sub schema is added.

Data: name of service, schema type, name of sub schema

Triggers: Execute add sub schema Commandline interface.

FAILED_ADD_SUB_SCHEMA

ID: AMCLI-2352

Level: INFO

Description: Unable to add sub schema.

Data: name of service, schema type, name of sub schema, error message

Triggers: Execute add sub schema configurations Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_SUB_SCHEMA

ID: AMCLI-2360

Level: INFO

Description: Attempt to remove sub schema.

Data: name of service, schema type, name of parent sub schema, name of sub schema

Triggers: Execute remove sub schema Commandline interface.

SUCCEED_REMOVE_SUB_SCHEMA

ID: AMCLI-2361

Level: INFO

Description: Sub schema is removed.

Data: name of service, schema type, name of parent sub schema, name of sub schema

Triggers: Execute remove sub schema Commandline interface.

FAILED_REMOVE_SUB_SCHEMA

ID: AMCLI-2362

Level: INFO

Description: Unable to remove sub schema.

Data: name of service, schema type, name of parent sub schema, name of sub schema, error message

Triggers: Execute remove sub schema configurations Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_INHERITANCE_SUB_SCHEMA

ID: AMCLI-2370

Level: INFO

Description: Attempt to modify inheritance of sub schema.

Data: name of service, schema type, name of sub schema

Triggers: Execute modify inheritance of sub schema Commandline interface.

SUCCEED_MODIFY_INHERITANCE_SUB_SCHEMA

ID: AMCLI-2371

Level: INFO

Description: Sub schema is modified.

Data: name of service, schema type, name of sub schema

Triggers: Execute modify inheritance of sub schema Commandline interface.

FAILED_MODIFY_INHERITANCE_SUB_SCHEMA

ID: AMCLI-2372

Level: INFO

Description: Unable to modify sub schema.

Data: name of service, schema type, name of sub schema, error message

Triggers: Execute modify inheritance of sub schema configurations Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_SUB_CONFIGURATION

ID: AMCLI-2380

Level: INFO

Description: Attempt to modify sub configuration.

Data: name of sub configuration, name of service

Triggers: Execute modify sub configuration Commandline interface.

SUCCEED_MODIFY_SUB_CONFIGURATION

ID: AMCLI-2381

Level: INFO

Description: Sub configuration is modified.

Data: name of sub configuration, name of service

Triggers: Execute modify sub configuration Commandline interface.

FAILED_MODIFY_SUB_CONFIGURATION

ID: AMCLI-2382

Level: INFO

Description: Unable to modify sub configuration.

Data: name of sub configuration, name of service, error message

Triggers: Execute modify sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SUB_CONFIGURATION

ID: AMCLI-2383

Level: INFO

Description: Attempt to retrieve sub configuration.

Data: name of sub configuration, name of service

Triggers: Execute get sub configuration Commandline interface.

SUCCEED_GET_SUB_CONFIGURATION

ID: AMCLI-2384

Level: INFO

Description: Sub configuration is retrieved.

Data: name of sub configuration, name of service

Triggers: Execute get sub configuration Commandline interface.

FAILED_GET_SUB_CONFIGURATION

ID: AMCLI-2385

Level: INFO

Description: Unable to retrieve sub configuration.

Data: name of sub configuration, name of service, error message

Triggers: Execute get sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2390

Level: INFO

Description: Attempt to modify sub configuration in realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute modify sub configuration Commandline interface.

SUCCEED_MODIFY_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2391

Level: INFO

Description: Sub configuration is modified.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute modify sub configuration Commandline interface.

FAILED_MODIFY_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2392

Level: INFO

Description: Unable to modify sub configuration in realm.

Data: name of realm, name of sub configuration, name of service, error message

Triggers: Execute modify sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2393

Level: INFO

Description: Attempt to retrieve sub configuration in realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute get sub configuration Commandline interface.

SUCCEED_GET_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2394

Level: INFO

Description: Sub configuration is retrieved.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute get sub configuration Commandline interface.

FAILED_GET_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2395

Level: INFO

Description: Unable to retrieve sub configuration in realm.

Data: name of realm, name of sub configuration, name of service, error message

Triggers: Execute get sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_PLUGIN_INTERFACE

ID: AMCLI-2400

Level: INFO

Description: Attempt to add Plug-in interface to service.

Data: name of service, name of plugin

Triggers: Execute add Plug-in interface Commandline interface.

SUCCEED_ADD_PLUGIN_INTERFACE

ID: AMCLI-2401

Level: INFO

Description: Plug-in interface is added.

Data: name of service, name of plugin

Triggers: Execute add Plug-in interface Commandline interface.

FAILED_ADD_PLUGIN_INTERFACE

ID: AMCLI-2402

Level: INFO

Description: Unable to add Plug-in interface to service.

Data: name of service, name of plugin, error message

Triggers: Execute add Plug-in interface Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_PLUGIN_SCHEMA_PROP_VIEWBEAN_URL

ID: AMCLI-2410

Level: INFO

Description: Attempt to set Plug-in schema's properties view bean.

Data: name of service, name of plugin

Triggers: Execute set Plug-in schema's properties view bean Commandline interface.

SUCCEED_SET_PLUGIN_SCHEMA_PROP_VIEWBEAN_URL

ID: AMCLI-2411

Level: INFO

Description: Plug-in schema's properties view bean is set.

Data: name of service, name of plugin

Triggers: Execute set Plug-in schema's properties view bean Commandline interface.

FAILED_SET_PLUGIN_SCHEMA_PROP_VIEWBEAN_URL

ID: AMCLI-2412

Level: INFO

Description: Unable to set Plug-in schema's properties view bean.

Data: name of service, name of plugin, error message

Triggers: Execute set Plug-in schema's properties view bean Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_POLICY_IN_REALM

ID: AMCLI-2420

Level: INFO

Description: Attempt to create policies under realm.

Data: name of realm

Triggers: Execute create policies under realm Commandline interface.

SUCCEED_CREATE_POLICY_IN_REALM

ID: AMCLI-2421

Level: INFO

Description: Policies are created.

Data: name of realm

Triggers: Execute create policies under realm Commandline interface.

FAILED_CREATE_POLICY_IN_REALM

ID: AMCLI-2422

Level: INFO

Description: Unable to create policies under realm.

Data: name of realm, error message

Triggers: Execute create policies under realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_POLICY_IN_REALM

ID: AMCLI-2430

Level: INFO

Description: Attempt to delete policy in realm.

Data: name of realm, name of policy

Triggers: Execute delete policy in realm Commandline interface.

SUCCEED_DELETE_POLICY_IN_REALM

ID: AMCLI-2431

Level: INFO

Description: Policy is deleted.

Data: name of realm, name of policy

Triggers: Execute delete policy in realm Commandline interface.

FAILED_DELETE_POLICY_IN_REALM

ID: AMCLI-2432

Level: INFO

Description: Unable to delete policy under realm.

Data: name of realm, name of policy, error message

Triggers: Execute delete policy under realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_TO_GET_POLICY_NAMES_IN_REALM

ID: AMCLI-2433

Level: INFO

Description: Attempt to get policy names in realm.

Data: name of realm

Triggers: Execute get policy names in realm Commandline interface.

GOT_POLICY_NAMES_IN_REALM

ID: AMCLI-2434

Level: INFO

Description: Got policy names in realm.

Data: name of realm

Triggers: Execute get policy names in realm Commandline interface.

FAILED_GET_POLICY_NAMES_IN_REALM

ID: AMCLI-2435

Level: INFO

Description: Unable to get policy names in realm.

Data: name of realm

Triggers: Execute get policy names in realm Commandline interface.

ATTEMPT_GET_POLICY_IN_REALM

ID: AMCLI-2440

Level: INFO

Description: Attempt to get policy definition in realm.

Data: name of realm, name of policy

Triggers: Execute get policy definition in realm Commandline interface.

SUCCEED_GET_POLICY_IN_REALM

ID: AMCLI-2441

Level: INFO

Description: Policy definition is returned.

Data: name of realm, name of policy

Triggers: Execute get policy definition in realm Commandline interface.

FAILED_GET_POLICY_IN_REALM

ID: AMCLI-2442

Level: INFO

Description: Unable to get policy definition under realm.

Data: name of realm, name of policy, error message

Triggers: Execute get policy definition under realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_IDENTITY

ID: AMCLI-2450

Level: INFO

Description: Attempt to create an identity in realm.

Data: name of realm, identity type, name of identity

Triggers: Execute create identity in realm Commandline interface.

SUCCEED_CREATE_IDENTITY

ID: AMCLI-2451

Level: INFO

Description: Identity is created.

Data: name of realm, identity type, name of identity

Triggers: Execute create identity in realm Commandline interface.

FAILED_CREATE_IDENTITY

ID: AMCLI-2452

Level: INFO

Description: Unable to create identity in realm.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute create identity in realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_IDENTITY

ID: AMCLI-2460

Level: INFO

Description: Attempt to delete an identity in realm.

Data: name of realm, identity type, name of identity

Triggers: Execute delete identity in realm Commandline interface.

SUCCEED_DELETE_IDENTITY

ID: AMCLI-2461

Level: INFO

Description: Identity is deleted.

Data: name of realm, identity type, name of identity

Triggers: Execute delete identity in realm Commandline interface.

FAILED_DELETE_IDENTITY

ID: AMCLI-2462

Level: INFO

Description: Unable to delete identity in realm.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute delete identity in realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SEARCH_IDENTITIES

ID: AMCLI-2470

Level: INFO

Description: Attempt to search identities in realm.

Data: name of realm, identity type, search pattern

Triggers: Execute search identities in realm Commandline interface.

SUCCEED_SEARCH_IDENTITIES

ID: AMCLI-2471

Level: INFO

Description: Search Result is returned.

Data: name of realm, identity type, search pattern

Triggers: Execute search identities in realm Commandline interface.

FAILED_SEARCH_IDENTITIES

ID: AMCLI-2472

Level: INFO

Description: Unable to search identities in realm.

Data: name of realm, identity type, search pattern, error message

Triggers: Execute search identities in realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ALLOWED_OPS

ID: AMCLI-2480

Level: INFO

Description: Attempt to get the allowed operation of an identity type in realm.

Data: name of realm, identity type

Triggers: Execute get the allowed operation of an identity type in realm Commandline interface.

SUCCEED_GET_ALLOWED_OPS

ID: AMCLI-2481

Level: INFO

Description: Allowed operations are returned.

Data: name of realm, identity type

Triggers: Execute get the allowed operation of an identity type in realm Commandline interface.

FAILED_GET_ALLOWED_OPS

ID: AMCLI-2482

Level: INFO

Description: Unable to get the allowed operation of an identity type in realm.

Data: name of realm, identity type, error message

Triggers: Execute get the allowed operation of an identity type in realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SUPPORTED_IDTYPES

ID: AMCLI-2490

Level: INFO

Description: Attempt to get the supported identity type in realm.

Data: name of realm

Triggers: Execute get the supported identity type in realm Commandline interface.

SUCCEED_GET_SUPPORTED_IDTYPES

ID: AMCLI-2491

Level: INFO

Description: Allowed identity types are returned.

Data: name of realm

Triggers: Execute get the supported identity type in realm Commandline interface.

FAILED_GET_SUPPORTED_IDTYPES

ID: AMCLI-2492

Level: INFO

Description: Unable to get the supported identity type in realm.

Data: name of realm, error message

Triggers: Execute get the supported identity type in realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ASSIGNABLE_SERVICES

ID: AMCLI-2500

Level: INFO

Description: Attempt to get the assignable services of an identity.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the assignable services of an identity Commandline interface.

SUCCEED_GET_ASSIGNABLE_SERVICES

ID: AMCLI-2501

Level: INFO

Description: Assignable services are returned.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the assignable services of an identity Commandline interface.

FAILED_GET_ASSIGNABLE_SERVICES

ID: AMCLI-2502

Level: INFO

Description: Unable to get the assignable services of an identity.

Data: name of realm, name of identity type, name of identity, error message

Triggers: Execute get the assignable services of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ASSIGNED_SERVICES

ID: AMCLI-2510

Level: INFO

Description: Attempt to get the assigned services of an identity.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the assigned services of an identity Commandline interface.

SUCCEED_GET_ASSIGNED_SERVICES

ID: AMCLI-2511

Level: INFO

Description: Assigned services are returned.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the assigned services of an identity Commandline interface.

FAILED_GET_ASSIGNED_SERVICES

ID: AMCLI-2512

Level: INFO

Description: Unable to get the assigned services of an identity.

Data: name of realm, name of identity type, name of identity, error message

Triggers: Execute get the assigned services of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_GET_SERVICE_ATTRIBUTES

ID: AMCLI-2520

Level: INFO

Description: Attempt to get service attribute values of an identity.

Data: name of realm, name of identity type, name of identity, name of service

Triggers: Execute get the service attribute values of an identity Commandline interface.

SUCCEED_IDREPO_GET_SERVICE_ATTRIBUTES

ID: AMCLI-2521

Level: INFO

Description: Service attribute values are returned.

Data: name of realm, name of identity type, name of identity, name of service

Triggers: Execute get the service attribute values of an identity Commandline interface.

FAILED_IDREPO_GET_SERVICE_ATTRIBUTES

ID: AMCLI-2522

Level: INFO

Description: Unable to get the service attribute values of an identity.

Data: name of realm, name of identity type, name of identity, name of service, error message

Triggers: Execute get the service attribute values of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_GET_ATTRIBUTES

ID: AMCLI-2530

Level: INFO

Description: Attempt to get attribute values of an identity.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the attribute values of an identity Commandline interface.

SUCCEED_IDREPO_GET_ATTRIBUTES

ID: AMCLI-2531

Level: INFO

Description: Attribute values are returned.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the attribute values of an identity Commandline interface.

FAILED_IDREPO_GET_ATTRIBUTES

ID: AMCLI-2532

Level: INFO

Description: Unable to get the attribute values of an identity.

Data: name of realm, name of identity type, name of identity, error message

Triggers: Execute get the attribute values of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_GET_MEMBERSHIPS

ID: AMCLI-2540

Level: INFO

Description: Attempt to get memberships of an identity.

Data: name of realm, name of identity type, name of identity, name of membership identity type

Triggers: Execute get the memberships of an identity Commandline interface.

SUCCEED_IDREPO_GET_MEMBERSHIPS

ID: AMCLI-2541

Level: INFO

Description: Memberships are returned.

Data: name of realm, name of identity type, name of identity, name of membership identity type

Triggers: Execute get the memberships of an identity Commandline interface.

FAILED_IDREPO_GET_MEMBERSHIPS

ID: AMCLI-2542

Level: INFO

Description: Unable to get the memberships of an identity.

Data: name of realm, name of identity type, name of identity, name of membership identity type, error message

Triggers: Execute get the memberships of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_GET_MEMBERS

ID: AMCLI-2550

Level: INFO

Description: Attempt to get members of an identity.

Data: name of realm, name of identity type, name of identity, name of membership identity type

Triggers: Execute get the members of an identity Commandline interface.

SUCCEED_IDREPO_GET_MEMBERS

ID: AMCLI-2551

Level: INFO

Description: Members are returned.

Data: name of realm, name of identity type, name of identity, name of membership identity type

Triggers: Execute get the members of an identity Commandline interface.

FAILED_IDREPO_GET_MEMBERS

ID: AMCLI-2552

Level: INFO

Description: Unable to get the members of an identity.

Data: name of realm, name of identity type, name of identity, name of membership identity type, error message

Triggers: Execute get the members of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_IS_MEMBER

ID: AMCLI-2560

Level: INFO

Description: Attempt to determine if an identity is a member of another identity.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute determine if an identity is a member of another identity Commandline interface.

SUCCEED_IDREPO_IS_MEMBER

ID: AMCLI-2561

Level: INFO

Description: Membership is determined.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute determine if an identity is a member of another identity Commandline interface.

FAILED_IDREPO_IS_MEMBER

ID: AMCLI-2562

Level: INFO

Description: Unable to determine the membership of an identity of another.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity, error message

Triggers: Execute determine if an identity is a member of another identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_IS_ACTIVE

ID: AMCLI-2570

Level: INFO

Description: Attempt to determine if an identity is active.

Data: name of realm, name of identity type, name of identity

Triggers: Execute determine if an identity is active Commandline interface.

SUCCEED_IDREPO_IS_ACTIVE

ID: AMCLI-2571

Level: INFO

Description: Active status of identity is determined.

Data: name of realm, name of identity type, name of identity

Triggers: Execute determine if an identity is active Commandline interface.

FAILED_IDREPO_IS_ACTIVE

ID: AMCLI-2572

Level: INFO

Description: Unable to determine if an identity is active.

Data: name of realm, name of identity type, name of identity, error message

Triggers: Execute determine if an identity is a active Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_ADD_MEMBER

ID: AMCLI-2580

Level: INFO

Description: Attempt to make an identity a member of another identity.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute make an identity a member of another identity Commandline interface.

SUCCEED_IDREPO_ADD_MEMBER

ID: AMCLI-2581

Level: INFO

Description: Membership is set.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute make an identity a member of another identity Commandline interface.

FAILED_IDREPO_ADD_MEMBER

ID: AMCLI-2582

Level: INFO

Description: Unable to add member of an identity to another.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity, error message

Triggers: Execute make an identity a member of another identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_REMOVE_MEMBER

ID: AMCLI-2590

Level: INFO

Description: Attempt to remove membership an identity from another identity.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute remove membership an identity from another identity Commandline interface.

SUCCEED_IDREPO_REMOVE_MEMBER

ID: AMCLI-2591

Level: INFO

Description: Membership is removed.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute remove membership an identity from another identity Commandline interface.

FAILED_IDREPO_REMOVE_MEMBER

ID: AMCLI-2592

Level: INFO

Description: Unable to remove membership of an identity.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity, error message

Triggers: Execute remove membership an identity from another identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_ASSIGN_SERVICE

ID: AMCLI-2600

Level: INFO

Description: Attempt to assign service to an identity.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute assign service to an identity Commandline interface.

SUCCEED_IDREPO_ASSIGN_SERVICE

ID: AMCLI-2601

Level: INFO

Description: Service is assigned to an identity.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute assign service to an identity Commandline interface.

FAILED_IDREPO_ASSIGN_SERVICE

ID: AMCLI-2602

Level: INFO

Description: Unable to assign service to an identity.

Data: name of realm, identity type, name of identity, name of service, error message

Triggers: Execute assign service to an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_UNASSIGN_SERVICE

ID: AMCLI-2610

Level: INFO

Description: Attempt to unassign service from an identity.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute unassign service from an identity Commandline interface.

SUCCEED_IDREPO_UNASSIGN_SERVICE

ID: AMCLI-2611

Level: INFO

Description: Service is unassigned from an identity.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute unassign service from an identity Commandline interface.

FAILED_IDREPO_UNASSIGN_SERVICE

ID: AMCLI-2612

Level: INFO

Description: Unable to unassign service to an identity.

Data: name of realm, identity type, name of identity, name of service, error message

Triggers: Execute unassign service from an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_MODIFY_SERVICE

ID: AMCLI-2620

Level: INFO

Description: Attempt to modify service attribute values of an identity.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute modify service attribute values of an identity Commandline interface.

SUCCEED_IDREPO_MODIFY_SERVICE

ID: AMCLI-2621

Level: INFO

Description: Service attribute values are modified.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute modify service attribute values of an identity Commandline interface.

FAILED_IDREPO_MODIFY_SERVICE

ID: AMCLI-2622

Level: INFO

Description: Unable to modify service attribute values of an identity.

Data: name of realm, identity type, name of identity, name of service, error message

Triggers: Execute modify service attribute values of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_SET_ATTRIBUTE_VALUES

ID: AMCLI-2630

Level: INFO

Description: Attempt to set attribute values of an identity.

Data: name of realm, identity type, name of identity

Triggers: Execute set attribute values of an identity Commandline interface.

SUCCEED_IDREPO_SET_ATTRIBUTE_VALUES

ID: AMCLI-2631

Level: INFO

Description: Attribute values are modified.

Data: name of realm, identity type, name of identity

Triggers: Execute set attribute values of an identity Commandline interface.

FAILED_IDREPO_SET_ATTRIBUTE_VALUES

ID: AMCLI-2632

Level: INFO

Description: Unable to set attribute values of an identity.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute set attribute values of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_GET_PRIVILEGES

ID: AMCLI-2640

Level: INFO

Description: Attempt to get privileges of an identity.

Data: name of realm, identity type, name of identity

Triggers: Execute get privileges of an identity Commandline interface.

SUCCEED_IDREPO_GET_PRIVILEGES

ID: AMCLI-2641

Level: INFO

Description: Privileges are returned.

Data: name of realm, identity type, name of identity

Triggers: Execute get privileges of an identity Commandline interface.

FAILED_IDREPO_GET_PRIVILEGES

ID: AMCLI-2642

Level: INFO

Description: Unable to get privileges of an identity.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute get privileges of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_ADD_PRIVILEGES

ID: AMCLI-2650

Level: INFO

Description: Attempt to add privileges to an identity.

Data: name of realm, identity type, name of identity

Triggers: Execute add privileges to an identity Commandline interface.

SUCCEED_IDREPO_ADD_PRIVILEGES

ID: AMCLI-2651

Level: INFO

Description: Privileges are added.

Data: name of realm, identity type, name of identity

Triggers: Execute add privileges to an identity Commandline interface.

FAILED_IDREPO_ADD_PRIVILEGES

ID: AMCLI-2652

Level: INFO

Description: Unable to add privileges to an identity.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute add privileges to an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_REMOVE_PRIVILEGES

ID: AMCLI-2660

Level: INFO

Description: Attempt to remove privileges from an identity.

Data: name of realm, identity type, name of identity

Triggers: Execute remove privileges from an identity Commandline interface.

SUCCEED_IDREPO_REMOVE_PRIVILEGES

ID: AMCLI-2661

Level: INFO

Description: Privileges are removed.

Data: name of realm, identity type, name of identity

Triggers: Execute remove privileges from an identity Commandline interface.

FAILED_IDREPO_REMOVE_PRIVILEGES

ID: AMCLI-2662

Level: INFO

Description: Unable to remove privileges from an identity.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute remove privileges from an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_ATTRIBUTE_SCHEMA_BOOLEAN_VALUES

ID: AMCLI-2670

Level: INFO

Description: Attempt to set boolean values to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute set attribute schema boolean values Commandline interface.

SUCCEED_SET_ATTRIBUTE_SCHEMA_BOOLEAN_VALUES

ID: AMCLI-2671

Level: INFO

Description: Boolean values are set.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute set attribute schema boolean values Commandline interface.

FAILED_SET_ATTRIBUTE_SCHEMA_BOOLEAN_VALUES

ID: AMCLI-2672

Level: INFO

Description: Unable to set boolean values to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema, error message

Triggers: Execute set attribute schema boolean values Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_AUTH_INSTANCES

ID: AMCLI-2680

Level: INFO

Description: Attempt to list authentication instances.

Data: name of realm

Triggers: Execute list authentication instances Commandline interface.

SUCCEEDED_LIST_AUTH_INSTANCES

ID: AMCLI-2681

Level: INFO

Description: List authentication instances succeeded.

Data: name of realm

Triggers: Execute list authentication instances Commandline interface.

FAILED_LIST_AUTH_INSTANCES

ID: AMCLI-2682

Level: INFO

Description: Failed to list authentication instances.

Data: name of realm

Triggers: Execute list authentication instances Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_AUTH_INSTANCE

ID: AMCLI-2690

Level: INFO

Description: Attempt to create authentication instance.

Data: name of realm, name of authentication instance, type of authentication instance

Triggers: Execute create authentication instance Commandline interface.

SUCCEEDED_CREATE_AUTH_INSTANCE

ID: AMCLI-2691

Level: INFO

Description: Authentication instance created.

Data: name of realm, name of authentication instance, type of authentication instance

Triggers: Execute create authentication instance Commandline interface.

FAILED_CREATE_AUTH_INSTANCE

ID: AMCLI-2692

Level: INFO

Description: Failed to create authentication instance.

Data: name of realm, name of authentication instance, type of authentication instance

Triggers: Execute create authentication instance Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_AUTH_INSTANCES

ID: AMCLI-2700

Level: INFO

Description: Attempt to delete authentication instances.

Data: name of realm, name of authentication instances

Triggers: Execute delete authentication instance Commandline interface.

SUCCEEDED_DELETE_AUTH_INSTANCES

ID: AMCLI-2701

Level: INFO

Description: Authentication instances are deleted.

Data: name of realm, name of authentication instances

Triggers: Execute delete authentication instances Commandline interface.

FAILED_DELETE_AUTH_INSTANCES

ID: AMCLI-2702

Level: INFO

Description: Failed to delete authentication instance.

Data: name of realm, name of authentication instances

Triggers: Execute delete authentication instances Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_AUTH_INSTANCE

ID: AMCLI-2710

Level: INFO

Description: Attempt to update authentication instance.

Data: name of realm, name of authentication instance

Triggers: Execute update authentication instance Commandline interface.

SUCCEEDED_UPDATE_AUTH_INSTANCE

ID: AMCLI-2711

Level: INFO

Description: Authentication instance is updated.

Data: name of realm, name of authentication instance

Triggers: Execute update authentication instance Commandline interface.

FAILED_UPDATE_AUTH_INSTANCE

ID: AMCLI-2712

Level: INFO

Description: Failed to update authentication instance.

Data: name of realm, name of authentication instance

Triggers: Execute update authentication instance Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_AUTH_INSTANCE

ID: AMCLI-2710

Level: INFO

Description: Attempt to get authentication instance.

Data: name of realm, name of authentication instance

Triggers: Execute get authentication instance Commandline interface.

SUCCEEDED_GET_AUTH_INSTANCE

ID: AMCLI-2711

Level: INFO

Description: Authentication instance profile is displayed.

Data: name of realm, name of authentication instance

Triggers: Execute get authentication instance Commandline interface.

FAILED_GET_AUTH_INSTANCE

ID: AMCLI-2712

Level: INFO

Description: Failed to get authentication instance.

Data: name of realm, name of authentication instance

Triggers: Execute get authentication instance Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_AUTH_CONFIGURATIONS

ID: AMCLI-2720

Level: INFO

Description: Attempt to list authentication configurations.

Data: name of realm

Triggers: Execute list authentication configurations Commandline interface.

SUCCEEDED_LIST_AUTH_CONFIGURATIONS

ID: AMCLI-2721

Level: INFO

Description: List authentication configurations succeeded.

Data: name of realm

Triggers: Execute list authentication configurations Commandline interface.

FAILED_LIST_AUTH_CONFIGURATIONS

ID: AMCLI-2722

Level: INFO

Description: Failed to list authentication configurations.

Data: name of realm

Triggers: Execute list authentication configurations Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_AUTH_CONFIGURATION

ID: AMCLI-2730

Level: INFO

Description: Attempt to create authentication configuration.

Data: name of realm, name of authentication configuration

Triggers: Execute create authentication configuration Commandline interface.

SUCCEEDED_CREATE_AUTH_CONFIGURATION

ID: AMCLI-2731

Level: INFO

Description: Authentication configuration created.

Data: name of realm, name of authentication configuration

Triggers: Execute create authentication configuration Commandline interface.

FAILED_CREATE_AUTH_CONFIGURATION

ID: AMCLI-2732

Level: INFO

Description: Failed to create authentication configuration.

Data: name of realm, name of authentication configuration

Triggers: Execute create authentication configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_AUTH_CONFIGURATIONS

ID: AMCLI-2740

Level: INFO

Description: Attempt to delete authentication configurations.

Data: name of realm, name of authentication configurations

Triggers: Execute delete authentication configurations Commandline interface.

SUCCEEDED_DELETE_AUTH_CONFIGURATIONS

ID: AMCLI-2741

Level: INFO

Description: Authentication configurations are deleted.

Data: name of realm, name of authentication configurations

Triggers: Execute delete authentication configurations Commandline interface.

FAILED_DELETE_AUTH_CONFIGURATIONS

ID: AMCLI-2742

Level: INFO

Description: Failed to delete authentication instance.

Data: name of realm, name of authentication configurations

Triggers: Execute delete authentication configurations Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2750

Level: INFO

Description: Attempt to get authentication configuration entries.

Data: name of realm, name of authentication configuration

Triggers: Execute get authentication configuration entries Commandline interface.

SUCCEEDED_GET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2751

Level: INFO

Description: Authentication instance configuration entries are displayed.

Data: name of realm, name of authentication configuration

Triggers: Execute get authentication configuration entries Commandline interface.

FAILED_GET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2752

Level: INFO

Description: Failed to get authentication configuration entries.

Data: name of realm, name of authentication configuration

Triggers: Execute get authentication configuration entries Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2760

Level: INFO

Description: Attempt to set authentication configuration entries.

Data: name of realm, name of authentication configuration

Triggers: Execute set authentication configuration entries Commandline interface.

SUCCEEDED_SET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2761

Level: INFO

Description: Authentication instance configuration entries are displayed.

Data: name of realm, name of authentication configuration

Triggers: Execute set authentication configuration entries Commandline interface.

FAILED_SET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2762

Level: INFO

Description: Failed to set authentication configuration entries.

Data: name of realm, name of authentication configuration

Triggers: Execute set authentication configuration entries Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_DATASTORES

ID: AMCLI-2770

Level: INFO

Description: Attempt to list datastores.

Data: name of realm

Triggers: Execute list datastores Commandline interface.

SUCCEEDED_LIST_DATASTORES

ID: AMCLI-2771

Level: INFO

Description: List datastores succeeded.

Data: name of realm

Triggers: Execute list datastores Commandline interface.

FAILED_LIST_DATASTORES

ID: AMCLI-2772

Level: INFO

Description: Failed to list datastores.

Data: name of realm, error message

Triggers: Execute list datastores Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_DATASTORE

ID: AMCLI-2780

Level: INFO

Description: Attemp to create datastore.

Data: name of realm, name of datastore, type of datastore

Triggers: Execute create datastore Commandline interface.

SUCCEEDED_CREATE_DATASTORE

ID: AMCLI-2781

Level: INFO

Description: Create datastore succeeded.

Data: name of realm, name of datastore, type of datastore

Triggers: Execute create datastore Commandline interface.

FAILED_CREATE_DATASTORE

ID: AMCLI-2782

Level: INFO

Description: Failed to create datastore.

Data: name of realm, name of datastore, type of datastore

Triggers: Execute create datastore Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_DATASTORES

ID: AMCLI-2790

Level: INFO

Description: Attempt to delete datastores.

Data: name of realm, names of datastore

Triggers: Execute delete datastores Commandline interface.

Reference OpenAM 11 (2018-01-25T14:19:04.804)
391

SUCCEEDED_DELETE_DATASTORES

ID: AMCLI-2791

Level: INFO

Description: Delete datastores succeeded.

Data: name of realm, names of datastore

Triggers: Execute delete datastores Commandline interface.

FAILED_DELETE_DATASTORES

ID: AMCLI-2792

Level: INFO

Description: Failed to delete datastores.

Data: name of realm, names of datastore

Triggers: Execute delete datastore Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_DATASTORE

ID: AMCLI-2800

Level: INFO

Description: Attempt to update datastore profile.

Data: name of realm, name of datastore

Triggers: Execute update datastore Commandline interface.

SUCCEEDED_UPDATE_DATASTORE

ID: AMCLI-2801

Level: INFO

Description: Update datastore succeeded.

Data: name of realm, name of datastore

Triggers: Execute update datastore Commandline interface.

FAILED_UPDATE_DATASTORE

ID: AMCLI-2802

Level: INFO

Description: Failed to update datastore.

Data: name of realm, name of datastore, error message

Triggers: Execute update datastore Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IMPORT_SM_CONFIG_DATA

ID: AMCLI-2900

Level: INFO

Description: Attempt to import service management configuration data.

Data: name of file

Triggers: Execute export configuration data Commandline interface.

SUCCEEDED_IMPORT_SM_CONFIG_DATA

ID: AMCLI-2901

Level: INFO

Description: Import service management configuration data succeeded.

Data: name of file

Triggers: Execute export configuration data Commandline interface.

FAILED_IMPORT_SM_CONFIG_DATA

ID: AMCLI-2902

Level: INFO

Description: Failed to import service management configuration data.

Data: name of file, error message

Triggers: Execute export configuration data Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_EXPORT_SM_CONFIG_DATA

ID: AMCLI-3000

Level: INFO

Description: Attempt to export service management configuration data.

Data: name of file

Triggers: Execute export configuration data Commandline interface.

SUCCEEDED_IMPORT_SM_CONFIG_DATA

ID: AMCLI-3001

Level: INFO

Description: Export service management configuration data succeeded.

Data: name of file

Triggers: Execute export configuration data Commandline interface.

FAILED_EXPORT_SM_CONFIG_DATA

ID: AMCLI-3002

Level: INFO

Description: Failed to export service management configuration data.

Data: name of file, error message

Triggers: Execute export configuration data Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_SERVERCONFIG_XML

ID: AMCLI-3010

Level: INFO

Description: Attempt to create server configuration xml.

Data: name of file

Triggers: Execute create server configuration xml Commandline interface.

SUCCEEDED_CREATE_SERVERCONFIG_XML

ID: AMCLI-3011

Level: INFO

Description: Create server configuration xml succeeded.

Data: name of file

Triggers: Execute create server configuration xml Commandline interface.

FAILED_CREATE_SERVERCONFIG_XML

ID: AMCLI-3012

Level: INFO

Description: Failed to create server configuration xml.

Data: name of file, error message

Triggers: Execute create server configuration xml Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REALM_REMOVE_SERVICE_ATTR_VALUES

ID: AMCLI-3020

Level: INFO

Description: Attempt to remove service attribute values of realm.

Data: name of realm, name of service

Triggers: Execute remove service attribute values of realm Commandline interface.

SUCCEED_REALM_REMOVE_SERVICE_ATTR_VALUES

ID: AMCLI-3021

Level: INFO

Description: Service attribute values of realm are removed.

Data: name of realm, name of service

Triggers: Execute remove service attribute values of realm Commandline interface.

FAILED_REALM_REMOVE_SERVICE_ATTR_VALUES

ID: AMCLI-3022

Level: INFO

Description: Unable to remove service attribute values of realm.

Data: name of realm, name of service, error message

Triggers: Execute remove service attribute values of realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REALM_ADD_SERVICE_ATTR_VALUES

ID: AMCLI-3030

Level: INFO

Description: Attempt to add service attribute values of realm.

Data: name of realm, name of service

Triggers: Execute add service attribute values of realm Commandline interface.

SUCCEED_REALM_ADD_SERVICE_ATTR_VALUES

ID: AMCLI-3031

Level: INFO

Description: Service attribute values of realm are added.

Data: name of realm, name of service

Triggers: Execute add service attribute values of realm Commandline interface.

FAILED_REALM_ADD_SERVICE_ATTR_VALUES

ID: AMCLI-3032

Level: INFO

Description: Unable to add service attribute values of realm.

Data: name of realm, name of service, error message

Triggers: Execute add service attribute values of realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_SERVER_CONFIG

ID: AMCLI-3040

Level: INFO

Description: Attempt to list server configuration.

Data: name of server

Triggers: Execute list server configuration Commandline interface.

SUCCEED_LIST_SERVER_CONFIG

ID: AMCLI-3041

Level: INFO

Description: Server configuration is displayed.

Data: name of server

Triggers: Execute list server configuration Commandline interface.

FAILED_LIST_SERVER_CONFIG

ID: AMCLI-3042

Level: INFO

Description: Unable to list server configuration.

Data: name of server, error message

Triggers: Execute list server configuration Commandline interface.

Actions: Check if servername is correct.; Look under debug file for more information.

ATTEMPT_UPDATE_SERVER_CONFIG

ID: AMCLI-3050

Level: INFO

Description: Attempt to update server configuration.

Data: name of server

Triggers: Execute update server configuration Commandline interface.

SUCCEED_UPDATE_SERVER_CONFIG

ID: AMCLI-3051

Level: INFO

Description: Server configuration is updated.

Data: name of server

Triggers: Execute update server configuration Commandline interface.

FAILED_UPDATE_SERVER_CONFIG

ID: AMCLI-3052

Level: INFO

Description: Unable to update server configuration.

Data: name of server, error message

Triggers: Execute update server configuration Commandline interface.

Actions: Check if servername is correct.; Look under debug file for more information.

ATTEMPT_REMOVE_SERVER_CONFIG

ID: AMCLI-3060

Level: INFO

Description: Attempt to remove server configuration.

Data: name of server

Triggers: Execute remove server configuration Commandline interface.

SUCCEED_REMOVE_SERVER_CONFIG

ID: AMCLI-3061

Level: INFO

Description: Server configuration is removed.

Data: name of server

Triggers: Execute remove server configuration Commandline interface.

FAILED_REMOVE_SERVER_CONFIG

ID: AMCLI-3062

Level: INFO

Description: Remove server configuration.

Data: name of server, error message

Triggers: Execute remove server configuration Commandline interface.

Actions: Check if servername is correct.; Look under debug file for more information.

ATTEMPT_CREATE_SERVER

ID: AMCLI-3070

Level: INFO

Description: Attempt to create server.

Data: name of server

Triggers: Execute create server Commandline interface.

SUCCEED_CREATE_SERVER

ID: AMCLI-3071

Level: INFO

Description: Server is created.

Data: name of server

Triggers: Execute create server Commandline interface.

FAILED_CREATE_SERVER

ID: AMCLI-3072

Level: INFO

Description: Unable to create server.

Data: name of server, error message

Triggers: Execute create server Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_SERVER

ID: AMCLI-3080

Level: INFO

Description: Attempt to delete server.

Data: name of server

Triggers: Execute delete server Commandline interface.

SUCCEED_DELETE_SERVER

ID: AMCLI-3081

Level: INFO

Description: Server is deleted.

Data: name of server

Triggers: Execute delete server Commandline interface.

FAILED_DELETE_SERVER

ID: AMCLI-3082

Level: INFO

Description: Unable to delete server.

Data: name of server, error message

Triggers: Execute delete server Commandline interface.

Actions: Check the name of the server.; Look under debug file for more information.

ATTEMPT_LIST_SERVERS

ID: AMCLI-3090

Level: INFO

Description: Attempt to list servers.

Triggers: Execute list servers Commandline interface.

SUCCEED_LIST_SERVERS

ID: AMCLI-3091

Level: INFO

Description: Servers are displayed.

Triggers: Execute list servers Commandline interface.

FAILED_LIST_SERVERS

ID: AMCLI-3092

Level: INFO

Description: Unable to list servers.

Data: error message

Triggers: Execute list servers Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_SITE

ID: AMCLI-3100

Level: INFO

Description: Attempt to create site.

Data: name of site, primary URL of site

Triggers: Execute create site Commandline interface.

SUCCEED_CREATE_SITE

ID: AMCLI-3101

Level: INFO

Description: Site is created.

Data: name of site, primary URL of site

Triggers: Execute create site Commandline interface.

FAILED_CREATE_SITE

ID: AMCLI-3102

Level: INFO

Description: Unable to create site.

Data: name of site, primary URL of site, error message

Triggers: Execute create site Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_SITES

ID: AMCLI-3110

Level: INFO

Description: Attempt to list sites.

Triggers: Execute list sites Commandline interface.

SUCCEED_LIST_SITES

ID: AMCLI-3111

Level: INFO

Description: Sites are displayed.

Triggers: Execute list sites Commandline interface.

FAILED_LIST_SITES

ID: AMCLI-3112

Level: INFO

Description: Unable to list sites.

Data: error message

Triggers: Execute list sites Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_SITE_MEMBERS

ID: AMCLI-3120

Level: INFO

Description: Attempt to show site members.

Data: name of site

Triggers: Execute show site members Commandline interface.

SUCCEED_SHOW_SITE_MEMBERS

ID: AMCLI-3121

Level: INFO

Description: Site members are displayed.

Data: name of site

Triggers: Execute show site members Commandline interface.

FAILED_SHOW_SITE_MEMBERS

ID: AMCLI-3122

Level: INFO

Description: Unable to show site members.

Data: name of site, error message

Triggers: Execute show site members Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SITE_MEMBERS

ID: AMCLI-3130

Level: INFO

Description: Attempt to add members to site.

Data: name of site

Triggers: Execute add members to site Commandline interface.

SUCCEED_ADD_SITE_MEMBERS

ID: AMCLI-3131

Level: INFO

Description: Members are added to site.

Data: name of site

Triggers: Execute add members to site Commandline interface.

FAILED_ADD_SITE_MEMBERS

ID: AMCLI-3132

Level: INFO

Description: Unable to add members to site.

Data: name of site, error message

Triggers: Execute add members to site Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_SITE_MEMBERS

ID: AMCLI-3140

Level: INFO

Description: Attempt to remove members from site.

Data: name of site

Triggers: Execute remove members from site Commandline interface.

SUCCEED_REMOVE_SITE_MEMBERS

ID: AMCLI-3141

Level: INFO

Description: Members are removed from site.

Data: name of site

Triggers: Execute remove members from site Commandline interface.

FAILED_REMOVE_SITE_MEMBERS

ID: AMCLI-3142

Level: INFO

Description: Unable to remove members from site.

Data: name of site, error message

Triggers: Execute remove members from site Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_SITE

ID: AMCLI-3150

Level: INFO

Description: Attempt to delete site.

Data: name of site

Triggers: Execute delete site Commandline interface.

SUCCEED_DELETE_SITE

ID: AMCLI-3151

Level: INFO

Description: Site is deleted.

Data: name of site

Triggers: Execute delete site Commandline interface.

FAILED_DELETE_SITE

ID: AMCLI-3152

Level: INFO

Description: Unable to delete members from site.

Data: name of site, error message

Triggers: Execute delete site Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SITE_PRIMARY_URL

ID: AMCLI-3160

Level: INFO

Description: Attempt to set site primary URL.

Data: name of site, primary URL of site

Triggers: Execute set site primary URL Commandline interface.

SUCCEED_SET_SITE_PRIMARY_URL

ID: AMCLI-3161

Level: INFO

Description: Site primary URL is set.

Data: name of site, primary URL of site

Triggers: Execute set site primary URL Commandline interface.

FAILED_SET_SITE_PRIMARY_URL

ID: AMCLI-3162

Level: INFO

Description: Unable to set site primary URL.

Data: name of site, primary URL of site, error message

Triggers: Execute set site primary URL Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_SITE

ID: AMCLI-3170

Level: INFO

Description: Attempt to show site profile.

Data: name of site

Triggers: Execute show site profile Commandline interface.

SUCCEED_SHOW_SITE

ID: AMCLI-3171

Level: INFO

Description: Site profile is displayed.

Data: name of site

Triggers: Execute show site profile Commandline interface.

FAILED_SHOW_SITE

ID: AMCLI-3172

Level: INFO

Description: Unable to show site profile.

Data: name of site, error message

Triggers: Execute show site profile Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SITE_FAILOVER_URLS

ID: AMCLI-3180

Level: INFO

Description: Attempt to set site failover URLs.

Data: name of site

Triggers: Execute set site failover URLs Commandline interface.

SUCCEED_SET_SITE_FAILOVER_URLS

ID: AMCLI-3181

Level: INFO

Description: Site failover URLs are set.

Data: name of site

Triggers: Execute set site failover URLs Commandline interface.

FAILED_SET_SITE_FAILOVER_URLS

ID: AMCLI-3182

Level: INFO

Description: Unable to set site failover URLs.

Data: name of site, error message

Triggers: Execute set site failover URLs Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SITE_FAILOVER_URLS

ID: AMCLI-3190

Level: INFO

Description: Attempt to add site failover URLs.

Data: name of site

Triggers: Execute add site failover URLs Commandline interface.

SUCCEED_ADD_SITE_FAILOVER_URLS

ID: AMCLI-3191

Level: INFO

Description: Site failover URLs are added.

Data: name of site

Triggers: Execute add site failover URLs Commandline interface.

FAILED_ADD_SITE_FAILOVER_URLS

ID: AMCLI-3192

Level: INFO

Description: Unable to add site failover URLs.

Data: name of site, error message

Triggers: Execute add site failover URLs Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_SITE_FAILOVER_URLS

ID: AMCLI-3200

Level: INFO

Description: Attempt to remove site failover URLs.

Data: name of site

Triggers: Execute remove site failover URLs Commandline interface.

SUCCEED_REMOVE_SITE_FAILOVER_URLS

ID: AMCLI-3201

Level: INFO

Description: Site failover URLs are removed.

Data: name of site

Triggers: Execute remove site failover URLs Commandline interface.

FAILED_REMOVE_SITE_FAILOVER_URLS

ID: AMCLI-3202

Level: INFO

Description: Unable to remove site failover URLs.

Data: name of site, error message

Triggers: Execute remove site failover URLs Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CLONE_SERVER

ID: AMCLI-3210

Level: INFO

Description: Attempt to clone server.

Data: name of server, name of cloned server

Triggers: Execute clone server Commandline interface.

SUCCEED_CLONE_SERVER

ID: AMCLI-3211

Level: INFO

Description: Server is cloned.

Data: name of server, name of cloned server

Triggers: Execute clone server Commandline interface.

FAILED_CLONE_SERVER

ID: AMCLI-3212

Level: INFO

Description: Unable to clone server.

Data: name of server, name of cloned server, error message

Triggers: Execute clone server Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_EXPORT_SERVER

ID: AMCLI-3220

Level: INFO

Description: Attempt to export server.

Data: name of server

Triggers: Execute export server Commandline interface.

SUCCEED_EXPORT_SERVER

ID: AMCLI-3221

Level: INFO

Description: Server is cloned.

Data: name of server

Triggers: Execute export server Commandline interface.

FAILED_EXPORT_SERVER

ID: AMCLI-3222

Level: INFO

Description: Unable to export server.

Data: name of server, error message

Triggers: Execute export server Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IMPORT_SERVER

ID: AMCLI-3230

Level: INFO

Description: Attempt to import server configuration.

Data: name of server

Triggers: Execute import server configuration Commandline interface.

SUCCEED_IMPORT_SERVER

ID: AMCLI-3231

Level: INFO

Description: Server configuration is imported.

Data: name of server

Triggers: Execute import server configuration Commandline interface.

FAILED_IMPORT_SERVER

ID: AMCLI-3232

Level: INFO

Description: Unable to import server configuration.

Data: name of server, error message

Triggers: Execute import server configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SUPPORTED_DATA_TYPES

ID: AMCLI-5000

Level: INFO

Description: Attempt to get the supported data types.

Triggers: Execute get the supported data type Commandline interface.

SUCCEED_GET_SUPPORTED_DATA_TYPES

ID: AMCLI-5001

Level: INFO

Description: The supported data types are retrieved.

Triggers: Execute add service attribute values Commandline interface.

FAILED_GET_SUPPORTED_DATA_TYPES

ID: AMCLI-5002

Level: INFO

Description: Unable to get the supported data types.

Data: error message

Triggers: Execute get the supported data types Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_AGENT

ID: AMCLI-4000

Level: INFO

Description: Attempt to create an agent.

Data: realm, agent type, name of agent

Triggers: Execute create agent Commandline interface.

SUCCEED_CREATE_AGENT

ID: AMCLI-4001

Level: INFO

Description: Agent is created.

Data: realm, agent type, name of agent

Triggers: Execute create agent Commandline interface.

FAILED_CREATE_AGENT

ID: AMCLI-4002

Level: INFO

Description: Unable to create agent.

Data: realm, agent type, name of agent, error message

Triggers: Execute create agent Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_AGENTS

ID: AMCLI-4010

Level: INFO

Description: Attempt to delete agents.

Data: name of realm, name of agents

Triggers: Execute delete agents Commandline interface.

SUCCEED_DELETE_AGENTS

ID: AMCLI-4011

Level: INFO

Description: Agents are deleted.

Data: name of realm, name of agents

Triggers: Execute delete agents Commandline interface.

FAILED_DELETE_AGENTS

ID: AMCLI-4012

Level: INFO

Description: Unable to delete agents.

Data: name of realm, name of agents, error message

Triggers: Execute delete agents Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_AGENT

ID: AMCLI-4020

Level: INFO

Description: Attempt to set attribute values of an agent.

Data: name of realm, name of agent

Triggers: Execute update agent Commandline interface.

SUCCEED_UPDATE_AGENT

ID: AMCLI-4021

Level: INFO

Description: Agent profile is modified.

Data: name of realm, name of agent

Triggers: Execute update agent Commandline interface.

FAILED_UPDATE_AGENT

ID: AMCLI-4022

Level: INFO

Description: Unable to update an agent.

Data: name of realm, name of agent, error message

Triggers: Execute update agent Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_AGENTS

ID: AMCLI-4030

Level: INFO

Description: Attempt to list agents.

Data: name of realm, agent type, search pattern

Triggers: Execute list agents Commandline interface.

SUCCEED_LIST_AGENTS

ID: AMCLI-4031

Level: INFO

Description: Search Result is returned.

Data: name of realm, agent type, search pattern

Triggers: Execute list agents Commandline interface.

FAILED_LIST_AGENTS

ID: AMCLI-4032

Level: INFO

Description: Unable to list agents.

Data: name of realm, agent type, search pattern, error message

Triggers: Execute list agents Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_AGENT

ID: AMCLI-4040

Level: INFO

Description: Attempt to get attribute values of an agent.

Data: name of realm, name of agent

Triggers: Execute get the attribute values of an agent Commandline interface.

SUCCEED_SHOW_AGENT

ID: AMCLI-4041

Level: INFO

Description: Attribute values are returned.

Data: name of realm, name of agent

Triggers: Execute get the attribute values of an agent Commandline interface.

FAILED_SHOW_AGENT

ID: AMCLI-4042

Level: INFO

Description: Unable to get the attribute values of an agent.

Data: name of realm, name of agent, error message

Triggers: Execute get the attribute values of an agent Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_AGENT_GROUP

ID: AMCLI-4050

Level: INFO

Description: Attempt to create an agent group.

Data: realm, agent type, name of agent group

Triggers: Execute create agent group Commandline interface.

SUCCEED_CREATE_AGENT_GROUP

ID: AMCLI-4051

Level: INFO

Description: Agent group is created.

Data: realm, agent type, name of agent group

Triggers: Execute create agent group Commandline interface.

FAILED_CREATE_AGENT_GROUP

ID: AMCLI-4052

Level: INFO

Description: Unable to create agent group.

Data: realm, agent type, name of agent group, error message

Triggers: Execute create agent group Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_AGENT_GROUPS

ID: AMCLI-4060

Level: INFO

Description: Attempt to delete agent groups.

Data: name of realm, name of agent groups

Triggers: Execute delete agent groups Commandline interface.

SUCCEED_DELETE_AGENT_GROUPS

ID: AMCLI-4061

Level: INFO

Description: Agent groups are deleted.

Data: name of realm, name of agent groups

Triggers: Execute delete agent groups Commandline interface.

FAILED_DELETE_AGENT_GROUPS

ID: AMCLI-4062

Level: INFO

Description: Unable to delete agent groups.

Data: name of realm, name of agent groups, error message

Triggers: Execute delete agent groups Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_AGENT_GROUPS

ID: AMCLI-4070

Level: INFO

Description: Attempt to list agent groups.

Data: name of realm, agent type, search pattern

Triggers: Execute list agent groups Commandline interface.

SUCCEED_LIST_AGENT_GROUPS

ID: AMCLI-4071

Level: INFO

Description: Search Result is returned.

Data: name of realm, agent type, search pattern

Triggers: Execute list agent groups Commandline interface.

FAILED_LIST_AGENT_GROUPS

ID: AMCLI-4072

Level: INFO

Description: Unable to list agent groups.

Data: name of realm, agent type, search pattern, error message

Triggers: Execute list agent groups Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_AGENT_TO_GROUP

ID: AMCLI-4080

Level: INFO

Description: Attempt to add agent to group.

Data: name of realm, name of agent group, name of agent

Triggers: Execute add agents to group Commandline interface.

SUCCEED_ADD_AGENT_TO_GROUP

ID: AMCLI-4081

Level: INFO

Description: Agent is added to group.

Data: name of realm, name of agent group, name of agent

Triggers: Execute add agent to group Commandline interface.

FAILED_ADD_AGENT_TO_GROUP

ID: AMCLI-4082

Level: INFO

Description: Unable to add agent to group.

Data: name of realm, name of agent group, name of agent, error message

Triggers: Execute add agent to group Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_AGENT_FROM_GROUP

ID: AMCLI-4090

Level: INFO

Description: Attempt to remove agent from group.

Data: name of realm, name of agent group, name of agent

Triggers: Execute remove agent from group Commandline interface.

SUCCEED_REMOVE_AGENT_FROM_GROUP

ID: AMCLI-4091

Level: INFO

Description: Agent is removed to group.

Data: name of realm, name of agent group, name of agent

Triggers: Execute remove agent from group Commandline interface.

FAILED_REMOVE_AGENT_FROM_GROUP

ID: AMCLI-4092

Level: INFO

Description: Unable to remove agent from group.

Data: name of realm, name of agent group, name of agent, error message

Triggers: Execute remove agent from group Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_AGENT_PWD

ID: AMCLI-4100

Level: INFO

Description: Attempt to set agent password.

Data: realm, name of agent

Triggers: Execute set agent password Commandline interface.

SUCCEED_SET_AGENT_PWD

ID: AMCLI-4101

Level: INFO

Description: Agent password is modified.

Data: realm, name of agent

Triggers: Execute set agent password Commandline interface.

FAILED_SET_AGENT_PWD

ID: AMCLI-4102

Level: INFO

Description: Unable to set agent password.

Data: realm, name of agent, error message

Triggers: Execute set agent password Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_AGENT_GROUP

ID: AMCLI-4110

Level: INFO

Description: Attempt to get attribute values of an agent group.

Data: name of realm, name of agent group

Triggers: Execute get the attribute values of an agent group Commandline interface.

SUCCEED_SHOW_AGENT_GROUP

ID: AMCLI-4111

Level: INFO

Description: Attribute values are returned.

Data: name of realm, name of agent group

Triggers: Execute get the attribute values of an agent group Commandline interface.

FAILED_SHOW_AGENT_GROUP

ID: AMCLI-4112

Level: INFO

Description: Unable to get the attribute values of an agent group.

Data: name of realm, name of agent group, error message

Triggers: Execute get the attribute values of an agent group Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_AGENT_GROUP

ID: AMCLI-4120

Level: INFO

Description: Attempt to set attribute values of an agent group.

Data: name of realm, name of agent group

Triggers: Execute update agent group Commandline interface.

SUCCEED_UPDATE_AGENT_GROUP

ID: AMCLI-4121

Level: INFO

Description: Agent group profile is modified.

Data: name of realm, name of agent group

Triggers: Execute update agent group Commandline interface.

FAILED_UPDATE_AGENT_GROUP

ID: AMCLI-4122

Level: INFO

Description: Unable to update an agent.

Data: name of realm, name of agent group, error message

Triggers: Execute update agent group Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_AGENT_TYPES

ID: AMCLI-4130

Level: INFO

Description: Attempt to show supported agent types.

Triggers: Execute show supported agent types Commandline interface.

SUCCEED_SHOW_AGENT_TYPES

ID: AMCLI-4131

Level: INFO

Description: Supported agent types is displayed.

Triggers: Execute show supported agent types Commandline interface.

FAILED_SHOW_AGENT_TYPES

ID: AMCLI-4132

Level: INFO

Description: Unable to show supported agent types.

Data: error message

Triggers: Execute show supported agent types Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_AGENT_GROUP_MEMBERS

ID: AMCLI-4140

Level: INFO

Description: Attempt to show agent group members.

Data: name of realm, name of agent group

Triggers: Execute show agent group members Commandline interface.

SUCCEED_SHOW_AGENT_GROUP_MEMBERS

ID: AMCLI-4141

Level: INFO

Description: Agent group's members are displayed.

Data: name of realm, name of agent group

Triggers: Execute show agent group members Commandline interface.

FAILED_SHOW_AGENT_GROUP_MEMBERS

ID: AMCLI-4142

Level: INFO

Description: Unable to show agent group members.

Data: name of realm, name of agent group, error message

Triggers: Execute show agent group members Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_AGENT_MEMBERSHIP

ID: AMCLI-4150

Level: INFO

Description: Attempt to show agent's membership.

Data: name of realm, name of agent

Triggers: Execute show agent's membership Commandline interface.

SUCCEED_LIST_AGENT_MEMBERSHIP

ID: AMCLI-4151

Level: INFO

Description: Agent's membership are displayed.

Data: name of realm, name of agent

Triggers: Execute show agent's membership Commandline interface.

FAILED_LIST_AGENT_MEMBERSHIP

ID: AMCLI-4152

Level: INFO

Description: Unable to show agent's membership.

Data: name of realm, name of agent, error message

Triggers: Execute show agent's membership Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REGISTER_AUTH_MODULE

ID: AMCLI-4500

Level: INFO

Description: Attempt to register authentication module.

Data: name of service

Triggers: Execute register authentication module Commandline interface.

SUCCEED_REGISTER_AUTH_MODULE

ID: AMCLI-4501

Level: INFO

Description: Authentication module is registered.

Data: name of service

Triggers: Execute register authentication module Commandline interface.

FAILED_REGISTER_AUTH_MODULE

ID: AMCLI-4502

Level: INFO

Description: Unable to register authentication module.

Data: name of service, error message

Triggers: Execute register authentication module Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UNREGISTER_AUTH_MODULE

ID: AMCLI-4510

Level: INFO

Description: Attempt to unregister authentication module.

Data: name of service

Triggers: Execute unregister authentication module Commandline interface.

SUCCEED_UNREGISTER_AUTH_MODULE

ID: AMCLI-4511

Level: INFO

Description: Authentication module is unregistered.

Data: name of service

Triggers: Execute unregister authentication module Commandline interface.

FAILED_UNREGISTER_AUTH_MODULE

ID: AMCLI-4512

Level: INFO

Description: Unable to unregister authentication module.

Data: name of service, error message

Triggers: Execute unregister authentication module Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SUPPORTED_AUTH_MODULES

ID: AMCLI-4515

Level: INFO

Description: Attempt to get supported authentication modules in the system.

Triggers: Execute get supported authentication modules in the system Commandline interface.

SUCCEED_GET_SUPPORTED_AUTH_MODULES

ID: AMCLI-4516

Level: INFO

Description: Supported authentication modules in the system are displayed.

Triggers: Execute get supported authentication modules in the system module Commandline interface.

FAILED_GET_SUPPORTED_AUTH_MODULES

ID: AMCLI-4517

Level: INFO

Description: Failed to get supported authentication modules in the system.

Data: error message

Triggers: Execute get supported authentication modules in the system Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_AGENT_PROPERTIES

ID: AMCLI-4520

Level: INFO

Description: Attempt to remove property values of an agent.

Data: name of realm, name of agent, property names

Triggers: Execute remove property values of an agent Commandline interface.

SUCCEED_REMOVE_AGENT_PROPERTIES

ID: AMCLI-4521

Level: INFO

Description: Property values are removed.

Data: name of realm, name of agent, property names

Triggers: Execute remove property values of an agent Commandline interface.

FAILED_REMOVE_AGENT_PROPERTIES

ID: AMCLI-4522

Level: INFO

Description: Unable to remove property values of an agent.

Data: name of realm, name of agent, property names, error message

Triggers: Execute remove property values of an agent Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SERVER_CONFIG_XML

ID: AMCLI-4600

Level: INFO

Description: Attempt to get server configuration XML.

Data: name of server

Triggers: Execute get server configuration XML Commandline interface.

SUCCEED_GET_SERVER_CONFIG_XML

ID: AMCLI-4601

Level: INFO

Description: Server configuration XML is displayed.

Data: name of server

Triggers: Execute get server configuration XML Commandline interface.

FAILED_GET_SERVER_CONFIG_XML

ID: AMCLI-4602

Level: INFO

Description: Unable to get server configuration XML.

Data: name of server, error message

Triggers: Execute get server configuration XML Commandline interface.

Actions: Check if servername is correct.; Look under debug file for more information.

ATTEMPT_SET_SERVER_CONFIG_XML

ID: AMCLI-4610

Level: INFO

Description: Attempt to set server configuration XML.

Data: name of server

Triggers: Execute set server configuration XML Commandline interface.

SUCCEED_SET_SERVER_CONFIG_XML

ID: AMCLI-4611

Level: INFO

Description: Server configuration XML is set.

Data: name of server

Triggers: Execute set server configuration XML Commandline interface.

FAILED_SET_SERVER_CONFIG_XML

ID: AMCLI-4612

Level: INFO

Description: Unable to set server configuration XML.

Data: name of server, error message

Triggers: Execute set server configuration XML Commandline interface.

Actions: Check if servername is correct.; Look under debug file for more information.

ATTEMPT_LIST_DATASTORE_TYPES

ID: AMCLI-4700

Level: INFO

Description: Attempt to list supported datastore types.

Triggers: Execute list supported datastore types Commandline interface.

SUCCEEDED_LIST_DATASTORE_TYPES

ID: AMCLI-4701

Level: INFO

Description: List supported datastore types succeeded.

Triggers: Execute list supported datastore types Commandline interface.

FAILED_LIST_DATASTORE_TYPES

ID: AMCLI-4702

Level: INFO

Description: Failed to list supported datastore types.

Data: error message

Triggers: Execute list supported datastore types Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_AUTH_CONFIG_ENTRY

ID: AMCLI-4800

Level: INFO

Description: Attempt to add authentication configuration entry.

Data: name of realm, name of authentication configuration, name of module

Triggers: Execute add authentication configuration entry Commandline interface.

SUCCEEDED_ADD_AUTH_CONFIG_ENTRY

ID: AMCLI-4801

Level: INFO

Description: Authentication instance configuration entry is created.

Data: name of realm, name of authentication configuration, name of module

Triggers: Execute add authentication configuration entry Commandline interface.

FAILED_ADD_AUTH_CONFIG_ENTRY

ID: AMCLI-4802

Level: INFO

Description: Failed to add authentication configuration entry.

Data: name of realm, name of authentication configuration, name of module, error message

Triggers: Execute add authentication configuration entry Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_DATASTORE

ID: AMCLI-5000

Level: INFO

Description: Attempt to show datastore profile.

Data: name of realm, name of datastore

Triggers: Execute show datastore Commandline interface.

SUCCEEDED_SHOW_DATASTORE

ID: AMCLI-5001

Level: INFO

Description: Show datastore succeeded.

Data: name of realm, name of datastore

Triggers: Execute show datastore Commandline interface.

FAILED_SHOW_DATASTORE

ID: AMCLI-5002

Level: INFO

Description: Failed to show datastore profile.

Data: name of realm, name of datastore, error message

Triggers: Execute show datastore Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_AMSDK_PLUGIN

ID: AMCLI-5100

Level: INFO

Description: Add AMSDK IdRepo Plugin.

Data: name of datastore name

Triggers: Execute add AMSDK IdRepo Plugin Commandline interface.

SUCCEED_ADD_AMSDK_PLUGIN

ID: AMCLI-5101

Level: INFO

Description: AMSDK plugin is added.

Data: name of datastore name

Triggers: Execute add AMSDK IdRepo Plugin Commandline interface.

FAILED_ADD_AMSDK_PLUGIN

ID: AMCLI-5102

Level: INFO

Description: Failed to add AMSDK IdRepo Plugin.

Data: name of datastore name, error message

Triggers: Execute add AMSDK IdRepo Plugin Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SVC_ATTR_VALUES_REALM

ID: AMCLI-5200

Level: INFO

Description: Attempt to set attribute value to a service that is assigned to a realm.

Data: name of realm, name of service

Triggers: Execute set attribute values a service that is assigned to a to realm Commandline interface.

SUCCEED_SET_SVC_ATTR_VALUES_REALM

ID: AMCLI-5201

Level: INFO

Description: Attribute values is set to a service that is assigned to a realm.

Data: name of realm, name of service

Triggers: Execute set attribute values to a service that is assigned to a realm Commandline interface.

FAILED_SET_SVC_ATTR_VALUES_REALM

ID: AMCLI-5202

Level: INFO

Description: Unable to set attribute values to a service that is assigned to a realm.

Data: name of realm, name of service, error message

Triggers: Execute set attribute values to a service that is assigned to a realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_EMBEDDED_STATUS

ID: AMCLI-5103

Level: INFO

Description: Get Embedded Status.

Data: port number of embedded store

Triggers: Execute Embedded Status Commandline interface.

SUCCEEDED_EMBEDDED_STATUS

ID: AMCLI-5104

Level: INFO

Description: Embedded Status Successful.

Data: port number of embedded store

Triggers: Execute Embedded Status Commandline interface.

FAILED_EMBEDDED_STATUS

ID: AMCLI-5105

Level: INFO

Description: Failed to get embedded status.

Data: port number of embedded store, error message

Triggers: Execute Embedded Status Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_COT_MEMBER

ID: AMCLI-5106

Level: INFO

Description: Attempt to add a member to a Circle of Trust.

Data: realm, entity ID, circle of trust, protocol specification

Triggers: Execute add a member to a Circle of Trust Commandline interface.

SUCCEEDED_ADD_COT_MEMBER

ID: AMCLI-5107

Level: INFO

Description: Adding a member to a Circle of Trust succeeded.

Data: realm, entity ID, circle of trust, protocol specification

Triggers: Execute add a member to a Circle of Trust Commandline interface.

FAILED_ADD_COT_MEMBER

ID: AMCLI-5108

Level: INFO

Description: Failed to add a member to a circle of trust.

Data: realm, entity ID, circle of trust, protocol specification, error message

Triggers: Execute add a member to a Circle of Trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DO_BULK_FEDERATION

ID: AMCLI-5109

Level: INFO

Description: Attempt to do bulk federation.

Data: metaAlias for local provider, Remote entity Id, File name of local to remote user Id mapping, Name of file that will be created by this sub command, protocol specification

Triggers: Execute Do Bulk Federation Commandline interface.

SUCCEEDED_DO_BULK_FEDERATION

ID: AMCLI-5110

Level: INFO

Description: Bulk Federation succeeded.

Data: metaAlias for local provider, Remote entity Id, File name of local to remote user Id mapping, Name of file that will be created by this sub command, protocol specification

Triggers: Execute Do Bulk Federation Commandline interface.

FAILED_DO_BULK_FEDERATION

ID: AMCLI-5111

Level: INFO

Description: Failed to do bulk federation.

Data: metaAlias for local provider, Remote entity Id, File name of local to remote user Id mapping, Name of file that will be created by this sub command, protocol specification, error message

Triggers: Execute Do Bulk Federation Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_COT

ID: AMCLI-5112

Level: INFO

Description: Attempt to create Circle of Trust.

Data: Realm, Circle of Trust, Trusted Providers, Prefix URL for idp discovery reader and writer URL

Triggers: Execute Create Circle of Trust Commandline interface.

SUCCEEDED_CREATE_COT

ID: AMCLI-5113

Level: INFO

Description: Creating Circle of Trust succeeded.

Data: Realm, Circle of Trust, Trusted Providers, Prefix URL for idp discovery reader and writer URL

Triggers: Execute Create Circle of Trust Commandline interface.

FAILED_CREATE_COT

ID: AMCLI-5114

Level: INFO

Description: Failed to create Circle of Trust.

Data: Realm, Circle of Trust, Trusted Providers, Prefix URL for idp discovery reader and writer URL, error message

Triggers: Execute Create Circle of Trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_METADATA_TEMPL

ID: AMCLI-5115

Level: INFO

Description: Attempt to create metadata template.

Data: Entity ID, file name for the standard metadata to be created, file name for the extended metadata to be created, metaAlias for hosted identity provider to be created, metaAlias for hosted service provider to be created, metaAlias for hosted attribute authority to be created, metaAlias for hosted attribute query provider to be created, metaAlias for hosted authentication authority to be created, metaAlias for policy decision point to be created, metaAlias for policy enforcement point to be created, metaAlias for hosted affiliation, protocol specification

Triggers: Execute Create MetaData Template Commandline interface.

SUCCEEDED_CREATE_METADATA_TEMPL

ID: AMCLI-5116

Level: INFO

Description: Creating MetaData Template succeeded.

Data: Entity ID, file name for the standard metadata to be created, file name for the extended metadata to be created, metaAlias for hosted identity provider to be created, metaAlias for hosted service provider to be created, metaAlias for hosted attribute authority to be created, metaAlias for hosted attribute query provider to be created, metaAlias for hosted authentication authority to be created, metaAlias for policy decision point to be created, metaAlias for policy enforcement point to be created, metaAlias for hosted affiliation, protocol specification

Triggers: Execute Create MetaData Template Commandline interface.

FAILED_CREATE_METADATA_TEMPL

ID: AMCLI-5117

Level: INFO

Description: Failed to create metaData template.

Data: Entity ID, protocol specification, error message

Triggers: Execute Create MetaData Template Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_COT

ID: AMCLI-5118

Level: INFO

Description: Attempt to delete Circle of Trust.

Data: Realm, Circle of Trust

Triggers: Execute Delete Circle of Trust Commandline interface.

SUCCEEDED_DELETE_COT

ID: AMCLI-5119

Level: INFO

Description: Deleting Circle of Trust succeeded.

Data: Realm, Circle of Trust

Triggers: Execute Delete Circle of Trust Commandline interface.

FAILED_DELETE_COT

ID: AMCLI-5120

Level: INFO

Description: Failed to delete Circle of Trust.

Data: Realm, Circle of Trust, error message

Triggers: Execute Delete Circle of Trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_ENTITY

ID: AMCLI-5121

Level: INFO

Description: Attempt to delete metadata.

Data: Realm, Entity ID, protocol specification

Triggers: Execute Delete Metadata Commandline interface.

SUCCEEDED_DELETE_ENTITY

ID: AMCLI-5122

Level: INFO

Description: Deleting Metadata succeeded.

Data: Realm, Entity ID, protocol specification

Triggers: Execute Delete Metadata Commandline interface.

FAILED_DELETE_ENTITY

ID: AMCLI-5123

Level: INFO

Description: Failed to delete metadata.

Data: Realm, Entity ID, protocol specification, error message

Triggers: Execute Delete Metadata Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_EXPORT_ENTITY

ID: AMCLI-5124

Level: INFO

Description: Attempt to export entity.

Data: Realm, Entity ID, Name of file to save the standard metadata XML, Name of file to save the extended metadata XML, protocol specification

Triggers: Execute export entity Commandline interface.

SUCCEEDED_EXPORT_ENTITY

ID: AMCLI-5125

Level: INFO

Description: Exporting entity succeeded.

Data: Realm, Entity ID, Name of file to save the standard metadata XML, Name of file to save the extended metadata XML, protocol specification

Triggers: Execute export entity Commandline interface.

FAILED_EXPORT_ENTITY

ID: AMCLI-5126

Level: INFO

Description: Failed to export entity.

Data: Realm, Entity ID, Name of file to save the standard metadata XML, Name of file to save the extended metadata XML, protocol specification, error message

Triggers: Execute export entity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IMPORT_BULK_FED_DATA

ID: AMCLI-5127

Level: INFO

Description: Attempt to import bulk federation data.

Data: metaAlias for local provider, File name of bulk federation data which is generated by this command, protocol specification

Triggers: Execute import bulk federation data Commandline interface.

SUCCEEDED_IMPORT_BULK_FED_DATA

ID: AMCLI-5128

Level: INFO

Description: Importing bulk federation data succeeded.

Data: metaAlias for local provider, File name of bulk federation data which is generated by this command, protocol specification

Triggers: Execute import bulk federation data Commandline interface.

FAILED_IMPORT_BULK_FED_DATA

ID: AMCLI-5129

Level: INFO

Description: Failed to import bulk federation data.

Data: metaAlias for local provider, File name of bulk federation data which is generated by this command, protocol specification, error message

Triggers: Execute import bulk federation data Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IMPORT_ENTITY

ID: AMCLI-5130

Level: INFO

Description: Attempt to import entity.

Data: Realm where entity resides, file name for the standard metadata to be imported, file name for the extended entity configuration to be imported, name of the Circle of Trust this entity belongs, protocol specification

Triggers: Execute import entity Commandline interface.

SUCCEEDED_IMPORT_ENTITY

ID: AMCLI-5131

Level: INFO

Description: Importing entity succeeded.

Data: Realm where entity resides, file name for the standard metadata to be imported, file name for the extended entity configuration to be imported, name of the Circle of Trust this entity belongs, protocol specification

Triggers: Execute import entity Commandline interface.

FAILED_IMPORT_ENTITY

ID: AMCLI-5132

Level: INFO

Description: Failed to import entity.

Data: Realm where entity resides, file name for the standard metadata to be imported, file name for the extended entity configuration to be imported, name of the Circle of Trust this entity belongs, protocol specification, error message

Triggers: Execute import entity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_COT_MEMBERS

ID: AMCLI-5133

Level: INFO

Description: Attempt to list members in a circle of trust.

Data: Realm, Circle of trust, protocol specification

Triggers: Execute list members in a circle of trust Commandline interface.

SUCCEEDED_LIST_COT_MEMBERS

ID: AMCLI-5134

Level: INFO

Description: Listing members in a circle of trust succeeded.

Data: Realm, Circle of trust, protocol specification

Triggers: Execute list members in a circle of trust Commandline interface.

FAILED_LIST_COT_MEMBERS

ID: AMCLI-5135

Level: INFO

Description: Failed to list members in a circle of trust.

Data: Realm, Circle of trust, protocol specification, error message

Triggers: Execute list members in a circle of trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_COTS

ID: AMCLI-5136

Level: INFO

Description: Attempt to list circles of trust.

Data: realm

Triggers: Execute list circles of trust Commandline interface.

SUCCEEDED_LIST_COTS

ID: AMCLI-5137

Level: INFO

Description: Listing circles of trust succeeded.

Data: realm

Triggers: Execute list circles of trust Commandline interface.

FAILED_LIST_COTS

ID: AMCLI-5138

Level: INFO

Description: Failed to list circles of trust.

Data: realm, error message

Triggers: Execute list circles of trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_ENTITIES

ID: AMCLI-5139

Level: INFO

Description: Attempt to list entities under a realm.

Data: realm, protocol specification

Triggers: Execute list entities under a realm Commandline interface.

SUCCEEDED_LIST_ENTITIES

ID: AMCLI-5140

Level: INFO

Description: Listing entities under a realm succeeded.

Data: realm, protocol specification

Triggers: Execute list entities under a realm Commandline interface.

FAILED_LIST_ENTITIES

ID: AMCLI-5141

Level: INFO

Description: Failed to list entities under a realm.

Data: realm, protocol specification, error message

Triggers: Execute list entities under a realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_COT_MEMBER

ID: AMCLI-5142

Level: INFO

Description: Attempt to remove a member from a circle of trust.

Data: Realm where circle of trust resides, Circle of trust, Entity ID, protocol specification

Triggers: Execute remove a member from a circle of trust Commandline interface.

SUCCEEDED_REMOVE_COT_MEMBER

ID: AMCLI-5143

Level: INFO

Description: Removing a member from a circle of trust successful.

Data: Realm where circle of trust resides, Circle of trust, Entity ID, protocol specification

Triggers: Execute remove a member from a circle of trust Commandline interface.

FAILED_REMOVE_COT_MEMBER

ID: AMCLI-5144

Level: INFO

Description: Failed to remove a member from a circle of trust.

Data: Realm where circle of trust resides, Circle of trust, Entity ID, protocol specification, error message

Triggers: Execute remove a member from a circle of trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_ENTITY_KEYINFO

ID: AMCLI-5145

Level: INFO

Description: Attempt to update XML signing and encryption key information in hosted entity metadata.

Data: Realm, Entity ID, Service provider signing certificate alias, Identity provider signing certificate alias, Service provider encryption certificate alias, Identity provider encryption certificate alias, protocol specification

Triggers: Execute Commandline interface.

SUCCEEDED_UPDATE_ENTITY_KEYINFO

ID: AMCLI-5146

Level: INFO

Description: Updating XML signing and encryption key information in hosted entity metadata succeeded.

Data: Realm, Entity ID, Service provider signing certificate alias, Identity provider signing certificate alias, Service provider encryption certificate alias, Identity provider encryption certificate alias

Triggers: Execute update XML signing and encryption key information in hosted entity metadata Commandline interface.

FAILED_UPDATE_ENTITY_KEYINFO

ID: AMCLI-5147

Level: INFO

Description: Failed to update XML signing and encryption key information in hosted entity metadata.

Data: Realm, Entity ID, Service provider signing certificate alias, Identity provider signing certificate alias, Service provider encryption certificate alias, Identity provider encryption certificate alias, error message

Triggers: Execute update XML signing and encryption key information in hosted entity metadata Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_APPLICATION

ID: AMCLI-5500

Level: INFO

Description: Attempt to create application.

Data: Realm, Application name

Triggers: Execute create application Commandline interface.

SUCCEEDED_CREATE_APPLICATION

ID: AMCLI-5501

Level: INFO

Description: Create application succeeded.

Data: Realm, Application name

Triggers: Execute create application Commandline interface.

FAILED_CREATE_APPLICATION

ID: AMCLI-5502

Level: INFO

Description: Failed to create application.

Data: Realm, Application name, error message

Triggers: Execute create application Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_APPLICATIONS

ID: AMCLI-5510

Level: INFO

Description: Attempt to list applications in a realm.

Data: Realm

Triggers: Execute list applications Commandline interface.

SUCCEEDED_LIST_APPLICATIONS

ID: AMCLI-5511

Level: INFO

Description: List applications in a realm succeeded.

Data: Realm

Triggers: Execute list applications Commandline interface.

FAILED_LIST_APPLICATIONS

ID: AMCLI-5512

Level: INFO

Description: Failed to list applications.

Data: Realm, error message

Triggers: Execute list applications Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_APPLICATION_TYPES

ID: AMCLI-5520

Level: INFO

Description: Attempt to list application types.

Triggers: Execute list application types Commandline interface.

SUCCEEDED_LIST_APPLICATION_TYPES

ID: AMCLI-5521

Level: INFO

Description: List application types succeeded.

Triggers: Execute list application types Commandline interface.

FAILED_LIST_APPLICATION_TYPES

ID: AMCLI-5522

Level: INFO

Description: Failed to list application types.

Data: error message

Triggers: Execute list application types Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_APPLICATION

ID: AMCLI-5530

Level: INFO

Description: Attempt to show application attributes.

Data: Realm, Application Name

Triggers: Execute show application Commandline interface.

SUCCEEDED_SHOW_APPLICATION

ID: AMCLI-5531

Level: INFO

Description: Attributes of application is displayed succeeded.

Data: Realm, Application Name

Triggers: Execute show application Commandline interface.

FAILED_SHOW_APPLICATION

ID: AMCLI-5532

Level: INFO

Description: Failed to show application attributes.

Data: Realm, Application Name, error message

Triggers: Execute show application Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_APPLICATION

ID: AMCLI-5540

Level: INFO

Description: Attempt to set application attributes.

Data: Realm, Application Name

Triggers: Execute set application attributes Commandline interface.

SUCCEEDED_SET_APPLICATION

ID: AMCLI-5541

Level: INFO

Description: Attributes of application is modified succeeded.

Data: Realm, Application Name

Triggers: Execute set application attributes Commandline interface.

FAILED_SET_APPLICATION

ID: AMCLI-5542

Level: INFO

Description: Failed to set application attributes.

Data: Realm, Application Name, error message

Triggers: Execute set application attributes Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_APPLICATIONS

ID: AMCLI-5550

Level: INFO

Description: Attempt to delete applications.

Data: Realm

Triggers: Execute delete applications Commandline interface.

SUCCEEDED_DELETE_APPLICATIONS

ID: AMCLI-5551

Level: INFO

Description: Application are deleted.

Data: Realm

Triggers: Execute delete applications Commandline interface.

FAILED_DELETE_APPLICATIONS

ID: AMCLI-5552

Level: INFO

Description: Failed to delete applications.

Data: Realm, error message

Triggers: Execute delete applications Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_APPLICATION_TYPE

ID: AMCLI-5553

Level: INFO

Description: Attempt to show application type details.

Data: Application Type name

Triggers: Execute show application type Commandline interface.

SUCCEEDED_SHOW_APPLICATION_TYPE

ID: AMCLI-5554

Level: INFO

Description: Show application type details succeded.

Data: Application Type name

Triggers: Execute show application type Commandline interface.

ATTEMPT_DELETE_APPLICATION_TYPES

ID: AMCLI-5555

Level: INFO

Description: Attempt to delete application types.

Data: Application Type names

Triggers: Execute delete application types Commandline interface.

SUCCEEDED_DELETE_APPLICATION_TYPES

ID: AMCLI-5556

Level: INFO

Description: Delete application types succeeded.

Data: Application Type names

Triggers: Execute delete application types Commandline interface.

FAILED_DELETE_APPLICATION_TYPES

ID: AMCLI-5557

Level: INFO

Description: Delete application types failed.

Data: Application Type names, error message

Triggers: Execute delete application types Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_APPLICATION_TYPE

ID: AMCLI-5558

Level: INFO

Description: Attempt to create application type.

Data: Application Type name

Triggers: Execute create application type Commandline interface.

SUCCEEDED_CREATE_APPLICATION_TYPE

ID: AMCLI-5559

Level: INFO

Description: Create application type succeeded.

Data: Application Type name

Triggers: Execute create application type Commandline interface.

FAILED_CREATE_APPLICATION_TYPE

ID: AMCLI-5560

Level: INFO

Description: Failed to create application type.

Data: Application Type name, error message

Triggers: Execute create application type Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_ENTITLEMENT_SVC

ID: AMCLI-5600

Level: INFO

Description: Attempt to show entitlement service configuration.

Triggers: Execute show entitlement service configuration Commandline interface.

SUCCEEDED_SHOW_ENTITLEMENT_SVC

ID: AMCLI-5601

Level: INFO

Description: Entitlement service configuration is displayed.

Triggers: Execute show entitlement service configuration Commandline interface.

FAILED_SHOW_ENTITLEMENT_SVC

ID: AMCLI-5602

Level: INFO

Description: Failed to display entitlement service configuration.

Data: error message

Triggers: Execute show entitlement service configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ENTITLEMENT_SVC

ID: AMCLI-5610

Level: INFO

Description: Attempt to modify entitlement service configuration.

Triggers: Execute set entitlement service configuration Commandline interface.

SUCCEEDED_MODIFY_ENTITLEMENT_SVC

ID: AMCLI-5611

Level: INFO

Description: Entitlement service configuration is modified.

Triggers: Execute set entitlement service configuration Commandline interface.

FAILED_MODIFY_ENTITLEMENT_SVC

ID: AMCLI-5612

Level: INFO

Description: Failed to modify entitlement service configuration.

Data: error message

Triggers: Execute set entitlement service configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_APPLICATION_PRIVILEGE

ID: AMCLI-6010

Level: INFO

Description: Attempt to create application privilege.

Data: realm, application privilege name

Triggers: Execute create application privilege Commandline interface.

SUCCEEDED_CREATE_APPLICATION_PRIVILEGE

ID: AMCLI-6011

Level: INFO

Description: Application privilege is created.

Data: realm, application privilege name

Triggers: Execute create application privilege Commandline interface.

FAILED_CREATE_APPLICATION_PRIVILEGE

ID: AMCLI-6012

Level: INFO

Description: Failed to create application privilege.

Data: realm, application privilege name, error message

Triggers: Execute create application privilege Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_APPLICATION_PRIVILEGE

ID: AMCLI-6020

Level: INFO

Description: Attempt to delete application privilege.

Data: realm, application privilege name

Triggers: Execute delete application privilege Commandline interface.

SUCCEEDED_DELETE_APPLICATION_PRIVILEGE

ID: AMCLI-6021

Level: INFO

Description: Application privilege is deleted.

Data: realm, application privilege name

Triggers: Execute delete application privilege Commandline interface.

FAILED_DELETE_APPLICATION_PRIVILEGE

ID: AMCLI-6022

Level: INFO

Description: Failed to delete application privilege.

Data: realm, application privilege name, error message

Triggers: Execute delete application privilege Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_APPLICATION_PRIVILEGE

ID: AMCLI-6020

Level: INFO

Description: Attempt to show application privilege.

Data: realm, application privilege name

Triggers: Execute show application privilege Commandline interface.

SUCCEEDED_SHOW_APPLICATION_PRIVILEGE

ID: AMCLI-6021

Level: INFO

Description: Application privilege is displayed.

Data: realm, application privilege name

Triggers: Execute show application privilege Commandline interface.

FAILED_SHOW_APPLICATION_PRIVILEGE

ID: AMCLI-6022

Level: INFO

Description: Failed to show application privilege.

Data: realm, application privilege name, error message

Triggers: Execute show application privilege Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_APPLICATION_PRIVILEGES

ID: AMCLI-6030

Level: INFO

Description: Attempt to list application privileges in a realm.

Data: realm

Triggers: Execute list application privileges Commandline interface.

SUCCEEDED_LIST_APPLICATION_PRIVILEGES

ID: AMCLI-6031

Level: INFO

Description: Application privileges are displayed.

Data: realm

Triggers: Execute list application privileges Commandline interface.

FAILED_LIST_APPLICATION_PRIVILEGES

ID: AMCLI-6032

Level: INFO

Description: Failed to list application privileges.

Data: realm, error message

Triggers: Execute list application privileges Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_APPLICATION_PRIVILEGE

ID: AMCLI-6040

Level: INFO

Description: Attempt to update application privilege.

Data: realm, application privilege name

Triggers: Execute update application privilege Commandline interface.

SUCCEEDED_UPDATE_APPLICATION_PRIVILEGE

ID: AMCLI-6041

Level: INFO

Description: Application privilege is updated.

Data: realm, application privilege name

Triggers: Execute update application privilege Commandline interface.

FAILED_UPDATE_APPLICATION_PRIVILEGE

ID: AMCLI-6042

Level: INFO

Description: Failed to update application privilege.

Data: realm, application privilege name, error message

Triggers: Execute update application privileges Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_PLUGIN_SCHEMA

ID: AMCLI-6043

Level: INFO

Description: Attempt to add Plug-in schema.

Data: name of service, name of interface, name of plugin, name of i18n key, name of i18n name, name of class

Triggers: Execute add Plug-in schema Commandline interface.

SUCCEED_ADD_PLUGIN_SCHEMA

ID: AMCLI-6044

Level: INFO

Description: Added Plug-in schema.

Data: name of service, name of plugin

Triggers: Execute add Plug-in schema Commandline interface.

FAILED_ADD_PLUGIN_SCHEMA

ID: AMCLI-6045

Level: INFO

Description: Failed to add Plug-in schema.

Data: name of service, name of plugin, error message

Triggers: Execute add Plug-in schema Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_PLUGIN_SCHEMA

ID: AMCLI-6046

Level: INFO

Description: Attempt to remove Plug-in schema.

Data: name of service, name of interface, name of plugin, name of i18n key, name of i18n name, name of class

Triggers: Execute remove Plug-in schema Commandline interface.

SUCCEED_REMOVE_PLUGIN_SCHEMA

ID: AMCLI-6047

Level: INFO

Description: Removed Plug-in schema.

Data: name of service, name of plugin

Triggers: Execute remove Plug-in schema Commandline interface.

FAILED_REMOVE_PLUGIN_SCHEMA

ID: AMCLI-6048

Level: INFO

Description: Failed to remove Plug-in schema.

Data: name of service, name of plugin, error message

Triggers: Execute remove Plug-in schema Commandline interface.

Actions: Look under debug file for more information.

SUCCEED_SET_SITE_ID

ID: AMCLI-6049

Level: INFO

Description: Site ID is set.

Data: name of site, id of site

Triggers: Execute set site ID Commandline interface.

SUCCEED_SET_SITE_ID

ID: AMCLI-6050

Level: INFO

Description: Unable to set site ID.

Data: name of site, site ID, error message

Triggers: Execute set site ID Commandline interface.

Actions: Look under debug file for more information.

OpenAM logs the following CONSOLE messages.

ATTEMPT_IDENTITY_CREATION

ID: CONSOLE-1

Level: INFO

Description: Attempt to create Identity

Data: identity name, identity type, realm name

Triggers: Click on create button in Realm Creation Page.

IDENTITY_CREATED

ID: CONSOLE-2

Level: INFO

Description: Creation of Identity succeeded.

Data: identity name, identity type, realm name

Triggers: Click on create button in Realm Creation Page.

SSO_EXCEPTION_IDENTITY_CREATION

ID: CONSOLE-3

Level: SEVERE

Description: Creation of Identity failed

Data: identity name, identity type, realm name, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_IDENTITY_CREATION

ID: CONSOLE-4

Level: SEVERE

Description: Creation of Identity failed

Data: identity name, identity type, realm name, error message

Triggers: Unable to create an identity under a realm due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_SEARCH_IDENTITY

ID: CONSOLE-11

Level: INFO

Description: Attempt to search for Identities

Data: base realm, identity type, search pattern, search size limit, search time limit

Triggers: Click on Search button in identity search view.

SUCCEED_SEARCH_IDENTITY

ID: CONSOLE-12

Level: INFO

Description: Searching for Identities succeeded

Data: base realm, identity type, search pattern, search size limit, search time limit

Triggers: Click on Search button in identity search view.

SSO_EXCEPTION_SEARCH_IDENTITY

ID: CONSOLE-13

Level: SEVERE

Description: Searching for identities failed

Data: identity name, identity type, realm name, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_SEARCH_IDENTITY

ID: CONSOLE-14

Level: SEVERE

Description: Searching for identities failed

Data: identity name, identity type, realm name, error message

Triggers: Unable to perform search operation on identities under a realm due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-21

Level: INFO

Description: Attempt to read attribute values of an identity

Data: identity name, name of attributes

Triggers: View identity profile view.

SUCCEED_READ_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-22

Level: INFO

Description: Reading of attribute values of an identity succeeded

Data: identity name, name of attributes

Triggers: View identity profile view.

SSO_EXCEPTION_READ_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-23

Level: SEVERE

Description: Reading of attribute values of an identity failed

Data: identity name, name of attributes, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_READ_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-24

Level: SEVERE

Description: Reading of attribute values of an identity failed

Data: identity name, name of attributes, error message

Triggers: Unable to read attribute values of an identity due to data store error.

Actions: Look under data store log for more information.

SMS_EXCEPTION_READ_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-25

Level: SEVERE

Description: Reading of attribute values of an identity failed

Data: identity name, name of attributes, error message

Triggers: Unable to read attribute values of an identity due to exception service manager API.

Actions: Look under service manage log for more information.

ATTEMPT_MODIFY_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-31

Level: INFO

Description: Attempt to modify attribute values of an identity

Data: identity name, name of attributes

Triggers: Click on Save button in identity profile view.

SUCCEED_MODIFY_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-32

Level: INFO

Description: Modification of attribute values of an identity succeeded

Data: identity name, name of attributes

Triggers: Click on Save button in identity profile view.

SSO_EXCEPTION_MODIFY_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-33

Level: SEVERE

Description: Modification of attribute values of an identity failed

Data: identity name, name of attributes, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_MODIFY_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-34

Level: SEVERE

Description: Modification of attribute values of an identity failed

Data: identity name, name of attributes, error message

Triggers: Unable to modify attribute values of an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_DELETE_IDENTITY

ID: CONSOLE-41

Level: INFO

Description: Attempt to delete identities

Data: realm name, name of identities to be deleted

Triggers: Click on Delete button in identity search view.

SUCCEED_DELETE_IDENTITY

ID: CONSOLE-42

Level: INFO

Description: Deletion of identities succeeded

Data: realm name, name of identities to be deleted

Triggers: Click on Delete button in identity search view.

SSO_EXCEPTION_DELETE_IDENTITY

ID: CONSOLE-43

Level: SEVERE

Description: Deletion of identities failed

Data: realm name, name of identities to be deleted, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_DELETE_IDENTITY

ID: CONSOLE-44

Level: SEVERE

Description: Deletion of identities failed

Data: realm name, name of identities to be deleted, error message

Triggers: Unable to delete identities due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_IDENTITY_MEMBERSHIP

ID: CONSOLE-51

Level: INFO

Description: Attempt to read identity's memberships information

Data: name of identity, membership identity type

Triggers: View membership page of an identity.

SUCCEED_READ_IDENTITY_MEMBERSHIP

ID: CONSOLE-52

Level: INFO

Description: Reading of identity's memberships information succeeded

Data: name of identity, membership identity type

Triggers: View membership page of an identity.

SSO_EXCEPTION_READ_IDENTITY_MEMBERSHIP

ID: CONSOLE-53

Level: SEVERE

Description: Reading of identity's memberships information failed.

Data: name of identity, membership identity type, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_READ_IDENTITY_MEMBERSHIP

ID: CONSOLE-54

Level: SEVERE

Description: Reading of identity's memberships information failed.

Data: name of identity, membership identity type, error message

Triggers: Unable to read identity's memberships information due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_IDENTITY_MEMBER

ID: CONSOLE-61

Level: INFO

Description: Attempt to read identity's members information

Data: name of identity, members identity type

Triggers: View members page of an identity.

SUCCEED_READ_IDENTITY_MEMBER

ID: CONSOLE-62

Level: INFO

Description: Reading of identity's members information succeeded

Data: name of identity, members identity type

Triggers: View members page of an identity.

SSO_EXCEPTION_READ_IDENTITY_MEMBER

ID: CONSOLE-63

Level: SEVERE

Description: Reading of identity's members information failed.

Data: name of identity, member identity type, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_READ_IDENTITY_MEMBER

ID: CONSOLE-64

Level: SEVERE

Description: Reading of identity's members information failed.

Data: name of identity, member identity type, error message

Triggers: Unable to read identity's members information due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_ADD_IDENTITY_MEMBER

ID: CONSOLE-71

Level: INFO

Description: Attempt to add member to an identity

Data: name of identity, name of identity to be added.

Triggers: Select members to be added to an identity.

SUCCEED_ADD_IDENTITY_MEMBER

ID: CONSOLE-72

Level: INFO

Description: Addition of member to an identity succeeded

Data: name of identity, name of identity added.

Triggers: Select members to be added to an identity.

SSO_EXCEPTION_ADD_IDENTITY_MEMBER

ID: CONSOLE-73

Level: SEVERE

Description: Addition of member to an identity failed.

Data: name of identity, name of identity to be added., error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_ADD_IDENTITY_MEMBER

ID: CONSOLE-74

Level: SEVERE

Description: Addition of member to an identity failed.

Data: name of identity, name of identity to be added., error message

Triggers: Unable to add member to an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_REMOVE_IDENTITY_MEMBER

ID: CONSOLE-81

Level: INFO

Description: Attempt to remove member from an identity

Data: name of identity, name of identity to be removed.

Triggers: Select members to be removed from an identity.

SUCCEED_REMOVE_IDENTITY_MEMBER

ID: CONSOLE-82

Level: INFO

Description: Removal of member from an identity succeeded

Data: name of identity, name of identity removed.

Triggers: Select members to be removed from an identity.

SSO_EXCEPTION_REMOVE_IDENTITY_MEMBER

ID: CONSOLE-83

Level: SEVERE

Description: Removal of member to an identity failed.

Data: name of identity, name of identity to be removed., error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_REMOVE_IDENTITY_MEMBER

ID: CONSOLE-84

Level: SEVERE

Description: Removal of member from an identity failed.

Data: name of identity, name of identity to be removed., error message

Triggers: Unable to remove member to an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_IDENTITY_ASSIGNED_SERVICE

ID: CONSOLE-91

Level: INFO

Description: Attempt to read assigned service names of an identity

Data: name of identity

Triggers: Click on Add button in service assignment view of an identity.

SUCCEED_READ_IDENTITY_ASSIGNED_SERVICE

ID: CONSOLE-92

Level: INFO

Description: Reading assigned service names of an identity succeeded

Data: name of identity

Triggers: Click on Add button in service assignment view of an identity.

SSO_EXCEPTION_READ_IDENTITY_ASSIGNED_SERVICE

ID: CONSOLE-93

Level: SEVERE

Description: Reading assigned service names of an identity failed.

Data: name of identity, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_READ_IDENTITY_ASSIGNED_SERVICE

ID: CONSOLE-94

Level: SEVERE

Description: Reading assigned service names of an identity failed.

Data: name of identity, error message

Triggers: Unable to read assigned service names of an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_IDENTITY_ASSIGNABLE_SERVICE

ID: CONSOLE-101

Level: INFO

Description: Attempt to read assignable service names of an identity

Data: name of identity

Triggers: View the services page of an identity.

SUCCEED_READ_IDENTITY_ASSIGNABLE_SERVICE

ID: CONSOLE-102

Level: INFO

Description: Reading assignable service names of an identity succeeded

Data: name of identity

Triggers: View the services page of an identity.

SSO_EXCEPTION_READ_IDENTITY_ASSIGNABLE_SERVICE

ID: CONSOLE-103

Level: SEVERE

Description: Reading assignable service names of an identity failed.

Data: name of identity, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_READ_IDENTITY_ASSIGNABLE_SERVICE

ID: CONSOLE-104

Level: SEVERE

Description: Reading assignable service names of an identity failed.

Data: name of identity, error message

Triggers: Unable to read assignable service names of an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_IDENTITY_ASSIGN_SERVICE

ID: CONSOLE-111

Level: INFO

Description: Attempt to assign a service to an identity

Data: name of identity, name of service

Triggers: Click Add button of service view of an identity.

SUCCEED_IDENTITY_ASSIGN_SERVICE

ID: CONSOLE-112

Level: INFO

Description: Assignment of service to an identity succeeded

Data: name of identity, name of service

Triggers: Click Add button of service view of an identity.

SSO_EXCEPTION_IDENTITY_ASSIGN_SERVICE

ID: CONSOLE-113

Level: SEVERE

Description: Assignment of service to an identity failed.

Data: name of identity, name of service, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_IDENTITY_ASSIGN_SERVICE

ID: CONSOLE-114

Level: SEVERE

Description: Assignment of service to an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to assign service to an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_IDENTITY_UNASSIGN_SERVICE

ID: CONSOLE-121

Level: INFO

Description: Attempt to unassign a service from an identity

Data: name of identity, name of service

Triggers: Click Remove button in service view of an identity.

SUCCEED_IDENTITY_UNASSIGN_SERVICE

ID: CONSOLE-122

Level: INFO

Description: Unassignment of service to an identity succeeded

Data: name of identity, name of service

Triggers: Click Remove button in service view of an identity.

SSO_EXCEPTION_IDENTITY_UNASSIGN_SERVICE

ID: CONSOLE-123

Level: SEVERE

Description: Unassignment of service from an identity failed.

Data: name of identity, name of service, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_IDENTITY_UNASSIGN_SERVICE

ID: CONSOLE-124

Level: SEVERE

Description: Unassignment of service from an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to unassign service from an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_IDENTITY_READ_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-131

Level: INFO

Description: Attempt to read service attribute values of an identity

Data: name of identity, name of service

Triggers: View service profile view of an identity.

SUCCEED_IDENTITY_READ_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-132

Level: INFO

Description: Reading of service attribute values of an identity succeeded

Data: name of identity, name of service

Triggers: View service profile view of an identity.

SSO_EXCEPTION_IDENTITY_READ_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-133

Level: SEVERE

Description: Reading of service attribute values of an identity failed.

Data: name of identity, name of service, error message

Triggers: 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

Actions: Look under data store log for more information.

IDM_EXCEPTION_IDENTITY_READ_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-134

Level: SEVERE

Description: Reading of service attribute values of an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to read service attribute values of an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_IDENTITY_WRITE_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-141

Level: INFO

Description: Attempt to write service attribute values to an identity

Data: name of identity, name of service

Triggers: Click on Save button in service profile view of an identity.

SUCCEED_IDENTITY_WRITE_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-142

Level: INFO

Description: Writing of service attribute values to an identity succeeded

Data: name of identity, name of service

Triggers: Click on Save button in service profile view of an identity.

SSO_EXCEPTION_IDENTITY_WRITE_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-143

Level: SEVERE

Description: Writing of service attribute values to an identity failed.

Data: name of identity, name of service, error message

Triggers: 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.

Actions: Look under data store log for more information.

IDM_EXCEPTION_IDENTITY_WRITE_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-144

Level: SEVERE

Description: Writing of service attribute values to an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to write service attribute values to an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_ALL_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-201

Level: INFO

Description: Attempt to read all global service default attribute values

Data: name of service

Triggers: View global configuration view of a service.

SUCCEED_READ_ALL_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-202

Level: INFO

Description: Reading of all global service default attribute values succeeded

Data: name of service

Triggers: View global configuration view of a service.

ATTEMPT_READ_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-203

Level: INFO

Description: Attempt to read global service default attribute values

Data: name of service, name of attribute

Triggers: View global configuration view of a service.

SUCCEED_READ_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-204

Level: INFO

Description: Reading of global service default attribute values succeeded

Data: name of service, name of attribute

Triggers: View global configuration view of a service.

FAILED_READ_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-205

Level: INFO

Description: Reading of global service default attribute values failed

Data: name of service, name of attribute

Triggers: View global configuration view of a service.

Actions: Look under service management log for more information.

ATTEMPT_WRITE_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-211

Level: INFO

Description: Attempt to write global service default attribute values

Data: name of service, name of attribute

Triggers: Click on Save button in global configuration view of a service.

SUCCEED_WRITE_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-212

Level: INFO

Description: Writing of global service default attribute values succeeded

Data: name of service, name of attribute

Triggers: Click on Save button in global configuration view of a service.

SSO_EXCEPTION_WRITE_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-213

Level: SEVERE

Description: Writing of global service default attribute values failed.

Data: name of service, name of attribute, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_WRITE_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-214

Level: SEVERE

Description: Writing of global service default attribute values failed.

Data: name of service, name of attribute, error message

Triggers: Unable to write service default attribute values due to service management error.

Actions: Look under service management log for more information.

ATTEMPT_READ_GLOBAL_SUB_CONFIGURATION_NAMES

ID: CONSOLE-221

Level: INFO

Description: Attempt to get sub configuration names

Data: name of service, name of base global sub configuration

Triggers: View a global service view of which its service has sub schema.

SUCCEED_READ_GLOBAL_SUB_CONFIGURATION_NAMES

ID: CONSOLE-222

Level: INFO

Description: Reading of global sub configuration names succeeded

Data: name of service, name of base global sub configuration

Triggers: View a global service view of which its service has sub schema.

SSO_EXCEPTION_READ_GLOBAL_SUB_CONFIGURATION_NAMES

ID: CONSOLE-223

Level: SEVERE

Description: Reading of global sub configuration names failed.

Data: name of service, name of base global sub configuration, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_READ_GLOBAL_SUB_CONFIGURATION_NAMES

ID: CONSOLE-224

Level: SEVERE

Description: Reading of global sub configuration names failed.

Data: name of service, name of base global sub configuration, error message

Triggers: Unable to get global sub configuration names due to service management error.

Actions: Look under service management log for more information.

ATTEMPT_DELETE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-231

Level: INFO

Description: Attempt to delete sub configuration

Data: name of service, name of base global sub configuration, name of sub configuration to be deleted

Triggers: Click on delete selected button in global service profile view.

SUCCEED_DELETE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-232

Level: INFO

Description: Deletion of sub configuration succeeded

Data: name of service, name of base global sub configuration, name of sub configuration to be deleted

Triggers: Click on delete selected button in global service profile view.

SSO_EXCEPTION_DELETE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-233

Level: SEVERE

Description: Deletion of sub configuration failed.

Data: name of service, name of base global sub configuration, name of sub configuration to be deleted, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_DELETE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-234

Level: SEVERE

Description: Deletion of sub configuration failed.

Data: name of service, name of base global sub configuration, name of sub configuration to be deleted, error message

Triggers: Unable to delete sub configuration due to service management error.

Actions: Look under service management log for more information.

ATTEMPT_CREATE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-241

Level: INFO

Description: Attempt to create sub configuration

Data: name of service, name of base global sub configuration, name of sub configuration to be created, name of sub schema to be created

Triggers: Click on add button in create sub configuration view.

SUCCEED_CREATE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-242

Level: INFO

Description: Creation of sub configuration succeeded

Data: name of service, name of base global sub configuration, name of sub configuration to be created, name of sub schema to be created

Triggers: Click on add button in create sub configuration view.

SSO_EXCEPTION_CREATE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-243

Level: SEVERE

Description: Creation of sub configuration failed.

Data: 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

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_CREATE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-244

Level: SEVERE

Description: Creation of sub configuration failed.

Data: 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

Triggers: Unable to create sub configuration due to service management error.

Actions: Look under service management log for more information.

SUCCEED_READ_GLOBAL_SUB_CONFIGURATION_ATTRIBUTE_VALUES

ID: CONSOLE-251

Level: INFO

Description: Reading of sub configuration's attribute values succeeded

Data: name of service, name of sub configuration

Triggers: View sub configuration profile view.

ATTEMPT_WRITE_GLOBAL_SUB_CONFIGURATION_ATTRIBUTE_VALUES

ID: CONSOLE-261

Level: INFO

Description: Attempt to write sub configuration's attribute values

Data: name of service, name of sub configuration

Triggers: Click on save button in sub configuration profile view.

SUCCEED_WRITE_GLOBAL_SUB_CONFIGURATION_ATTRIBUTE_VALUES

ID: CONSOLE-262

Level: INFO

Description: Writing of sub configuration's attribute values succeeded

Data: name of service, name of sub configuration

Triggers: Click on save button in sub configuration profile view.

SSO_EXCEPTION_WRITE_GLOBAL_SUB_CONFIGURATION_ATTRIBUTE_VALUES

ID: CONSOLE-263

Level: SEVERE

Description: Writing of sub configuration's attribute value failed.

Data: name of service, name of sub configuration, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_WRITE_GLOBAL_SUB_CONFIGURATION_ATTRIBUTE_VALUES_NAMES

ID: CONSOLE-264

Level: SEVERE

Description: Writing of sub configuration's attribute value failed.

Data: name of service, name of sub configuration, error message

Triggers: Unable to write sub configuration's attribute value due to service management error.

Actions: Look under service management log for more information.

ATTEMPT_GET_POLICY_NAMES

ID: CONSOLE-301

Level: INFO

Description: Attempt to get policy names under a realm.

Data: name of realm

Triggers: View policy main page.

SUCCEED_GET_POLICY_NAMES

ID: CONSOLE-302

Level: INFO

Description: Getting policy names under a realm succeeded

Data: name of realm

Triggers: View policy main page.

SSO_EXCEPTION_GET_POLICY_NAMES

ID: CONSOLE-303

Level: SEVERE

Description: Getting policy names under a realm failed.

Data: name of realm, error message

Triggers: 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.

Actions: Look under policy log for more information.

POLICY_EXCEPTION_GET_POLICY_NAMES

ID: CONSOLE-304

Level: SEVERE

Description: Getting policy names under a realm failed.

Data: name of realm, error message

Triggers: Unable to get policy names under a realm due to policy SDK related errors.

Actions: Look under policy log for more information.

ATTEMPT_CREATE_POLICY

ID: CONSOLE-311

Level: INFO

Description: Attempt to create policy under a realm.

Data: name of realm, name of policy

Triggers: Click on New button in policy creation page.

SUCCEED_CREATE_POLICY

ID: CONSOLE-312

Level: INFO

Description: Creation of policy succeeded

Data: name of realm, name of policy

Triggers: Click on New button in policy creation page.

SSO_EXCEPTION_CREATE_POLICY

ID: CONSOLE-313

Level: SEVERE

Description: Creation of policy failed.

Data: name of realm, name of policy, error message

Triggers: 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.

Actions: Look under policy log for more information.

POLICY_EXCEPTION_CREATE_POLICY

ID: CONSOLE-314

Level: SEVERE

Description: Creation of policy failed.

Data: name of realm, name of policy, error message

Triggers: Unable to create policy under a realm due to policy SDK related errors.

Actions: Look under policy log for more information.

ATTEMPT_MODIFY_POLICY

ID: CONSOLE-321

Level: INFO

Description: Attempt to modify policy.

Data: name of realm, name of policy

Triggers: Click on Save button in policy profile page.

SUCCEED_MODIFY_POLICY

ID: CONSOLE-322

Level: INFO

Description: Modification of policy succeeded

Data: name of realm, name of policy

Triggers: Click on Save button in policy profile page.

SSO_EXCEPTION_MODIFY_POLICY

ID: CONSOLE-323

Level: SEVERE

Description: Modification of policy failed.

Data: name of realm, name of policy, error message

Triggers: 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.

Actions: Look under policy log for more information.

POLICY_EXCEPTION_MODIFY_POLICY

ID: CONSOLE-324

Level: SEVERE

Description: Modification of policy failed.

Data: name of realm, name of policy, error message

Triggers: Unable to modify policy due to policy SDK related errors.

Actions: Look under policy log for more information.

ATTEMPT_DELETE_POLICY

ID: CONSOLE-331

Level: INFO

Description: Attempt to delete policy.

Data: name of realm, names of policies

Triggers: Click on Delete button in policy main page.

SUCCEED_DELETE_POLICY

ID: CONSOLE-332

Level: INFO

Description: Deletion of policy succeeded

Data: name of realm, name of policies

Triggers: Click on Delete button in policy main page.

SSO_EXCEPTION_DELETE_POLICY

ID: CONSOLE-333

Level: SEVERE

Description: Deletion of policy failed.

Data: name of realm, name of policies, error message

Triggers: 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.

Actions: Look under policy log for more information.

POLICY_EXCEPTION_DELETE_POLICY

ID: CONSOLE-334

Level: SEVERE

Description: Deletion of policy failed.

Data: name of realm, name of policies, error message

Triggers: Unable to delete policy due to policy SDK related errors.

Actions: Look under policy log for more information.

ATTEMPT_GET_REALM_NAMES

ID: CONSOLE-401

Level: INFO

Description: Attempt to get realm names

Data: name of parent realm

Triggers: View realm main page.

SUCCEED_GET_REALM_NAMES

ID: CONSOLE-402

Level: INFO

Description: Getting realm names succeeded.

Data: name of parent realm

Triggers: View realm main page.

SMS_EXCEPTION_GET_REALM_NAMES

ID: CONSOLE-403

Level: SEVERE

Description: Getting realm names failed.

Data: name of parent realm, error message

Triggers: Unable to get realm names due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_CREATE_REALM

ID: CONSOLE-411

Level: INFO

Description: Attempt to create realm

Data: name of parent realm, name of new realm

Triggers: Click on New button in create realm page.

SUCCEED_CREATE_REALM

ID: CONSOLE-412

Level: INFO

Description: Creation of realm succeeded.

Data: name of parent realm, name of new realm

Triggers: Click on New button in create realm page.

SMS_EXCEPTION_CREATE_REALM

ID: CONSOLE-413

Level: SEVERE

Description: Creation of realm failed.

Data: name of parent realm, name of new realm, error message

Triggers: Unable to create new realm due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_DELETE_REALM

ID: CONSOLE-421

Level: INFO

Description: Attempt to delete realm

Data: name of parent realm, name of realm to delete

Triggers: Click on Delete button in realm main page.

SUCCEED_DELETE_REALM

ID: CONSOLE-422

Level: INFO

Description: Deletion of realm succeeded.

Data: name of parent realm, name of realm to delete

Triggers: Click on Delete button in realm main page.

SMS_EXCEPTION_DELETE_REALM

ID: CONSOLE-423

Level: SEVERE

Description: Deletion of realm failed.

Data: name of parent realm, name of realm to delete, error message

Triggers: Unable to delete realm due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_ATTR_VALUES_OF_REALM

ID: CONSOLE-431

Level: INFO

Description: Attempt to get attribute values of realm

Data: name of realm

Triggers: View realm profile page.

SUCCEED_GET_ATTR_VALUES_OF_REALM

ID: CONSOLE-432

Level: INFO

Description: Getting attribute values of realm succeeded.

Data: name of realm

Triggers: View realm profile page.

SMS_EXCEPTION_GET_ATTR_VALUES_OF_REALM

ID: CONSOLE-433

Level: SEVERE

Description: Getting attribute values of realm failed.

Data: name of realm, error message

Triggers: Unable to get attribute values of realm due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_SET_ATTR_VALUES_OF_REALM

ID: CONSOLE-441

Level: INFO

Description: Attempt to modify realm's profile

Data: name of realm

Triggers: Click on Save button in realm profile page.

SUCCEED_SET_ATTR_VALUES_OF_REALM

ID: CONSOLE-442

Level: INFO

Description: Modification of realm's profile succeeded.

Data: name of realm

Triggers: Click on Save button in realm profile page.

SMS_EXCEPTION_SET_ATTR_VALUES_OF_REALM

ID: CONSOLE-443

Level: SEVERE

Description: Modification of realm's profile failed.

Data: name of realm, error message

Triggers: Unable to modify realm's profile due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_DELEGATION_SUBJECTS

ID: CONSOLE-501

Level: INFO

Description: Attempt to get delegation subjects under a realm

Data: name of realm, search pattern

Triggers: View delegation main page.

SUCCEED_GET_DELEGATION_SUBJECTS

ID: CONSOLE-502

Level: INFO

Description: Getting delegation subjects under a realm succeeded.

Data: name of realm, search pattern

Triggers: View delegation main page.

SSO_EXCEPTION_GET_DELEGATION_SUBJECTS

ID: CONSOLE-503

Level: SEVERE

Description: Getting delegation subjects under a realm failed.

Data: name of realm, search pattern, error message

Triggers: 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.

Actions: Look under delegation management log for more information.

DELEGATION_EXCEPTION_GET_DELEGATION_SUBJECTS

ID: CONSOLE-504

Level: SEVERE

Description: Getting delegation subjects under a realm failed.

Data: name of realm, search pattern, error message

Triggers: Unable to get delegation subjects due to delegation management SDK related errors.

Actions: Look under delegation management log for more information.

ATTEMPT_GET_PRIVILEGES_OF_DELEGATION_SUBJECT

ID: CONSOLE-511

Level: INFO

Description: Attempt to get privileges of delegation subject

Data: name of realm, ID of delegation subject

Triggers: View delegation subject profile page.

SUCCEED_GET_PRIVILEGES_OF_DELEGATION_SUBJECT

ID: CONSOLE-512

Level: INFO

Description: Getting privileges of delegation subject succeeded.

Data: name of realm, ID of delegation subject

Triggers: View delegation subject profile page.

SSO_EXCEPTION_GET_PRIVILEGES_OF_DELEGATION_SUBJECT

ID: CONSOLE-513

Level: SEVERE

Description: Getting privileges of delegation subject failed.

Data: name of realm, ID of delegation subject, error message

Triggers: 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.

Actions: Look under delegation management log for more information.

DELEGATION_EXCEPTION_GET_PRIVILEGES_OF_DELEGATION_SUBJECT

ID: CONSOLE-514

Level: SEVERE

Description: Getting privileges of delegation subject failed.

Data: name of realm, ID of delegation subject, error message

Triggers: Unable to get privileges of delegation subject due to delegation management SDK related errors.

Actions: Look under delegation management log for more information.

ATTEMPT_MODIFY_DELEGATION_PRIVILEGE

ID: CONSOLE-521

Level: INFO

Description: Attempt to modify delegation privilege

Data: name of realm, ID of delegation privilege, ID of subject

Triggers: Click on Save button in delegation subject profile page.

SUCCEED_MODIFY_DELEGATION_PRIVILEGE

ID: CONSOLE-522

Level: INFO

Description: Modification of delegation privilege succeeded.

Data: name of realm, ID of delegation privilege, ID of subject

Triggers: Click on Save button in delegation subject profile page.

SSO_EXCEPTION_MODIFY_DELEGATION_PRIVILEGE

ID: CONSOLE-523

Level: SEVERE

Description: Modification of delegation privilege failed.

Data: name of realm, ID of delegation privilege, ID of subject, error message

Triggers: 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.

Actions: Look under delegation management log for more information.

DELEGATION_EXCEPTION_MODIFY_DELEGATION_PRIVILEGE

ID: CONSOLE-524

Level: SEVERE

Description: Modification of delegation privilege failed.

Data: name of realm, ID of delegation privilege, ID of subject, error message

Triggers: Unable to modify delegation privilege due to delegation management SDK related errors.

Actions: Look under delegation management log for more information.

ATTEMPT_GET_ID_REPO_NAMES

ID: CONSOLE-601

Level: INFO

Description: Attempt to get data store names

Data: name of realm

Triggers: View data store main page.

SUCCEED_GET_ID_REPO_NAMES

ID: CONSOLE-602

Level: INFO

Description: Getting data store names succeeded.

Data: name of realm

Triggers: View data store main page.

SSO_EXCEPTION_GET_ID_REPO_NAMES

ID: CONSOLE-603

Level: SEVERE

Description: Getting data store names failed.

Data: name of realm, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_GET_ID_REPO_NAMES

ID: CONSOLE-604

Level: SEVERE

Description: Getting data store names failed.

Data: name of realm, error message

Triggers: Unable to get data store names due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_ATTR_VALUES_ID_REPO

ID: CONSOLE-611

Level: INFO

Description: Attempt to get attribute values of identity repository

Data: name of realm, name of identity repository

Triggers: View data store profile page.

SUCCEED_GET_ATTR_VALUES_ID_REPO

ID: CONSOLE-612

Level: INFO

Description: Getting attribute values of data store succeeded.

Data: name of realm, name of identity repository

Triggers: View data store profile page.

SSO_EXCEPTION_GET_ATTR_VALUES_ID_REPO

ID: CONSOLE-613

Level: SEVERE

Description: Getting attribute values of data store failed.

Data: name of realm, name of identity repository, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_GET_ATTR_VALUES_ID_REPO

ID: CONSOLE-614

Level: SEVERE

Description: Getting attribute values of data store failed.

Data: name of realm, name of identity repository, error message

Triggers: Unable to get attribute values of data store due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_CREATE_ID_REPO

ID: CONSOLE-621

Level: INFO

Description: Attempt to create identity repository

Data: name of realm, name of identity repository, type of identity repository

Triggers: Click on New button in data store creation page.

SUCCEED_CREATE_ID_REPO

ID: CONSOLE-622

Level: INFO

Description: Creation of data store succeeded.

Data: name of realm, name of identity repository, type of identity repository

Triggers: Click on New button in data store creation page.

SSO_EXCEPTION_CREATE_ID_REPO

ID: CONSOLE-623

Level: SEVERE

Description: Creation of data store failed.

Data: name of realm, name of identity repository, type of identity repository, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_CREATE_ID_REPO

ID: CONSOLE-624

Level: SEVERE

Description: Creation data store failed.

Data: name of realm, name of identity repository, type of identity repository, error message

Triggers: Unable to create data store due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_DELETE_ID_REPO

ID: CONSOLE-631

Level: INFO

Description: Attempt to delete identity repository

Data: name of realm, name of identity repository

Triggers: Click on Delete button in data store main page.

SUCCEED_DELETE_ID_REPO

ID: CONSOLE-632

Level: INFO

Description: Deletion of data store succeeded.

Data: name of realm, name of identity repository

Triggers: Click on Delete button in data store main page.

SSO_EXCEPTION_DELETE_ID_REPO

ID: CONSOLE-633

Level: SEVERE

Description: Deletion of data store failed.

Data: name of realm, name of identity repository, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_DELETE_ID_REPO

ID: CONSOLE-634

Level: SEVERE

Description: Deletion data store failed.

Data: name of realm, name of identity repository, error message

Triggers: Unable to delete data store due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_MODIFY_ID_REPO

ID: CONSOLE-641

Level: INFO

Description: Attempt to modify identity repository

Data: name of realm, name of identity repository

Triggers: Click on Save button in data store profile page.

SUCCEED_MODIFY_ID_REPO

ID: CONSOLE-642

Level: INFO

Description: Modification of data store succeeded.

Data: name of realm, name of identity repository

Triggers: Click on Save button in data store profile page.

SSO_EXCEPTION_MODIFY_ID_REPO

ID: CONSOLE-643

Level: SEVERE

Description: Modification of data store failed.

Data: name of realm, name of identity repository, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_MODIFY_ID_REPO

ID: CONSOLE-644

Level: SEVERE

Description: Modification data store failed.

Data: name of realm, name of identity repository, error message

Triggers: Unable to modify data store due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-701

Level: INFO

Description: Attempt to get assigned services of realm

Data: name of realm

Triggers: View realm's service main page.

SUCCEED_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-702

Level: INFO

Description: Getting assigned services of realm succeeded.

Data: name of realm

Triggers: View realm's service main page.

CONFIGURATION_EXCEPTION_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-703

Level: SEVERE

Description: Getting assigned services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assigned services of realm due authentication configuration exception.

Actions: Look under authentication log for more information.

SMS_EXCEPTION_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-704

Level: SEVERE

Description: Getting assigned services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assigned services of realm due to service management SDK exception.

Actions: Look under service management log for more information.

IDREPO_EXCEPTION_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-705

Level: SEVERE

Description: Getting assigned services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assigned services of realm due to data store SDK exception.

Actions: Look under service management log for more information.

SSO_EXCEPTION_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-706

Level: SEVERE

Description: Getting assigned services of realm failed.

Data: name of realm, error message

Triggers: 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.

Actions: Look under service management log for more information.

ATTEMPT_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-711

Level: INFO

Description: Attempt to get assignable services of realm

Data: name of realm

Triggers: View realm's service main page.

SUCCEED_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-712

Level: INFO

Description: Getting assignable services of realm succeeded.

Data: name of realm

Triggers: View realm's service main page.

CONFIGURATION_EXCEPTION_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-713

Level: SEVERE

Description: Getting assignable services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assignable services of realm due authentication configuration exception.

Actions: Look under authentication log for more information.

SMS_EXCEPTION_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-714

Level: SEVERE

Description: Getting assignable services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assignable services of realm due to service management SDK exception.

Actions: Look under service management log for more information.

IDREPO_EXCEPTION_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-715

Level: SEVERE

Description: Getting assignable services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assignable services of realm due to ID Repository management SDK exception.

Actions: Look under ID Repository management log for more information.

SSO_EXCEPTION_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-716

Level: SEVERE

Description: Getting assignable services of realm failed.

Data: name of realm, error message

Triggers: 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.

Actions: Look under service management log for more information.

ATTEMPT_UNASSIGN_SERVICE_FROM_REALM

ID: CONSOLE-721

Level: INFO

Description: Attempt to unassign service from realm

Data: name of realm, name of service

Triggers: Click on Unassign button in realm's service page.

SUCCEED_UNASSIGN_SERVICE_FROM_REALM

ID: CONSOLE-722

Level: INFO

Description: Unassign service from realm succeeded.

Data: name of realm, name of service

Triggers: Click on Unassign button in realm's service page.

SMS_EXCEPTION_UNASSIGN_SERVICE_FROM_REALM

ID: CONSOLE-723

Level: SEVERE

Description: Unassign service from realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to unassign service from realm due to service management SDK exception.

Actions: Look under service management log for more information.

SSO_EXCEPTION_UNASSIGN_SERVICE_FROM_REALM

ID: CONSOLE-725

Level: SEVERE

Description: Unassign service from realm failed.

Data: name of realm, name of service, error message

Triggers: 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.

Actions: Look under data store management log for more information.

IDREPO_EXCEPTION_UNASSIGN_SERVICE_FROM_REALM

ID: CONSOLE-724

Level: SEVERE

Description: Unassign service from realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to unassign service from realm due to data store management SDK exception.

Actions: Look under data store management log for more information.

ATTEMPT_ASSIGN_SERVICE_TO_REALM

ID: CONSOLE-731

Level: INFO

Description: Attempt to assign service to realm

Data: name of realm, name of service

Triggers: Click on assign button in realm's service page.

SUCCEED_ASSIGN_SERVICE_TO_REALM

ID: CONSOLE-732

Level: INFO

Description: Assignment of service to realm succeeded.

Data: name of realm, name of service

Triggers: Click on assign button in realm's service page.

SMS_EXCEPTION_ASSIGN_SERVICE_TO_REALM

ID: CONSOLE-733

Level: SEVERE

Description: Assignment of service to realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to assign service to realm due to service management SDK exception.

Actions: Look under service management log for more information.

SSO_EXCEPTION_ASSIGN_SERVICE_TO_REALM

ID: CONSOLE-734

Level: SEVERE

Description: Assignment of service to realm failed.

Data: name of realm, name of service, error message

Triggers: 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.

Actions: Look under service management log for more information.

IDREPO_EXCEPTION_ASSIGN_SERVICE_TO_REALM

ID: CONSOLE-735

Level: SEVERE

Description: Assignment of service to realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to assign service to realm due to data store SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_ATTR_VALUE_OF_SERVICE_UNDER_REALM

ID: CONSOLE-741

Level: INFO

Description: Attempt to get attribute values of service in realm

Data: name of realm, name of service, name of attribute schema

Triggers: View realm's service profile page.

SUCCEED_GET_ATTR_VALUE_OF_SERVICE_UNDER_REALM

ID: CONSOLE-742

Level: INFO

Description: Getting of attribute values of service under realm succeeded.

Data: name of realm, name of service, name of attribute schema

Triggers: View realm's service profile page.

FORGEROCK

SMS_EXCEPTION_GET_ATTR_VALUE_OF_SERVICE_UNDER_REALM

ID: CONSOLE-743

Level: SEVERE

Description: Getting of attribute values of service under realm failed.

Data: name of realm, name of service, name of attribute schema, error message

Triggers: Unable to get attribute values of service due to service management SDK exception.

Actions: Look under service management log for more information.

IDREPO_EXCEPTION_GET_ATTR_VALUE_OF_SERVICE_UNDER_REALM

ID: CONSOLE-744

Level: INFO

Description: Getting of attribute values of service under realm failed.

Data: name of realm, name of service, name of attribute schema, error message

Triggers: Unable to get attribute values of service due to data store SDK exception.

Actions: Look under service management log for more information.

SSO_EXCEPTION_GET_ATTR_VALUE_OF_SERVICE_UNDER_REALM

ID: CONSOLE-745

Level: SEVERE

Description: Getting of attribute values of service under realm failed.

Data: name of realm, name of service, name of attribute schema, error message

Triggers: 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.

Actions: Look under service management log for more information.

ATTEMPT_MODIFY_SERVICE_UNDER_REALM

ID: CONSOLE-751

Level: INFO

Description: Attempt to modify attribute values of service in realm

Data: name of realm, name of service

Triggers: Click on Save button in realm's service profile page.

SUCCEED_MODIFY_SERVICE_UNDER_REALM

ID: CONSOLE-752

Level: INFO

Description: Modification of attribute values of service under realm succeeded.

Data: name of realm, name of service

Triggers: Click on Save button in realm's service profile page.

SMS_EXCEPTION_MODIFY_SERVICE_UNDER_REALM

ID: CONSOLE-753

Level: SEVERE

Description: Modification of attribute values of service under realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to modify attribute values of service due to service management SDK exception.

Actions: Look under service management log for more information.

IDREPO_EXCEPTION_MODIFY_SERVICE_UNDER_REALM

ID: CONSOLE-754

Level: SEVERE

Description: Modification of attribute values of service under realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to modify attribute values of service due to data store error.

Actions: Look under data store log for more information.

SSO_EXCEPTION_MODIFY_SERVICE_UNDER_REALM

ID: CONSOLE-755

Level: SEVERE

Description: Modification of attribute values of service under realm failed.

Data: name of realm, name of service, error message

Triggers: 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

Actions: Look under data store log for more information.

ATTEMPT_GET_AUTH_TYPE

ID: CONSOLE-801

Level: INFO

Description: Attempt to get authentication type

Data: server instance name

Triggers: View authentication profile page.

SUCCEED_GET_AUTH_TYPE

ID: CONSOLE-802

Level: INFO

Description: Getting of authentication type succeeded.

Data: server instance name

Triggers: View authentication profile page.

SMS_EXCEPTION_GET_AUTH_TYPE

ID: CONSOLE-803

Level: SEVERE

Description: Getting of authentication type failed.

Data: error message

Triggers: Unable to get authentication type due to authentication configuration SDK exception.

Actions: Look under authentication management log for more information.

ATTEMPT_GET_AUTH_INSTANCE

ID: CONSOLE-811

Level: INFO

Description: Attempt to get authentication instances under a realm

Data: name of realm

Triggers: View authentication profile page.

SUCCEED_GET_AUTH_INSTANCE

ID: CONSOLE-812

Level: INFO

Description: Getting of authentication instances under a realm succeeded.

Data: name of realm

Triggers: View authentication profile page.

AUTH_CONFIG_EXCEPTION_GET_AUTH_INSTANCE

ID: CONSOLE-813

Level: SEVERE

Description: Getting of authentication instances under a realm failed.

Data: name of realm, error message

Triggers: Unable to get authentication instance due to authentication configuration SDK exception.

Actions: Look under authentication management log for more information.

ATTEMPT_REMOVE_AUTH_INSTANCE

ID: CONSOLE-821

Level: INFO

Description: Attempt to remove authentication instances under a realm

Data: name of realm, name of authentication instance

Triggers: View authentication profile page.

SUCCEED_REMOVE_AUTH_INSTANCE

ID: CONSOLE-822

Level: INFO

Description: Removal of authentication instances under a realm succeeded.

Data: name of realm, name of authentication instance

Triggers: View authentication profile page.

AUTH_CONFIG_EXCEPTION_REMOVE_AUTH_INSTANCE

ID: CONSOLE-823

Level: SEVERE

Description: Removal of authentication instances under a realm failed.

Data: name of realm, name of authentication instance, error message

Triggers: Unable to remove authentication instance due to authentication configuration SDK exception.

Actions: Look under authentication management log for more information.

ATTEMPT_CREATE_AUTH_INSTANCE

ID: CONSOLE-831

Level: INFO

Description: Attempt to create authentication instance under a realm

Data: name of realm, name of authentication instance, type of authentication instance

Triggers: Click on New button in authentication creation page.

SUCCEED_CREATE_AUTH_INSTANCE

ID: CONSOLE-832

Level: INFO

Description: Creation of authentication instance under a realm succeeded.

Data: name of realm, name of authentication instance, type of authentication instance

Triggers: Click on New button in authentication creation page.

AUTH_CONFIG_EXCEPTION_CREATE_AUTH_INSTANCE

ID: CONSOLE-833

Level: SEVERE

Description: Creation of authentication instance under a realm failed.

Data: name of realm, name of authentication instance, type of authentication instance, error message

Triggers: Unable to create authentication instance due to authentication configuration exception.

Actions: Look under authentication configuration log for more information.

ATTEMPT_MODIFY_AUTH_INSTANCE

ID: CONSOLE-841

Level: INFO

Description: Attempt to modify authentication instance

Data: name of realm, name of authentication service

Triggers: Click on Save button in authentication profile page.

SUCCEED_MODIFY_AUTH_INSTANCE

ID: CONSOLE-842

Level: INFO

Description: Modification of authentication instance succeeded.

Data: name of realm, name of authentication service

Triggers: Click on Save button in authentication profile page.

SMS_EXCEPTION_MODIFY_AUTH_INSTANCE

ID: CONSOLE-843

Level: SEVERE

Description: Modification of authentication instance failed.

Data: name of realm, name of authentication service, error message

Triggers: Unable to modify authentication instance due to service management SDK exception.

Actions: Look under service anagement log for more information.

SSO_EXCEPTION_MODIFY_AUTH_INSTANCE

ID: CONSOLE-844

Level: SEVERE

Description: Modification of authentication instance failed.

Data: name of realm, name of authentication service, error message

Triggers: 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.

Actions: Look under service management log for more information.

ATTEMPT_GET_AUTH_INSTANCE_PROFILE

ID: CONSOLE-851

Level: INFO

Description: Attempt to get authentication instance profile

Data: name of realm, name of authentication instance

Triggers: View authentication instance profile page.

SUCCEED_GET_AUTH_INSTANCE_PROFILE

ID: CONSOLE-852

Level: INFO

Description: Getting of authentication instance profile succeeded.

Data: name of realm, name of authentication instance

Triggers: View authentication instance profile page.

AUTH_CONFIGURATION_EXCEPTION_GET_AUTH_INSTANCE_PROFILE

ID: CONSOLE-853

Level: SEVERE

Description: Getting of authentication instance profile failed.

Data: name of realm, name of authentication instance, error message

Triggers: Unable to get authentication instance profile due to authentication configuration SDK exception.

Actions: Look under authentication management log for more information.

ATTEMPT_MODIFY_AUTH_INSTANCE_PROFILE

ID: CONSOLE-861

Level: INFO

Description: Attempt to modify authentication instance profile

Data: name of realm, name of authentication instance

Triggers: Click on Save button in authentication instance profile page.

SUCCEED_MODIFY_AUTH_INSTANCE_PROFILE

ID: CONSOLE-862

Level: INFO

Description: Modification of authentication instance profile succeeded.

Data: name of realm, name of authentication instance

Triggers: Click on Save button in authentication instance profile page.

AUTH_CONFIGURATION_EXCEPTION_MODIFY_AUTH_INSTANCE_PROFILE

ID: CONSOLE-863

Level: SEVERE

Description: Modification of authentication instance profile failed.

Data: name of realm, name of authentication instance, error message

Triggers: Unable to modify authentication instance profile due to authentication configuration SDK exception.

Actions: Look under authentication management log for more information.

SMS_EXCEPTION_MODIFY_AUTH_INSTANCE_PROFILE

ID: CONSOLE-864

Level: SEVERE

Description: Modification of authentication instance profile failed.

Data: name of realm, name of authentication instance, error message

Triggers: Unable to modify authentication instance profile due to service management SDK exception.

Actions: Look under service management log for more information.

SSO_EXCEPTION_MODIFY_AUTH_INSTANCE_PROFILE

ID: CONSOLE-865

Level: SEVERE

Description: Modification of authentication instance profile failed.

Data: name of realm, name of authentication instance, error message

Triggers: 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.

Actions: Look under service management log for more information.

ATTEMPT_GET_AUTH_PROFILE_IN_REALM

ID: CONSOLE-871

Level: INFO

Description: Attempt to get authentication profile under a realm

Data: name of realm

Triggers: View authentication profile under a realm page.

SUCCEED_GET_AUTH_PROFILE_IN_REALM

ID: CONSOLE-872

Level: INFO

Description: Getting authentication profile under a realm succeeded.

Data: name of realm

Triggers: View authentication profile under a realm page.

SMS_CONFIGURATION_EXCEPTION_GET_AUTH_PROFILE_IN_REALM

ID: CONSOLE-873

Level: SEVERE

Description: Getting authentication profile under a realm failed.

Data: name of realm, error message

Triggers: Unable to get authentication profile under a realm due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_AUTH_CONFIG_PROFILE

ID: CONSOLE-881

Level: INFO

Description: Attempt to get authentication configuration profile

Data: name of realm, name of authentication configuration

Triggers: View authentication configuration profile page.

SUCCEED_GET_AUTH_CONFIG_PROFILE

ID: CONSOLE-882

Level: INFO

Description: Getting authentication configuration profile succeeded.

Data: name of realm, name of authentication configuration

Triggers: View authentication configuration profile page.

SSO_EXCEPTION_GET_AUTH_CONFIG_PROFILE

ID: CONSOLE-883

Level: SEVERE

Description: Getting authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_GET_AUTH_CONFIG_PROFILE

ID: CONSOLE-884

Level: SEVERE

Description: Getting authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to get authentication configuration profile due to service management SDK exception.

Actions: Look under service management log for more information.

AUTH_CONFIGURATION_EXCEPTION_GET_AUTH_CONFIG_PROFILE

ID: CONSOLE-885

Level: SEVERE

Description: Getting authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to get authentication configuration profile due to authentication configuration SDK exception.

Actions: Look under authentication configuration log for more information.

ATTEMPT_MODIFY_AUTH_CONFIG_PROFILE

ID: CONSOLE-891

Level: INFO

Description: Attempt to modify authentication configuration profile

Data: name of realm, name of authentication configuration

Triggers: Click on Save button in authentication configuration profile page.

SUCCEED_MODIFY_AUTH_CONFIG_PROFILE

ID: CONSOLE-892

Level: INFO

Description: Modification of authentication configuration profile succeeded.

Data: name of realm, name of authentication configuration

Triggers: Click on Save button in authentication configuration profile page.

SSO_EXCEPTION_MODIFY_AUTH_CONFIG_PROFILE

ID: CONSOLE-893

Level: SEVERE

Description: Modification of authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_MODIFY_AUTH_CONFIG_PROFILE

ID: CONSOLE-894

Level: SEVERE

Description: Modification of authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to modify authentication configuration profile due to service management SDK exception.

Actions: Look under service management log for more information.

AUTH_CONFIGURATION_EXCEPTION_MODIFY_AUTH_CONFIG_PROFILE

ID: CONSOLE-895

Level: SEVERE

Description: Modification of authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to modify authentication configuration profile due to authentication configuration SDK exception.

Actions: Look under authentication configuration log for more information.

ATTEMPT_CREATE_AUTH_CONFIG

ID: CONSOLE-901

Level: INFO

Description: Attempt to create authentication configuration

Data: name of realm, name of authentication configuration

Triggers: Click on New button in authentication configuration creation page.

SUCCEED_CREATE_AUTH_CONFIG

ID: CONSOLE-902

Level: INFO

Description: Creation of authentication configuration succeeded.

Data: name of realm, name of authentication configuration

Triggers: Click on New button in authentication configuration creation page.

SSO_EXCEPTION_CREATE_AUTH_CONFIG

ID: CONSOLE-903

Level: SEVERE

Description: Creation of authentication configuration failed.

Data: name of realm, name of authentication configuration, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_CREATE_AUTH_CONFIG

ID: CONSOLE-904

Level: SEVERE

Description: Creation of authentication configuration failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to create authentication configuration due to service management SDK exception.

Actions: Look under service management log for more information.

AUTH_CONFIGURATION_EXCEPTION_CREATE_AUTH_CONFIG

ID: CONSOLE-905

Level: SEVERE

Description: Creation of authentication configuration failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to create authentication configuration due to authentication configuration SDK exception.

Actions: Look under authentication configuration log for more information.

ATTEMPT_GET_ENTITY_DESCRIPTOR

ID: CONSOLE-1001

Level: INFO

Description: Attempt to get entity descriptor names.

Data: search pattern

Triggers: View entity descriptor main page.

SUCCEED_GET_ENTITY_DESCRIPTOR

ID: CONSOLE-1002

Level: INFO

Description: Getting entity descriptor names succeeded

Data: search pattern

Triggers: View entity descriptor main page.

FEDERATION_EXCEPTION_GET_ENTITY_DESCRIPTOR

ID: CONSOLE-1003

Level: SEVERE

Description: Getting entity descriptor names failed.

Data: search pattern, error message

Triggers: Unable to get entity descriptor names due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_CREATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1011

Level: INFO

Description: Attempt to create entity descriptor.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on New button in entity descriptor creation page.

SUCCEED_CREATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1012

Level: INFO

Description: Creation entity descriptor succeeded

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on New button in entity descriptor creation page.

FEDERATION_EXCEPTION_CREATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1013

Level: SEVERE

Description: Creation entity descriptor failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to create entity descriptor due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_DELETE_ENTITY_DESCRIPTORS

ID: CONSOLE-1021

Level: INFO

Description: Attempt to delete entity descriptors.

Data: descriptor names

Triggers: Click on Delete button in entity descriptor main page.

SUCCEED_DELETE_ENTITY_DESCRIPTORS

ID: CONSOLE-1022

Level: INFO

Description: Deletion entity descriptors succeeded

Data: descriptor names

Triggers: Click on Delete button in entity descriptor main page.

FEDERATION_EXCEPTION_DELETE_ENTITY_DESCRIPTORS

ID: CONSOLE-1023

Level: SEVERE

Description: Deletion entity descriptors failed.

Data: descriptor names, error message

Triggers: Unable to delete entity descriptors due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_AFFILIATE_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1031

Level: INFO

Description: Attempt to get attribute values of an affiliate entity descriptor.

Data: descriptor realm, descriptor name, descriptor protocol

Triggers: View affiliate entity descriptor profile page.

SUCCEED_GET_AFFILIATE_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1032

Level: INFO

Description: Getting of attribute values of an affiliate entity descriptor succeeded.

Data: descriptor realm, descriptor name, descriptor protocol

Triggers: View affiliate entity descriptor profile page.

FEDERATION_EXCEPTION_GET_AFFILIATE_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1033

Level: SEVERE

Description: Getting of attribute values of an affiliate entity descriptor failed.

Data: descriptor realm, descriptor name, descriptor protocol, error message

Triggers: Unable to get attribute value of an affiliate entity descriptor due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_AFFILIATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1041

Level: INFO

Description: Attempt to modify an affiliate entity descriptor.

Data: descriptor realm, descriptor name, descriptor protocol

Triggers: Click on Save button of affiliate entity descriptor profile page.

SUCCEED_MODIFY_AFFILIATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1042

Level: INFO

Description: Modification of an affiliate entity descriptor succeeded.

Data: descriptor realm, descriptor name, descriptor protocol

Triggers: Click on Save button of affiliate entity descriptor profile page.

FEDERATION_EXCEPTION_MODIFY_AFFILIATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1043

Level: SEVERE

Description: Modification of an affiliate entity descriptor failed.

Data: descriptor realm, descriptor name, descriptor protocol, error message

Triggers: Unable to modify an affiliate entity descriptor due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTRIBUTE_FORMAT_EXCEPTION_MODIFY_AFFILIATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1044

Level: SEVERE

Description: Modification of an affiliate entity descriptor failed.

Data: descriptor name, error message

Triggers: Unable to modify an affiliate entity descriptor due to incorrect number format of one or more attribute values.

Actions: Look under federation log for more information.

ATTEMPT_GET_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1051

Level: INFO

Description: Attempt to get attribute values of an entity descriptor.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View entity descriptor profile page.

SUCCEED_GET_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1052

Level: INFO

Description: Getting attribute values of entity descriptor succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View entity descriptor profile page.

FEDERATION_EXCEPTION_GET_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1053

Level: SEVERE

Description: Getting attribute values of entity descriptor failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to get attribute values of entity descriptor due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_ENTITY_DESCRIPTOR

ID: CONSOLE-1061

Level: INFO

Description: Attempt to modify entity descriptor.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in entity descriptor profile page.

SUCCEED_MODIFY_ENTITY_DESCRIPTOR

ID: CONSOLE-1062

Level: INFO

Description: Modification of entity descriptor succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in entity descriptor profile page.

FEDERATION_EXCEPTION_MODIFY_ENTITY_DESCRIPTOR

ID: CONSOLE-1063

Level: SEVERE

Description: Modification of entity descriptor failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to modify entity descriptor due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_AUTH_DOMAINS

ID: CONSOLE-1101

Level: INFO

Description: Attempt to get authentication domain names.

Data: search pattern

Triggers: View authentication domain main page.

SUCCEED_GET_AUTH_DOMAINS

ID: CONSOLE-1102

Level: INFO

Description: Getting authentication domain names succeeded.

Data: search pattern

Triggers: View authentication domain main page.

FEDERATION_EXCEPTION_GET_AUTH_DOMAINS

ID: CONSOLE-1103

Level: SEVERE

Description: Getting authentication domain names failed.

Data: name of realm, error message

Triggers: Unable to get authentication domain names due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_CREATE_AUTH_DOMAIN

ID: CONSOLE-1111

Level: INFO

Description: Attempt to create authentication domain

Data: name of authentication domain

Triggers: Click on New button in authentication domain creation page.

SUCCEED_CREATE_AUTH_DOMAIN

ID: CONSOLE-1112

Level: INFO

Description: Creation authentication domain succeeded.

Data: name of authentication domain

Triggers: Click on New button in authentication domain creation page.

FEDERATION_EXCEPTION_CREATE_AUTH_DOMAIN

ID: CONSOLE-1113

Level: SEVERE

Description: Creation authentication domain failed.

Data: name of authentication domain, error message

Triggers: Unable to create authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_DELETE_AUTH_DOMAINS

ID: CONSOLE-1121

Level: INFO

Description: Attempt to delete authentication domains

Data: name of realm, name of authentication domains

Triggers: Click on Delete button in authentication domain main page.

SUCCEED_DELETE_AUTH_DOMAIN

ID: CONSOLE-1122

Level: INFO

Description: Deletion authentication domain succeeded.

Data: name of realm, name of authentication domains

Triggers: Click on Delete button in authentication domain main page.

FEDERATION_EXCEPTION_DELETE_AUTH_DOMAIN

ID: CONSOLE-1123

Level: SEVERE

Description: Deletion authentication domain failed.

Data: name of realm, name of authentication domains, error message

Triggers: Unable to delete authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_AUTH_DOMAIN_ATTR_VALUES

ID: CONSOLE-1131

Level: INFO

Description: Attempt to get authentication domain's attribute values

Data: name of realm, name of authentication domain

Triggers: View authentication domain profile page.

SUCCEED_GET_AUTH_DOMAIN_ATTR_VALUES

ID: CONSOLE-1132

Level: INFO

Description: Getting attribute values of authentication domain succeeded.

Data: name of realm, name of authentication domain

Triggers: View authentication domain profile page.

FEDERATION_EXCEPTION_GET_AUTH_DOMAIN_ATTR_VALUES

ID: CONSOLE-1133

Level: SEVERE

Description: Getting attribute values of authentication domain failed.

Data: name of realm, name of authentication domains, error message

Triggers: Unable to get attribute values of authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_AUTH_DOMAIN

ID: CONSOLE-1141

Level: INFO

Description: Attempt to modify authentication domain

Data: name of realm, name of authentication domain

Triggers: Click on Save button in authentication domain profile page.

SUCCEED_MODIFY_AUTH_DOMAIN

ID: CONSOLE-1142

Level: INFO

Description: Modification authentication domain succeeded.

Data: name of realm, name of authentication domain

Triggers: Click on Save button in authentication domain profile page.

FEDERATION_EXCEPTION_MODIFY_AUTH_DOMAIN

ID: CONSOLE-1143

Level: SEVERE

Description: Modification authentication domain failed.

Data: name of realm, name of authentication domain, error message

Triggers: Unable to modify authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_ALL_PROVIDER_NAMES

ID: CONSOLE-1151

Level: INFO

Description: Attempt to get all provider names

Data: realm name

Triggers: View authentication domain profile page.

SUCCEED_GET_ALL_PROVIDER_NAMES

ID: CONSOLE-1152

Level: INFO

Description: Getting all provider names succeeded.

Data: realm name

Triggers: View authentication domain profile page.

FEDERATION_EXCEPTION_GET_ALL_PROVIDER_NAMES

ID: CONSOLE-1153

Level: SEVERE

Description: Getting all provider names failed.

Data: error message

Triggers: Unable to get all provider names due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_PROVIDER_NAMES_UNDER_AUTH_DOMAIN

ID: CONSOLE-1161

Level: INFO

Description: Attempt to get provider names under a authentication domain

Data: name of realm, name of authentication domain

Triggers: View authentication domain profile page.

SUCCEED_GET_PROVIDER_NAMES_UNDER_AUTH_DOMAIN

ID: CONSOLE-1162

Level: INFO

Description: Getting provider names under authentication domain succeeded.

Data: name of realm, name of authentication domain

Triggers: View authentication domain profile page.

FEDERATION_EXCEPTION_GET_PROVIDER_NAMES_UNDER_AUTH_DOMAIN

ID: CONSOLE-1163

Level: SEVERE

Description: Getting provider names under authentication domain failed.

Data: name of realm, name of authentication domain, error message

Triggers: Unable to get provider names under authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_ADD_PROVIDERS_TO_AUTH_DOMAIN

ID: CONSOLE-1171

Level: INFO

Description: Attempt to add providers to an authentication domain

Data: name of realm, name of authentication domain, name of providers

Triggers: Click on Save button in provider assignment page.

SUCCEED_ADD_PROVIDERS_TO_AUTH_DOMAIN

ID: CONSOLE-1172

Level: INFO

Description: Addition of provider to an authentication domain succeeded.

Data: name of realm, name of authentication domain, name of providers

Triggers: Click on Save button in provider assignment page.

FEDERATION_EXCEPTION_ADD_PROVIDERS_TO_AUTH_DOMAIN

ID: CONSOLE-1173

Level: SEVERE

Description: Addition of provider to an authentication domain failed.

Data: name of realm, name of authentication domain, name of providers, error message

Triggers: Unable to add provider to authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_REMOVE_PROVIDERS_FROM_AUTH_DOMAIN

ID: CONSOLE-1181

Level: INFO

Description: Attempt to remove providers from authentication domain

Data: name of realm, name of authentication domain, name of providers

Triggers: Click on Save button in provider assignment page.

SUCCEED_REMOVE_PROVIDERS_FROM_AUTH_DOMAIN

ID: CONSOLE-1182

Level: INFO

Description: Deletion of providers from authentication domain succeeded.

Data: name of realm, name of authentication domain, name of providers

Triggers: Click on Save button in provider assignment page.

FEDERATION_EXCEPTION_REMOVE_PROVIDERS_FROM_AUTH_DOMAIN

ID: CONSOLE-1183

Level: SEVERE

Description: Deletion of provider from authentication domain failed.

Data: name of realm, name of authentication domain, name of providers, error message

Triggers: Unable to remove provider from authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_CREATE_PROVIDER

ID: CONSOLE-1301

Level: INFO

Description: Attempt to create provider

Data: name of provider, role of provider, type of provider

Triggers: Click on Save button in provider assignment page.

SUCCEED_CREATE_PROVIDER

ID: CONSOLE-1302

Level: INFO

Description: Creation of providers succeeded.

Data: name of provider, role of provider, type of provider

Triggers: Click on Save button in provider assignment page.

FEDERATION_EXCEPTION_CREATE_PROVIDER

ID: CONSOLE-1303

Level: SEVERE

Description: Creation of provider failed.

Data: name of provider, role of provider, type of provider, error message

Triggers: Unable to create provider due to federation SDK related errors.

Actions: Look under federation log for more information.

FEDERATION_EXCEPTION_CREATE_PROVIDER

ID: CONSOLE-1304

Level: SEVERE

Description: Creation of provider failed.

Data: name of provider, role of provider, type of provider, error message

Triggers: Unable to create provider due to federation SDK related errors.

Actions: Look under federation log for more information.

INVOCATION_TARGET_EXCEPTION_CREATE_PROVIDER

ID: CONSOLE-1305

Level: SEVERE

Description: Creation of provider failed.

Data: name of provider, role of provider, type of provider, error message

Triggers: Unable to create provider because Administration Console cannot find the appropriate methods to set values for this provider.

Actions: This is a web application error. Please contact Sun Support for assistant.

ATTEMPT_GET_PROVIDER_ATTRIBUTE_VALUES

ID: CONSOLE-1311

Level: INFO

Description: Attempt to get attribute values for provider

Data: name of provider, role of provider, type of provider

Triggers: View provider profile page.

SUCCEED_GET_PROVIDER_ATTRIBUTE_VALUES

ID: CONSOLE-1312

Level: INFO

Description: Getting attribute values of providers succeeded.

Data: name of provider, role of provider, type of provider

Triggers: View provider profile page.

ATTEMPT_GET_HANDLER_TO_PROVIDER

ID: CONSOLE-1321

Level: INFO

Description: Attempt to get handler to provider

Data: name of provider, role of provider

Triggers: View provider profile page.

SUCCEED_GET_HANDLER_TO_PROVIDER

ID: CONSOLE-1322

Level: INFO

Description: Getting handler to provider succeeded.

Data: name of provider, role of provider

Triggers: View provider profile page.

FEDERATION_EXCEPTION_GET_HANDLER_TO_PROVIDER

ID: CONSOLE-1323

Level: SEVERE

Description: Getting handler to provider failed.

Data: name of provider, role of provider, error message

Triggers: Unable to get handler to provider due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_PROVIDER

ID: CONSOLE-1331

Level: INFO

Description: Attempt to modify provider

Data: name of provider, role of provider

Triggers: Click on Save button in provider profile page.

SUCCEED_MODIFY_PROVIDER

ID: CONSOLE-1332

Level: INFO

Description: Modification of provider succeeded.

Data: name of provider, role of provider

Triggers: Click on Save button in provider profile page.

FEDERATION_EXCEPTION_MODIFY_PROVIDER

ID: CONSOLE-1333

Level: SEVERE

Description: Modification of provider failed.

Data: name of provider, role of provider, error message

Triggers: Unable to modify provider due to federation SDK related errors.

Actions: Look under federation log for more information.

INVOCATION_TARGET_EXCEPTION_MODIFY_PROVIDER

ID: CONSOLE-1334

Level: SEVERE

Description: Modification of provider failed.

Data: name of provider, role of provider, error message

Triggers: Unable to modify provider because Administration Console cannot find the appropriate methods to set values for this provider.

Actions: This is a web application error. Please contact Sun Support for assistant.

ATTEMPT_DELETE_PROVIDER

ID: CONSOLE-1341

Level: INFO

Description: Attempt to delete provider

Data: name of provider, role of provider

Triggers: Click on delete provider button in provider profile page.

SUCCEED_DELETE_PROVIDER

ID: CONSOLE-1342

Level: INFO

Description: Deletion of provider succeeded.

Data: name of provider, role of provider

Triggers: Click on delete provider button in provider profile page.

FEDERATION_EXCEPTION_DELETE_PROVIDER

ID: CONSOLE-1343

Level: SEVERE

Description: Deletion of provider failed.

Data: name of provider, role of provider, error message

Triggers: Unable to delete provider due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_PROSPECTIVE_TRUSTED_PROVIDER

ID: CONSOLE-1351

Level: INFO

Description: Attempt to get prospective trusted provider

Data: name of provider, role of provider

Triggers: View add trusted provider page.

SUCCEED_GET_PROSPECTIVE_TRUSTED_PROVIDER

ID: CONSOLE-1352

Level: INFO

Description: Getting of prospective trusted provider succeeded.

Data: name of provider, role of provider

Triggers: View add trusted provider page.

FEDERATION_EXCEPTION_GET_PROSPECTIVE_TRUSTED_PROVIDER

ID: CONSOLE-1353

Level: SEVERE

Description: Getting of prospective trusted provider failed.

Data: name of provider, role of provider, error message

Triggers: Unable to get prospective trusted provider due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_ATTR_VALUE_SCHEMA_TYPE

ID: CONSOLE-2001

Level: INFO

Description: Attempt to get attribute values of schema type of a service schema

Data: name of service, name of schema type, name of attribute schemas

Triggers: View service profile page.

SUCCEED_GET_ATTR_VALUE_SCHEMA_TYPE

ID: CONSOLE-2002

Level: INFO

Description: Getting attribute values of schema type of a service schema succeeded.

Data: name of service, name of schema type, name of attribute schemas

Triggers: View service profile page.

SSO_EXCEPTION_GET_ATTR_VALUE_SCHEMA_TYPE

ID: CONSOLE-2003

Level: SEVERE

Description: Getting attribute values of schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_GET_ATTR_VALUE_SCHEMA_TYPE

ID: CONSOLE-2004

Level: SEVERE

Description: Getting attribute values of schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: Unable to get attribute values of schema type of a service schema due to service management SDK related errors.

Actions: Look under service management log for more information.

NO_SCHEMA_GET_ATTR_VALUE_SCHEMA_TYPE

ID: CONSOLE-2005

Level: INFO

Description: Getting attribute values of schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas

Triggers: View service profile page.

Actions: Need no action on this event. Console attempts to get a schema from a service but schema does not exist.

ATTEMPT_GET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2011

Level: INFO

Description: Attempt to get attribute values of attribute schema of a schema type of a service schema

Data: name of service, name of schema type, name of attribute schemas

Triggers: View service profile page.

SUCCEED_GET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2012

Level: INFO

Description: Getting attribute values of attribute schema of a schema type of a service schema succeeded.

Data: name of service, name of schema type, name of attribute schemas

Triggers: View service profile page.

SSO_EXCEPTION_GET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2013

Level: SEVERE

Description: Getting attribute values of attribute schema of a schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_GET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2014

Level: SEVERE

Description: Getting attribute values of attribute schema of a schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: Unable to get attribute values of schema type of a service schema due to service management SDK related errors.

Actions: Look under service management log for more information.

ATTEMPT_SET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2021

Level: INFO

Description: Attempt to modify attribute values of attribute schema of a schema type of a service schema

Data: name of service, name of schema type, name of attribute schemas

Triggers: Click on Save button in service profile page.

SUCCEED_SET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2022

Level: INFO

Description: Modification attribute values of attribute schema of a schema type of a service schema succeeded.

Data: name of service, name of schema type, name of attribute schemas

Triggers: Click on Save button in service profile page.

SSO_EXCEPTION_SET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2023

Level: SEVERE

Description: Modification attribute values of attribute schema of a schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: 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.

Actions: Look under service management log for more information.

SMS_EXCEPTION_SET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2024

Level: SEVERE

Description: Modification attribute values of attribute schema of a schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: Unable to modify attribute values of schema type of a service schema due to service management SDK related errors.

Actions: Look under service management log for more information.

ATTEMPT_CLIENT_DETECTION_GET_DEVICE_NAMES

ID: CONSOLE-2501

Level: INFO

Description: Attempt to get device names of client detection service

Data: name of profile, name of style, search pattern

Triggers: View client profile page.

SUCCEED_CLIENT_DETECTION_GET_DEVICE_NAMES

ID: CONSOLE-2502

Level: INFO

Description: Getting device names of client detection service succeeded.

Data: name of profile, name of style, search pattern

Triggers: View client profile page.

ATTEMPT_CLIENT_DETECTION_DELETE_CLIENT

ID: CONSOLE-2511

Level: INFO

Description: Attempt to delete client in client detection service

Data: type of client

Triggers: Click on client type delete hyperlink page.

SUCCEED_CLIENT_DETECTION_DELETE_CLIENT

ID: CONSOLE-2512

Level: INFO

Description: Deletion of client in client detection service succeeded.

Data: type of client

Triggers: Click on client type delete hyperlink page.

CLIENT_SDK_EXCEPTION_CLIENT_DETECTION_DELETE_CLIENT

ID: CONSOLE-2513

Level: SEVERE

Description: Deletion of client in client detection service failed.

Data: type of client, error message

Triggers: Unable to delete client due to client detection SDK related errors.

Actions: Look under client detection management log for more information.

ATTEMPT_CLIENT_DETECTION_CREATE_CLIENT

ID: CONSOLE-2521

Level: INFO

Description: Attempt to create client in client detection service

Data: type of client

Triggers: Click on New button in Client Creation Page.

SUCCEED_CLIENT_DETECTION_CREATE_CLIENT

ID: CONSOLE-2522

Level: INFO

Description: Creation of client in client detection service succeeded.

Data: type of client

Triggers: Click on New button in Client Creation Page.

CLIENT_SDK_EXCEPTION_CLIENT_DETECTION_CREATE_CLIENT

ID: CONSOLE-2523

Level: SEVERE

Description: Creation of client in client detection service failed.

Data: type of client, error message

Triggers: Unable to create client due to client detection SDK related errors.

Actions: Look under client detection management log for more information.

INVALID_CLIENT_TYPE_CLIENT_DETECTION_CREATE_CLIENT

ID: CONSOLE-2524

Level: INFO

Description: Creation of client in client detection service failed.

Data: type of client, error message

Triggers: Unable to create client because client type is invalid.

Actions: Check the client type again before creation.

ATTEMPT_CLIENT_DETECTION_GET_CLIENT_PROFILE

ID: CONSOLE-2531

Level: INFO

Description: Attempt to get client profile in client detection service

Data: type of client, classification

Triggers: View client profile page.

SUCCEED_CLIENT_DETECTION_GET_CLIENT_PROFILE

ID: CONSOLE-2532

Level: INFO

Description: Getting of client profile in client detection service succeeded.

Data: type of client, classification

Triggers: View client profile page.

ATTEMPT_CLIENT_DETECTION_MODIFY_CLIENT_PROFILE

ID: CONSOLE-2541

Level: INFO

Description: Attempt to modify client profile in client detection service

Data: type of client

Triggers: Click on Save button client profile page.

SUCCEED_CLIENT_DETECTION_MODIFY_CLIENT_PROFILE

ID: CONSOLE-2542

Level: INFO

Description: Modification of client profile in client detection service succeeded.

Data: type of client

Triggers: Click on Save button client profile page.

CLIENT_SDK_EXCEPTION_CLIENT_DETECTION_CREATE_CLIENT

ID: CONSOLE-2543

Level: SEVERE

Description: Modification of client profile in client detection service failed.

Data: type of client, error message

Triggers: Unable to modify client profile due to client detection SDK related errors.

Actions: Look under client detection management log for more information.

ATTEMPT_GET_CURRENT_SESSIONS

ID: CONSOLE-3001

Level: INFO

Description: Attempt to get current sessions

Data: name of server, search pattern

Triggers: View session main page.

SUCCEED_GET_CURRENT_SESSIONS

ID: CONSOLE-3002

Level: INFO

Description: Getting of current sessions succeeded.

Data: name of server, search pattern

Triggers: View session main page.

SESSION_EXCEPTION_GET_CURRENT_SESSIONS

ID: CONSOLE-3003

Level: SEVERE

Description: Getting of current sessions failed.

Data: name of server, name of realm, error message

Triggers: Unable to get current sessions due to session SDK exception.

Actions: Look under session management log for more information.

ATTEMPT_INVALIDATE_SESSIONS

ID: CONSOLE-3011

Level: INFO

Description: Attempt to invalidate session

Data: name of server, ID of session

Triggers: Click on Invalidate button in session main page.

SUCCEED_INVALIDATE_SESSIONS

ID: CONSOLE-3012

Level: INFO

Description: Invalidation of session succeeded.

Data: name of server, ID of session

Triggers: Click on Invalidate button in session main page.

SESSION_EXCEPTION_INVALIDATE_SESSIONS

ID: CONSOLE-3013

Level: SEVERE

Description: Invalidation of session failed.

Data: name of server, ID of session, error message

Triggers: Unable to invalidate session due to session SDK exception.

Actions: Look under session management log for more information.

ATTEMPT_GET_SITE_NAMES

ID: CONSOLE-12001

Level: INFO

Description: Attempt to get site names

Data: server instance name

Triggers: View site and server management page.

SUCCEED_GET_SITE_NAMES

ID: CONSOLE-12002

Level: INFO

Description: Site names are returned.

Data: server instance name

Triggers: View site and server management page.

SSO_EXCEPTION_GET_SITE_NAMES

ID: CONSOLE-12003

Level: SEVERE

Description: Get site names.

Data: error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SITE_NAMES

ID: CONSOLE-12004

Level: SEVERE

Description: Get site names.

Data: error message

Triggers: Unable to get site names due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_GET_SITE_PRIMARY_URL

ID: CONSOLE-12011

Level: INFO

Description: Attempt to get primary URL of site.

Data: Site Name

Triggers: View site profile page.

SUCCEED_GET_SITE_PRIMARY_URL

ID: CONSOLE-12012

Level: INFO

Description: Primary URL of site is returned.

Data: Site Name

Triggers: View site profile page.

SSO_EXCEPTION_GET_SITE_PRIMARY_URL

ID: CONSOLE-12013

Level: SEVERE

Description: Get primary URL of site.

Data: Site Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SITE_PRIMARY_URL

ID: CONSOLE-12014

Level: SEVERE

Description: Get primary URL of site.

Data: Site Name, error message

Triggers: Unable to get primary URL of site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_GET_SITE_FAILOVER_URLS

ID: CONSOLE-12021

Level: INFO

Description: Attempt to get failover URLs of site.

Data: Site Name

Triggers: View site profile page.

SUCCEED_GET_SITE_FAILOVER_URLS

ID: CONSOLE-12022

Level: INFO

Description: Failover URLs of site is returned.

Data: Site Name

Triggers: View site profile page.

SSO_EXCEPTION_GET_SITE_FAILOVER_URLS

ID: CONSOLE-12023

Level: SEVERE

Description: Get failover URLs of site.

Data: Site Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SITE_FAILOVER_URLS

ID: CONSOLE-12024

Level: SEVERE

Description: Get failover URLs of site.

Data: Site Name, error message

Triggers: Unable to get failover URLs of site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_GET_SITE_MEMBERS

ID: CONSOLE-12031

Level: INFO

Description: Attempt to get members of site.

Data: Site Name

Triggers: View site profile page.

SUCCEED_GET_SITE_MEMBERS

ID: CONSOLE-12032

Level: INFO

Description: Members of site is returned.

Data: Site Name

Triggers: View site profile page.

SSO_EXCEPTION_GET_SITE_MEMBERS

ID: CONSOLE-12033

Level: SEVERE

Description: Get members of site.

Data: Site Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SITE_MEMBERS

ID: CONSOLE-12034

Level: SEVERE

Description: Get members of site.

Data: Site Name, error message

Triggers: Unable to get members of site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_CREATE_SITE

ID: CONSOLE-12041

Level: INFO

Description: Attempt to create site.

Data: Site Name

Triggers: View create site page.

SUCCEED_CREATE_SITE

ID: CONSOLE-12042

Level: INFO

Description: Site is created.

Data: Site Name

Triggers: Click on create button on creation page.

SSO_EXCEPTION_CREATE_SITE

ID: CONSOLE-12043

Level: SEVERE

Description: Create site.

Data: Site Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_CREATE_SITE

ID: CONSOLE-12044

Level: SEVERE

Description: Create site.

Data: Site Name, error message

Triggers: Unable to create site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_CREATE_SERVER

ID: CONSOLE-12051

Level: INFO

Description: Attempt to create server.

Data: Server Name

Triggers: View create server page.

SUCCEED_CREATE_SERVER

ID: CONSOLE-12052

Level: INFO

Description: Server is created.

Data: Server Name

Triggers: Click on create button on creation page.

SSO_EXCEPTION_CREATE_SERVER

ID: CONSOLE-12053

Level: SEVERE

Description: Create server.

Data: Server Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_CREATE_SERVER

ID: CONSOLE-12054

Level: SEVERE

Description: Create server.

Data: Server Name, error message

Triggers: Unable to create server due the SMS API error.

Actions: Look under service management SDK log for more information.

CONFIGURATION_EXCEPTION_CREATE_SERVER

ID: CONSOLE-12055

Level: SEVERE

Description: Create server.

Data: Server Name, error message

Triggers: Unable to create server due the incorrect data format error.

Actions: Look under console log for more information.

IO_EXCEPTION_CREATE_SERVER

ID: CONSOLE-12056

Level: SEVERE

Description: Create server.

Data: Server Name, error message

Triggers: Unable to create server due the incorrect data format error.

Actions: Look under console log for more information.

ATTEMPT_DELETE_SITE

ID: CONSOLE-12061

Level: INFO

Description: Attempt to delete site.

Data: Site Name

Triggers: Click on delete site button.

SUCCEED_DELETE_SITE

ID: CONSOLE-12062

Level: INFO

Description: Site is deleted.

Data: Site Name

Triggers: Click on delete button.

SSO_EXCEPTION_DELETE_SITE

ID: CONSOLE-12063

Level: SEVERE

Description: Delete site.

Data: Site Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_DELETE_SITE

ID: CONSOLE-12064

Level: SEVERE

Description: Delete site.

Data: Site Name, error message

Triggers: Unable to delete site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_MODIFY_SITE

ID: CONSOLE-12071

Level: INFO

Description: Attempt to modify site.

Data: Site Name

Triggers: Click on OK button in site profile page.

SUCCEED_MODIFY_SITE

ID: CONSOLE-12072

Level: INFO

Description: Site is nodified.

Data: Site Name

Triggers: Click on OK button in site profile page.

SSO_EXCEPTION_MODIFY_SITE

ID: CONSOLE-12073

Level: SEVERE

Description: Modify site.

Data: Site Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_MODIFY_SITE

ID: CONSOLE-12074

Level: SEVERE

Description: Modify site.

Data: Site Name, error message

Triggers: Unable to modify site due the SMS API error.

Actions: Look under service management SDK log for more information.

CONFIGURATION_EXCEPTION_MODIFY_SITE

ID: CONSOLE-12075

Level: SEVERE

Description: Modify site.

Data: Site Name, error message

Triggers: Unable to modify site due the incorrect data format.

Actions: Look under console log for more information.

ATTEMPT_GET_SERVER_NAMES

ID: CONSOLE-12081

Level: INFO

Description: Attempt to get server names.

Data: server instance name

Triggers: View site and server management page.

SUCCEED_GET_SERVER_NAMES

ID: CONSOLE-12082

Level: INFO

Description: Server names are returned.

Data: server instance name

Triggers: View site and server management page.

SSO_EXCEPTION_GET_SERVER_NAMES

ID: CONSOLE-12083

Level: SEVERE

Description: Get server name.

Data: error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SERVER_NAMES

ID: CONSOLE-12084

Level: SEVERE

Description: Get server name.

Data: error message

Triggers: Unable to get server names due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_GET_SERVER_SITE

ID: CONSOLE-12091

Level: INFO

Description: Attempt to get server's site.

Data: Server Name

Triggers: View server profile page.

SUCCEED_GET_SERVER_SITE

ID: CONSOLE-12092

Level: INFO

Description: Server's site name is returned.

Data: Server Name

Triggers: View server profile page.

SSO_EXCEPTION_GET_SERVER_SITE

ID: CONSOLE-12093

Level: SEVERE

Description: Get server's site name.

Data: Server Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SERVER_SITE

ID: CONSOLE-12094

Level: SEVERE

Description: Get server's site name.

Data: Server Name, error message

Triggers: Unable to get server's site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_DELETE_SERVER

ID: CONSOLE-12101

Level: INFO

Description: Attempt to delete server.

Data: Server Name

Triggers: Click on delete button in server management page.

SUCCEED_DELETE_SERVER

ID: CONSOLE-12102

Level: INFO

Description: Server is delete.

Data: Server Name

Triggers: Click on delete button in server management page.

SSO_EXCEPTION_DELETE_SERVER

ID: CONSOLE-12103

Level: SEVERE

Description: Delete server.

Data: Server Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_DELETE_SERVER

ID: CONSOLE-12104

Level: SEVERE

Description: Delete server.

Data: Server Name, error message

Triggers: Unable to delete server due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_CLONE_SERVER

ID: CONSOLE-12201

Level: INFO

Description: Attempt to clone server.

Data: Server Name, Cloned Server Name

Triggers: Click on clone button in server management page.

SUCCEED_CLONE_SERVER

ID: CONSOLE-12202

Level: INFO

Description: Server is cloned.

Data: Server Name, Cloned Server Name

Triggers: Click on clone button in server management page.

SSO_EXCEPTION_CLONE_SERVER

ID: CONSOLE-12203

Level: SEVERE

Description: clone server.

Data: Server Name, Cloned Server Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_CLONE_SERVER

ID: CONSOLE-12204

Level: SEVERE

Description: clone server.

Data: Server Name, Cloned Server Name, error message

Triggers: Unable to clone server due the SMS API error.

Actions: Look under service management SDK log for more information.

CONFIGURATION_EXCEPTION_CLONE_SERVER

ID: CONSOLE-12205

Level: SEVERE

Description: clone server.

Data: Server Name, Cloned Server Name, error message

Triggers: Unable to clone server due the data format error.

Actions: Look under console log for more information.

ATTEMPT_GET_SERVER_CONFIG

ID: CONSOLE-12211

Level: INFO

Description: Attempt to get server's configuration.

Data: Server Name

Triggers: View server profile page.

SUCCEED_GET_SERVER_CONFIG

ID: CONSOLE-12212

Level: INFO

Description: Server's configuration is returned.

Data: Server Name

Triggers: View server profile page.

SSO_EXCEPTION_GET_SERVER_CONFIG

ID: CONSOLE-12213

Level: SEVERE

Description: Get server's configuration.

Data: Server Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SERVER_CONFIG

ID: CONSOLE-12214

Level: SEVERE

Description: Get server's configuration.

Data: Server Name, error message

Triggers: Unable to get server's configuration due the SMS API error.

Actions: Look under service management SDK log for more information.

IO_EXCEPTION_GET_SERVER_CONFIG

ID: CONSOLE-12215

Level: SEVERE

Description: get server's configuration.

Data: Server Name, error message

Triggers: Unable to get server's configuration due the data parsing error.

Actions: Look under console log for more information.

ATTEMPT_GET_SERVER_DEFAULT_CONFIG

ID: CONSOLE-12221

Level: INFO

Description: Attempt to get server default configuration.

Data: server instance name

Triggers: View server profile page.

SUCCEED_GET_SERVER_DEFAULT_CONFIG

ID: CONSOLE-12222

Level: INFO

Description: Server default configuration is returned.

Data: server instance name

Triggers: View server profile page.

ATTEMPT_MODIFY_SERVER

ID: CONSOLE-12231

Level: INFO

Description: Attempt to modify server.

Data: Server Name

Triggers: Click on OK button in server profile page.

SUCCEED_MODIFY_SERVER

ID: CONSOLE-12232

Level: INFO

Description: Server is modified.

Data: Server Name

Triggers: Click on OK button in server profile page.

SSO_EXCEPTION_MODIFY_SERVER

ID: CONSOLE-12233

Level: SEVERE

Description: modify server.

Data: Server Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_MODIFY_SERVER

ID: CONSOLE-12234

Level: SEVERE

Description: modify server.

Data: Server Name, error message

Triggers: Unable to modify server due the SMS API error.

Actions: Look under service management SDK log for more information.

IO_EXCEPTION_MODIFY_SERVER

ID: CONSOLE-12235

Level: SEVERE

Description: modify server.

Data: Server Name, error message

Triggers: Unable to modify server due the data parsing error.

Actions: Look under console log for more information.

CONFIGURATION_EXCEPTION_MODIFY_SERVER

ID: CONSOLE-12236

Level: SEVERE

Description: modify server.

Data: Server Name, error message

Triggers: Unable to modify server due the incorrect data format error.

Actions: Look under console log for more information.

ATTEMPT_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12241

Level: INFO

Description: Attempt to modify server's inheritance.

Data: Server Name

Triggers: Click on OK button in server inheritance setting page.

SUCCEED_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12242

Level: INFO

Description: Server's inheritance setting is modified.

Data: Server Name

Triggers: Click on OK button in server inheritance setting page.

SSO_EXCEPTION_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12243

Level: SEVERE

Description: Modify server's inheritance.

Data: Server Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12244

Level: SEVERE

Description: Modify server's inheritance.

Data: Server Name, error message

Triggers: Unable to modify server's inheritance due the SMS API error.

Actions: Look under service management SDK log for more information.

IO_EXCEPTION_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12245

Level: SEVERE

Description: modify server's inheritance.

Data: Server Name, error message

Triggers: Unable to modify server's inheritance due the data parsing error.

Actions: Look under console log for more information.

CONFIGURATION_EXCEPTION_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12246

Level: SEVERE

Description: modify server's inheritance.

Data: Server Name, error message

Triggers: Unable to modify server's inheritance due the incorrect data format error.

Actions: Look under console log for more information.

ATTEMPT_GET_SERVER_CONFIG_XML

ID: CONSOLE-12251

Level: INFO

Description: Attempt to get server's configuration XML.

Data: Server Name

Triggers: View server's server configuration XML profile page.

SUCCEED_GET_SERVER_CONFIG_XML

ID: CONSOLE-12252

Level: INFO

Description: Server's configuration XML is returned.

Data: Server Name

Triggers: View server's server configuration XML profile page.

SSO_EXCEPTION_GET_SERVER_CONFIG_XML

ID: CONSOLE-12253

Level: SEVERE

Description: Get server's configuration XML.

Data: Server Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SERVER_CONFIG_XML

ID: CONSOLE-12254

Level: SEVERE

Description: sGget server's configuration XML.

Data: Server Name, error message

Triggers: Unable to get server's configuration XML due the SMS API error.

Actions: Look under service management SDK log for more information.

GENERIC_EXCEPTION_GET_SERVER_CONFIG_XML

ID: CONSOLE-12255

Level: SEVERE

Description: sGget server's configuration XML.

Data: Server Name, error message

Triggers: Unable to get server's configuration XML due the data parsing error.

Actions: Look under console log for more information.

ATTEMPT_SET_SERVER_CONFIG_XML

ID: CONSOLE-12261

Level: INFO

Description: Attempt to set server's configuration XML.

Data: Server Name

Triggers: Click on OK button in server's server configuration XML profile page.

SUCCEED_SET_SERVER_CONFIG_XML

ID: CONSOLE-12262

Level: INFO

Description: Server's configuration XML is modified.

Data: Server Name

Triggers: Click on OK button in server's server configuration XML profile page.

SSO_EXCEPTION_SET_SERVER_CONFIG_XML

ID: CONSOLE-12263

Level: SEVERE

Description: set server's configuration XML.

Data: Server Name, error message

Triggers: 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.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_SET_SERVER_CONFIG_XML

ID: CONSOLE-12264

Level: SEVERE

Description: sGset server's configuration XML.

Data: Server Name, error message

Triggers: Unable to set server's configuration XML due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_SEARCH_AGENT

ID: CONSOLE-13001

Level: INFO

Description: Attempt to search for agents

Data: base realm, agent type, search pattern, search size limit, search time limit

Triggers: Click on Search button in agent search view.

SUCCEED_SEARCH_AGENT

ID: CONSOLE-13002

Level: INFO

Description: Searching for agents succeeded

Data: base realm, agent type, search pattern, search size limit, search time limit

Triggers: Click on Search button in agent search view.

EXCEPTION_SEARCH_AGENT

ID: CONSOLE-13003

Level: SEVERE

Description: Searching for agents failed

Data: base realm, agent type, search pattern, search size limit, search time limit, error message

Triggers: 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.

Actions: Look under data store log for more information.

ATTEMPT_DELETE_AGENT

ID: CONSOLE-13011

Level: INFO

Description: Attempt to delete agents

Data: base realm, agent names

Triggers: Click on Delete button in agent home page.

SUCCEED_DELETE_AGENT

ID: CONSOLE-13012

Level: INFO

Description: Agents are deleted

Data: base realm, agent names

Triggers: Click on Delete button in agent home page.

EXCEPTION_DELETE_AGENT

ID: CONSOLE-13013

Level: SEVERE

Description: Deletion of agents failed

Data: base realm, agent names, error message

Triggers: 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.

Actions: Look under data store log for more information.

ATTEMPT_SEARCH_AGENT_GROUP

ID: CONSOLE-13021

Level: INFO

Description: Attempt to search for agent groups

Data: base realm, agent type, search pattern, search size limit, search time limit

Triggers: Click on Search button in agent search view.

SUCCEED_SEARCH_AGENT_GROUP

ID: CONSOLE-13022

Level: INFO

Description: Searching for agent groups succeeded

Data: base realm, agent type, search pattern, search size limit, search time limit

Triggers: Click on Search button in agent search view.

EXCEPTION_SEARCH_AGENT_GROUP

ID: CONSOLE-13023

Level: SEVERE

Description: Searching for agent groups failed

Data: base realm, agent type, search pattern, search size limit, search time limit, error message

Triggers: 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.

Actions: Look under data store log for more information.

ATTEMPT_DELETE_AGENT_GROUP

ID: CONSOLE-13031

Level: INFO

Description: Attempt to delete agent groups

Data: base realm, agent group names

Triggers: Click on Delete button in agent home page.

SUCCEED_DELETE_AGENT_GROUP

ID: CONSOLE-13032

Level: INFO

Description: Agent groups are deleted

Data: base realm, agent group names

Triggers: Click on Delete button in agent home page.

EXCEPTION_DELETE_AGENT_GROUP

ID: CONSOLE-13033

Level: SEVERE

Description: Deletion of agent groups failed

Data: base realm, agent group names, error message

Triggers: 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.

Actions: Look under data store log for more information.

ATTEMPT_CREATE_AGENT

ID: CONSOLE-13041

Level: INFO

Description: Attempt to create agent

Data: base realm, agent name, agent type

Triggers: Click on New button in agent home page.

SUCCEED_CREATE_AGENT

ID: CONSOLE-13042

Level: INFO

Description: Agent is created

Data: base realm, agent name, agent type

Triggers: Click on New button in agent home page.

EXCEPTION_CREATE_AGENT

ID: CONSOLE-13043

Level: SEVERE

Description: Creation of agent failed

Data: base realm, agent name, agent type, error message

Triggers: 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.

Actions: Look under data store log for more information.

ATTEMPT_CREATE_AGENT_GROUP

ID: CONSOLE-13051

Level: INFO

Description: Attempt to create agent group

Data: base realm, agent group name, agent type

Triggers: Click on New button in agent home page.

SUCCEED_CREATE_AGENT_GROUP

ID: CONSOLE-13052

Level: INFO

Description: Agent group is created

Data: base realm, agent group name, agent type

Triggers: Click on New button in agent home page.

EXCEPTION_CREATE_AGENT_GROUP

ID: CONSOLE-13053

Level: SEVERE

Description: Creation of agent group failed

Data: base realm, agent group name, agent type, error message

Triggers: 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.

Actions: Look under data store log for more information.

ATTEMPT_GET_AGENT_ATTRIBUTE_VALUES

ID: CONSOLE-13061

Level: INFO

Description: Attempt to get agent attribute values

Data: agent universal Id

Triggers: Visit agent profile page.

SUCCEED_GET_AGENT_ATTRIBUTE_VALUES

ID: CONSOLE-13062

Level: INFO

Description: Agent attribute values is retrieved.

Data: agent universal Id

Triggers: Visit agent profile page.

EXCEPTION_GET_AGENT_ATTRIBUTE_VALUES

ID: CONSOLE-13063

Level: SEVERE

Description: Unable to get agent attribute values

Data: agent universal Id, error message

Triggers: 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.

Actions: Look under data store log for more information.

ATTEMPT_SET_AGENT_ATTRIBUTE_VALUE

ID: CONSOLE-13071

Level: INFO

Description: Attempt to set agent attribute values

Data: agent universal Id

Triggers: Click on save button in agent profile page.

SUCCEED_SET_AGENT_ATTRIBUTE_VALUE

ID: CONSOLE-13072

Level: INFO

Description: Agent attribute values set successfully

Data: agent universal Id

Triggers: Click on save button in agent profile page.

EXCEPTION_SET_AGENT_ATTRIBUTE_VALUE

ID: CONSOLE-13073

Level: SEVERE

Description: Unable to set agent attribute values

Data: agent universal Id, error message

Triggers: 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.

Actions: Look under data store log for more information.

ATTEMPT_GET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13074

Level: INFO

Description: Attempt to read session HA properties

Data: name of attribute

Triggers: Click on Save button in session profile page.

SUCCEED_GET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13075

Level: INFO

Description: Read Access of session HA properties succeeded.

Data: name of attribute

Triggers: Click on Save button in session profile page.

SMS_EXCEPTION_GET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13076

Level: SEVERE

Description: Read Access of session HA properties failed.

Data: name of attribute, error message

Triggers: Unable to modify session HA properties due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_SET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13077

Level: INFO

Description: Attempt to modify session HA properties

Data: name of attribute

Triggers: Click on Save button in session profile page.

SUCCEED_SET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13078

Level: INFO

Description: Modification of session HA properties succeeded.

Data: name of attribute

Triggers: Click on Save button in session profile page.

SMS_EXCEPTION_SET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13079

Level: SEVERE

Description: Modification of session HA properties failed.

Data: name of attribute, error message

Triggers: Unable to modify session HA properties due to service management SDK exception.

Actions: Look under service management log for more information.

OpenAM logs the following CORETOKEN messages.

TOKEN_CREATE_SUCCESS

ID: CORETOKEN-1

Level: INFO

Description: Creating a token succeeded

Data: token type, token subject, token attribute names

Triggers: Create token

TOKEN_READ_SUCCESS

ID: CORETOKEN-2

Level: INFO

Description: Retrieving a token succeeded

Data: token type, token subject

Triggers: Read token

TOKEN_UPDATE_SUCCESS

ID: CORETOKEN-3

Level: INFO

Description: Updating a token succeeded

Data: names of attributes updated

Triggers: Update token

TOKEN_SEARCH_SUCCESS

ID: CORETOKEN-4

Level: INFO

Description: Searching tokens succeeded

Data: query, number of entries returned

Triggers: Search token

TOKEN_DELETE_SUCCESS

ID: CORETOKEN-5

Level: INFO

Description: Removing a token succeeded

Triggers: Delete token

EXPIRED_TOKEN_DELETE_SUCCESS

ID: CORETOKEN-6

Level: INFO

Description: Removing an expired token succeeded

Triggers: Token expired

UNABLE_TO_CREATE_TOKEN

ID: CORETOKEN-7

Level: INFO

Description: Creating a token failed

Data: error message, token type, token subject, token attribute names

Triggers: Create token

UNABLE_TO_READ_TOKEN

ID: CORETOKEN-8

Level: INFO

Description: Retrieving a token failed

Data: error message

Triggers: Read token

UNABLE_TO_UPDATE_TOKEN

ID: CORETOKEN-9

Level: INFO

Description: Updating a token failed

Data: error message

Triggers: Update token

UNABLE_TO_SEARCH_TOKEN

ID: CORETOKEN-10

Level: INFO

Description: Searching tokens failed

Data: query, error message

Triggers: Search Token

UNABLE_TO_DELETE_TOKEN

ID: CORETOKEN-11

Level: INFO

Description: Removing a token failed

Data: error message

Triggers: Delete token

OpenAM logs the following ENTITLEMENT messages.

ATTEMPT_ADD_PRIVILEGE

ID: ENTITLEMENT-1

Level: INFO

Description: Attempt to add privilege.

Data: realm, privilege name

Triggers: Add privilege API is called.

SUCCEEDED_ADD_PRIVILEGE

ID: ENTITLEMENT-2

Level: INFO

Description: Privilege is added.

Data: realm, privilege name

Triggers: Add privilege API is called.

FAILED_ADD_PRIVILEGE

ID: ENTITLEMENT-3

Level: INFO

Description: Failed to add privilege.

Data: realm, privilege name, error message

Triggers: Add privilege API is called.

Actions: Privilege might already exists.; Administrator might not have the permission to add privilege.

ATTEMPT_ADD_REFERRAL

ID: ENTITLEMENT-11

Level: INFO

Description: Attempt to add referral privilege.

Data: realm, privilege name

Triggers: Add referral privilege API is called.

SUCCEEDED_ADD_REFERRAL

ID: ENTITLEMENT-12

Level: INFO

Description: Referral Privilege is added.

Data: realm, privilege name

Triggers: Add referral privilege API is called.

FAILED_ADD_REFERRAL

ID: ENTITLEMENT-13

Level: INFO

Description: Failed to add referral privilege.

Data: realm, privilege name, error message

Triggers: Add referral privilege API is called.

Actions: Privilege might already exists.; Administrator might not have the permission to add referral privilege.

ATTEMPT_REMOVE_PRIVILEGE

ID: ENTITLEMENT-21

Level: INFO

Description: Attempt to remove privilege.

Data: realm, privilege name

Triggers: Remove privilege API is called.

SUCCEEDED_REMOVE_PRIVILEGE

ID: ENTITLEMENT-22

Level: INFO

Description: Privilege is removed.

Data: realm, privilege name

Triggers: Removed privilege API is called.

FAILED_REMOVE_PRIVILEGE

ID: ENTITLEMENT-23

Level: INFO

Description: Failed to removed privilege.

Data: realm, privilege name, error message

Triggers: Removed privilege API is called.

Actions: Administrator might not have the permission to remove privilege.

ATTEMPT_REMOVE_REFERRAL

ID: ENTITLEMENT-31

Level: INFO

Description: Attempt to remove referral privilege.

Data: realm, privilege name

Triggers: Remove referral privilege API is called.

SUCCEEDED_REMOVE_REFERRAL

ID: ENTITLEMENT-32

Level: INFO

Description: Referral privilege is removed.

Data: realm, privilege name

Triggers: Removed referral privilege API is called.

FAILED_REMOVE_REFERRAL

ID: ENTITLEMENT-33

Level: INFO

Description: Failed to removed referral privilege.

Data: realm, privilege name, error message

Triggers: Removed referral privilege API is called.

Actions: Administrator might not have the permission to remove privilege.

ATTEMPT_SAVE_APPLICATION

ID: ENTITLEMENT-101

Level: INFO

Description: Attempt to save application.

Data: realm, application name

Triggers: Save application API is called.

SUCCEEDED_SAVE_APPLICATION

ID: ENTITLEMENT-102

Level: INFO

Description: Application is saved.

Data: realm, application name

Triggers: Save application API is called.

FAILED_SAVE_APPLICATION

ID: ENTITLEMENT-103

Level: INFO

Description: Failed to save application.

Data: realm, application name, error message

Triggers: Save application API is called.

Actions: Administrator might not have the permission to save application.

ATTEMPT_REMOVE_APPLICATION

ID: ENTITLEMENT-111

Level: INFO

Description: Attempt to remove application.

Data: realm, application name

Triggers: Remove application API is called.

SUCCEEDED_REMOVE_APPLICATION

ID: ENTITLEMENT-112

Level: INFO

Description: Application is removed.

Data: realm, application name

Triggers: Remove application API is called.

FAILED_REMOVE_APPLICATION

ID: ENTITLEMENT-113

Level: INFO

Description: Failed to remove application.

Data: realm, application name, error message

Triggers: Remove application API is called.

Actions: Administrator might not have the permission to remove application.

OpenAM logs the following LOG messages.

LOG_START_NEW_LOGGER

ID: LOG-1

Level: INFO

Description: Logging Started - New Logger

Data: current location

Triggers: Logging started by getting a new Logger.

LOG_END

ID: LOG-2

Level: INFO

Description: Logging Terminated - Server Stopped

Data: current location

Triggers: Logging terminated by server shutdown.

LOG_START_CONFIG

ID: LOG-3

Level: INFO

Description: Logging Started - Configuration Change

Data: old location, new location, old backend, new backend, old security status, new security status, old status, new status, old level, new level

Triggers: Logging started after logging configuration change.

LOG_END_CONFIG

ID: LOG-4

Level: INFO

Description: Logging Terminated - Configuration Change

Data: old location, new location, old backend, new backend, old security status, new security status, old status, new status, old level, new level

Triggers: Logging terminated by logging configuration change.

OpenAM logs the following OAuth2Provider messages.

CREATED_TOKEN

ID: OAuth2Provider-1

Level: INFO

Description: Created an oauth 2.0 token

Data: message, token info

Triggers: Creating a new oauth 2.0 token

DELETED_TOKEN

ID: OAuth2Provider-2

Level: INFO

Description: Deleted an oauth 2.0 token

Data: message, token info

Triggers: Deleteing an oauth 2.0 token

FAILED_CREATE_TOKEN

ID: OAuth2Provider-3

Level: INFO

Description: Failed to creating an oauth 2.0 token

Triggers: Failed creating an oauth 2.0 token

FAILED_DELETE_TOKEN

ID: OAuth2Provider-4

Level: INFO

Description: Failed deleting an oauth 2.0 token

Triggers: Failed deleting an oauth 2.0 token

CREATED_CLIENT

ID: OAuth2Provider-11

Level: INFO

Description: Created an oauth 2.0 Client

Data: message, token info

Triggers: Creating a new oauth 2.0 client

DELETED_CLIENT

ID: OAuth2Provider-12

Level: INFO

Description: Deleted an oauth 2.0 client

Data: message, token info

Triggers: Deleteing an oauth 2.0 client

FAILED_CREATE_CLIENT

ID: OAuth2Provider-13

Level: INFO

Description: Failed to creating an oauth 2.0 client

Triggers: Failed creating an oauth 2.0 client

FAILED_DELETE_CLIENT

ID: OAuth2Provider-14

Level: INFO

Description: Failed deleting an oauth 2.0 client

Triggers: Failed deleting an oauth 2.0 client

AUTHENTICATED_CLIENT

ID: OAuth2Provider-15

Level: INFO

Description: Authenticated an oauth 2.0 client

Data: message, client id

Triggers: Authenticating a oauth 2.0 client

FAILED_AUTHENTICATE_CLIENT

ID: OAuth2Provider-16

Level: INFO

Description: Failed authenticating an oauth 2.0 client

Triggers: Failed authenticating an oauth 2.0 client

OpenAM logs the following POLICY messages.

POLICY_EVALUATION

ID: POLICY-1

Level: INFO

Description: Evaluating policy succeeded

Data: policy name, realm name, service type name, resource name, action names, policy decision

Triggers: Evaluating policy.

PROTECTED_RESOURCES

ID: POLICY-2

Level: INFO

Description: Getting protected policy resources succeeded

Data: principal name, resource name, protecting policies

Triggers: Getting protected policy resources.

POLICY_CREATE_SUCCESS

ID: POLICY-3

Level: INFO

Description: Creating policy in a realm succeeded

Data: policy name, realm name

Triggers: Creating policy in a realm.

POLICY_MODIFY_SUCCESS

ID: POLICY-4

Level: INFO

Description: Modifying policy in a realm succeeded

Data: policy name, realm name

Triggers: Modifying policy in a realm.

POLICY_REMOVE_SUCCESS

ID: POLICY-5

Level: INFO

Description: Removing policy from a realm succeeded

Data: policy name, realm name

Triggers: Removing policy from a realm.

POLICY_ALREADY_EXISTS_IN_REALM

ID: POLICY-6

Level: INFO

Description: Policy already exists in the realm

Data: policy name, realm name

Triggers: Creating policy in the realm.

UNABLE_TO_ADD_POLICY

ID: POLICY-7

Level: INFO

Description: Creating policy in a realm failed

Data: policy name, realm name

Triggers: Creating policy in a realm.

Actions: Check if the user has privilege to create a policy in the realm.

UNABLE_TO_REPLACE_POLICY

ID: POLICY-8

Level: INFO

Description: Replacing policy in a realm failed

Data: policy name, realm name

Triggers: Replacing policy in a realm.

Actions: Check if the user has privilege to replace a policy in the realm.

DID_NOT_REPLACE_POLICY

ID: POLICY-81

Level: INFO

Description: Did not replace policy - A diifferent policy with the new name already exists in the realm

Data: new policy name, realm name

Triggers: Replacing policy in a realm

UNABLE_TO_REMOVE_POLICY

ID: POLICY-9

Level: INFO

Description: Removing policy from a realm failed

Data: policy name, realm name

Triggers: Removing policy from a realm.

Actions: Check if the user has privilege to remove a policy from the realm.

PROXIED_POLICY_EVALUATION

ID: POLICY-10

Level: INFO

Description: Computing policy decision by an administrator succeeded

Data: admin name, principal name, resource name, policy decision

Triggers: Computing policy decision by an administrator.

PROXIED_POLICY_EVALUATION_IGNORING_SUBJECTS

ID: POLICY-11

Level: INFO

Description: Computing policy decision by an administrator ignoring subjects succeeded

Data: admin name, resource name, policy decision

Triggers: Computing policy decision by an administrator ignoring subjects.

OpenAM logs the following SESSION messages.

SESSION_CREATED

ID: SESSION-1

Level: INFO

Description: Session is Created

Data: User ID

Triggers: User is authenticated.

SESSION_IDLE_TIMED_OUT

ID: SESSION-2

Level: INFO

Description: Session has idle timedout

Data: User ID

Triggers: User session idle for long time.

SESSION_MAX_TIMEOUT

ID: SESSION-3

Level: INFO

Description: Session has Expired

Data: User ID

Triggers: User session has reached its maximun time limit.

SESSION_LOGOUT

ID: SESSION-4

Level: INFO

Description: User has Logged out

Data: User ID

Triggers: User has logged out of the system.

SESSION_REACTIVATION

ID: SESSION-5

Level: INFO

Description: Session is Reactivated

Data: User ID

Triggers: User session state is active.

SESSION_DESTROYED

ID: SESSION-6

Level: INFO

Description: Session is Destroyed

Data: User ID

Triggers: User session is destroyed and cannot be referenced.

SESSION_PROPERTY_CHANGED

ID: SESSION-7

Level: INFO

Description: Session's property is changed.

Data: User ID

Triggers: User changed session's unprotected property.

SESSION_UNKNOWN_EVENT

ID: SESSION-8

Level: INFO

Description: Session received Unknown Event

Data: User ID

Triggers: Unknown session event

SESSION_PROTECTED_PROPERTY_ERROR

ID: SESSION-9

Level: INFO

Description: Attempt to set protected property

Data: User ID

Triggers: Attempt to set protected property

SESSION_QUOTA_EXHAUSTED

ID: SESSION-10

Level: INFO

Description: User's session quota has been exhausted.

Data: User ID

Triggers: Session quota exhausted

SESSION_DATABASE_UNAVAILABLE

ID: SESSION-11

Level: INFO

Description: Session database used for session failover and session constraint is not available.

Data: User ID

Triggers: Unable to reach the session database.

SESSION_DATABASE_BACK_ONLINE

ID: SESSION-12

Level: INFO

Description: Session database is back online.

Data: User ID

Triggers: Session database is back online..

SESSION_MAX_LIMIT_REACHED

ID: SESSION-13

Level: INFO

Description: The total number of valid sessions hosted on the AM server has reached the max limit.

Data: User ID

Triggers: Session max limit reached.

Chapter 3

Error Messages

This chapter lists common error messages from OpenAM, with remedial actions where possible.

Common Authentication Errors

An error occurred while storing the user profile.

When using the Membership module, the attributes and elements likely do not match the self-registration settings in the `Membership.xml` file.

Action: Enter a unique user name.

A user already exists with this name in the given organization.

When using the Membership module, you cannot create a new user with the same user name as an existing user.

Action: Enter a unique user name.

Authentication Exception

The authentication was not handled properly.

Action: Check the login URL for invalid characters, especially in the query string parameters.

Authentication Failed

Usually this occurs when the user provides incorrect credentials.

Action: If the credentials are valid and correct, check that you are using the correct authentication module.

Cannot redirect to default page

OpenAM cannot redirect to the Success URL or the Failure URL.

Action: Check the web application container logs where OpenAM is running.

Invalid Password

The password is not valid.

Action: If you have not incorrectly typed the password, check that the password has at least 8 characters, and has not expired.

Logout Failure

The user cannot log out.

Action: Restart OpenAM.

Maximum Session Limit was reached

Action: Logout and login again.

Missing the confirmation password field.

When using the Membership module to create a user account, you must confirm the password value.

Action: Enter a the password again.

No password was entered

When using the Membership module to create a user account, you must enter a password.

Action: Enter a password.

No user name was entered

When using the Membership module to create a user account, you must enter a user name.

Action: Enter a user name.

No user profile was found matching the entered user name in the given organization.

When using the Membership module, no profile exists for the user.

Action: Select New User from the login screen.

No configuration found

Action: Check the configuration for the authentication module or chain for the realm.

No organization found

Action: Check that the requested realm exists.

One of the required fields was not completed.

Action: Check for missing required fields.

Specified authentication module is denied.

Action: Check that the authentication module is registered in the realm, that templates are in place for the module, and that the module is selected in the Core Authentication module list.

This organization is not active

The requested realm is set to Inactive.

Action: Change the status in OpenAM Console.

The password and the confirm password do not match.

Error shown when using the Membership module.

Action: Type the password values again.

The password entered does not contain enough characters.

When using the Membership module, the password provided has fewer than 8 characters.

Action: Enter a longer password.

The User Name and Password fields cannot have the same value.

When using the Membership module, you cannot create a user with identical user name and password values.

Action: Use a different user name or password.

User has no profile in the specified organization.

Action: Check that the user exists in the subjects for the realm.

User is not active

Action: Change the user status from inactive to active in OpenAM console.

User session has timed out.

Action: Log in again.

You are already logged in

No Success URL redirect is defined for the user.

Action: Set up an appropriate Success URL redirect, or use the `goto` parameter in the login URL query string.

Common Console Errors

Could not create identity object. User does not have sufficient access.

Permissions prevented the operation.

Action: Perform the operation as a user with sufficient access, or have an administrator grant you sufficient access.

Invalid user's start location. Please contact your administrator.

The Administrator DN is no longer valid.

Action: Edit the User service to use the proper value for the Administrator DN.

Size limit exceeded.

Your search returned more entries that the data store allows.

Action: Refine your search, or increase Maximum Results Returned from a Search in the Administration service.

Time limit exceeded.

Your search took more time to search the data store than was allowed.

Action: Refine your search, or increase Timeout for Search in the Administration Service.

There are no attributes to display.

No user-editable attributes are defined for the selected object.

There are no entities.

What you are searching for did not match anything in the data store.

Action: Refine your search.

Unable to get attribute from data store.

Occurs when a profile has been modified concurrently by another user.

Action: Refresh the display.

FORGEROCK

Chapter 4
Ports Used

OpenAM software uses the following TCP/IP ports by default. Sometimes multiple services are configured on a single system with slightly different port numbers. For example, while the default port number for a servlet container such as Tomcat is 8080, a second instance of Tomcat might be configured with a port number of 18080. In all cases shown, communications proceed using TCP.

When you configure a firewall for OpenAM, make sure to include open ports for any installed and related components, including web services (80, 443), servlet containers (8009, 8080, 8443), and external applications such as a Remote Access Dial In User Service (1645).

Additional ports may be used, depending on other components of your deployment. If you are using external OpenDJ servers, refer to the *Ports Used* appendix of the OpenDJ Administration Guide.

Table 4.1. Default TCP/IP Ports Used by OpenAM

Port Number	Description
1689	Port for Java Management eXtension traffic, disabled by default
4444	Port for the embedded administration connector, enabled by default.
8080	Web application container port number
8082	HTTP port for monitoring OpenAM, disabled by default
8085	SNMP port for monitoring OpenAM, disabled by default
9999	RMI port for monitoring OpenAM, disabled by default.
50389, 50899, 58989	Supports LDAP communication between embedded OpenAM data stores.
57943, 58943	Used by the *SecurID Authentication Module* in the *Administration Guide*.

Chapter 5
Localization

This chapter lists languages and locales supported for OpenAM.

OpenAM console and end user pages are localized for the following languages.

- English

- French

- German

- Japanese

- Korean

- Simplified Chinese

- Spanish

- Traditional Chinese

OpenAM supports the following locales.

Afrikaans

Code tag: af

Albanian

Code tag: sq

Basque

Code tag: eu

Byelorussian

Code tag: be

Bulgarian

Code tag: bg

Catalan

Code tag: ca

Chinese

Code tag: zh

Croatian

Code tag: hr

Czech

Code tag: cs

Danish

Code tag: da

Dutch

Code tag: nl

English

Code tag: en

Faroese

Code tag: fo

Finnish

Code tag: fi

French

Code tag: fr

Galician

Code tag: gl

German

Code tag: de

Greek

Code tag: el

Hungarian

Code tag: hu

Icelandic

Code tag: is

Indonesian

Code tag: id

Irish

Code tag: ga

Italian

Code tag: it

Japanese

Code tag: ja

Korean

Code tag: ko

Norwegian

Code tag: no

Polish

Code tag: pl

Portuguese

Code tag: pt

Romanian

Code tag: ro

Russian

Code tag: ru

Serbian

Code tag: sr

Slovakian

Code tag: sk

Slovenian

Code tag: sl

Spanish

Code tag: es

Swedish

Code tag: sv

Turkish

Code tag: tr

Ukrainian

Code tag: uk

FORGEROCK

Chapter 6
Supported Standards

OpenAM implements the following RFCs, Internet-Drafts, and standards.

OAuth 2.0

The OAuth 2.0 Authorization Framework, in which OpenAM can play the roles of authorization server and of client.

The OAuth 2.0 Authorization Framework: Bearer Token Usage, in which OpenAM plays the role of authorization server.

Assertion Framework for OAuth 2.0, which is an Internet-Draft.

SAML 2.0 Bearer Assertion Profiles for OAuth 2.0, which is an Internet-Draft.

JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants, which is an Internet-Draft.

OpenID Connect 1.0

OpenAM plays the role of OpenID provider. The OpenID Connect specifications also depend on OAuth 2.0, JSON Web Token, and Simple Web Discovery and related specifications. The following descriptions are from the OpenID Connect 1.0 web site.

Basic Client Profile. Lightweight simple self-contained specification for a web-based Relying Party using the OAuth code flow.

Implicit Client Profile. Lightweight simple self-contained specification for a web-based Relying Party using the OAuth implicit flow.

Discovery. Defines how user and provider endpoints are dynamically discovered.

Dynamic Registration. Defines how clients dynamically register with OpenID Providers.

Standard. Full HTTP binding specification, for both clients and OpenID Providers; references Messages.

Messages. Lists all the messages that are used in OpenID Connect. You can use this to create additional bindings for Connect, such as an OpenID Connect binding for XMPP.

Session Management. Defines how to manage OpenID Connect sessions.

OAuth 2.0 Multiple Response Types. Registration document for several specific new response types, in accordance with the stipulations of the OAuth Parameters Registry.

Representational State Transfer (REST)

Style of software architecture for web-based, distributed systems.

Security Assertion Markup Language (SAML)

Standard, XML-based framework for creating and exchanging security information between online partners. OpenAM supports multiple versions of SAML including 2.0.

Liberty Alliance Project Identity Federation Framework (Liberty ID-FF)

Federation standard, whose concepts and capabilities contributed to SAML 2.0.

Simple Object Access Protocol

Lightweight protocol intended for exchanging structured information in a decentralized, distributed environment.

Web Services Description Language (WSDL)

XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information.

Web Services Federation Language (WS-Federation)

Identity federation standard, part of the Web Services Security framework.

eXtensible Access Control Markup Language (XACML)

Declarative access control policy language implemented in XML, and also a processing model, describing how to interpret policies.

Chapter 7
Service Endpoints

A service endpoint is a URL which serves as the access port for a web service. It may be a standard HTML-based web page, or it may be a *.jsp page.

As every service endpoint is a potential security issue, it may be appropriate to restrict access to some of those endpoints that you do not use. But be careful. Some endpoints, such as `isAlive.jsp` in the main /path/to/tomcat/webapps/openam directory, are essential and should not be blocked or changed.

Given the large number of available endpoints, this chapter has been organized primarily by subdirectory. Most of the directories were created when the OpenAM war archive was copied to the appropriate web application container, such as the webapps/ subdirectory.

OpenAM may expose several hundred service endpoints, listed in this chapter. Each endpoint shown is listed relative to the deployment URL. For example, if you have deployed OpenAM at `https://openam.example.com:8443/openam/`, the full URL to the `isAlive.jsp` endpoint is `https://openam.example.com:8443/openam/isAlive.jsp`.

OpenAM includes two types of endpoints. One is based on URL patterns, shown with the `url-pattern` tag. You can find these patterns in the web.xml file, in the /path/to/tomcat/webapps/openam/WEB-INF directory. The other type is based on *.jsp pages, starting in the main /path/to/tomcat/webapps/openam directory, and also in many associated subdirectories. If you copied or created a WAR archive to a name other than `openam.war`, as described in the installation guide, substitute for the second `openam` accordingly.

Some of these endpoints can be applied directly to a URL when you've connected to the OpenAM server; for example, if you've configured OpenAM on `http://idp.example.com:8080/openam`, you can log in and review debug options by navigating to `http://idp.example.com:8080/openam/Debug.jsp`

Other endpoints can only be used when called by some option in the OpenAM console. For example, while the AgentAdd.jsp endpoint exists in the console/agentconfig subdirectory, you would get an error by navigating directly to a URL such as `http://sp.example.com:8080/openam/console/agentconfig/AgentAdd.jsp`. For that particular endpoint, you'll have click through the options required to add an agent. (Access Control > *realm name* > Agents > Agent > New)

In general, this chapter does not include dynamic endpoints, such as those that may include security tokens. The endpoints described in this chapter are based on files included in the installation of an OpenAM server.

There have been two security advisories related to OpenAM endpoints: OpenAM Security Advisory #201203 and OpenAM Security Advisory #201204

Several options are available for endpoints at risk. Recommendations from the noted security advisories include the following:

- Filter requests to prevent or restrict access to vulnerable endpoints with a reverse proxy or equivalent hardware device. Such options can be configured to limit access by IP address or fully-qualified domain name.

- Use a patch. If available, download links should be listed in the security advisory. The patch may be limited to one or more endpoint files.

- Remove access from the configuration. If a problematic endpoint is configured in the web.xml file of the aforementioned WEB-INF subdirectory, you can remove the section that points to that endpoint.

- Remove the endpoint file from the configuration. Some endpoint files, such as proxy.jsp or ssoadm.jsp, are not essential to the basic operation of OpenAM.

Of course, you can take additional steps to help secure your OpenAM deployment. For more information, see the the chapter on *Securing OpenAM in the Administration Guide* in the *Administration Guide*.

7.1. JSP Endpoints

The OpenAM WAR archive includes *.jsp files in a number of different categories. Many are associated with the applicable subdirectory, such as console/realm. The following sections will examine each *.jsp file, divided by subdirectories.

In some highlighted cases, the noted *.jsp file appears in the code for one or more .java files. If you remove the noted *.jsp file from the container, there is a risk that will break some functionality within OpenAM. In other cases, such as any files related to the GUI installation wizard, the applicable *.jsp file can be safely removed from a production system.

7.2. Main Directory JSP Endpoints

If you're working in Tomcat, you'll find the endpoints in this subsection in the /path/to/tomcat/webapps/openam directory. For other web application containers, you may find the endpoints in a different openam subdirectory.

Debug.jsp

Supports debug logging by service. For more information, see the *Administration Guide* chapter on *Debug Logging by Service.* in the *Administration Guide*

encode.jsp

Enables access to a page that encodes text passwords. The algorithm is based on PBEWithMD5AndDES, password-based encryption (PBE) using the MD5 message-digest algorithm, configured with the data encryption standard (DES)

getServerInfo.jsp

Supports requests for server information. As getServerInfo.jsp is encoded in some .java files, you should retain getServerInfo.jsp in your deployment.

isAlive.jsp

Verifies the current status of the OpenAM service; the "Server is ALIVE:" message also verifies activity on OpenAM systems behind load balancers. This can be a useful tool in a production environment.

nowritewarning.jsp

Displays a permission error message, used by the GUI-based installation wizard.

proxyidpfinder.jsp

Supports access to a remote identity provider, through the federation broker.

services.jsp

Lists active services within OpenAM. The details shown on this page can be used with the `ssoadm` command to create a second OpenAM server with matching services. Be aware, the amadmin administrative user is hard-coded into this file. If you change the identity of the administrative user to something other than amadmin, that user won't have access to services.jsp.

showServerConfig.jsp

Specifies configuration information for the system, including the URL, the OS, the Java VM, the configuration directory, and more.

ssoadm.jsp

Supports GUI-based access to the options associated with the `ssoadm` command. The ssoadm.jsp file is disabled by default. Instructions for enabling this feature are available from the *Administration Guide* entry on *OpenAM ssoadm.jsp.* in the *Administration Guide*

validateWait.jsp

May be called by the validator.jsp or validatorMain.jsp files, to display progress in verifying the status of federation.

validator.jsp

Refers to the ValidateSAML2 function to identify the realm, IdP and SP for the federation.

validatorAuthFail.jsp

Starts an "Authentication Failed" message.

validatorFooter.jsp

Incorporates a "Back to Login" button in validatorMain.jsp.

validatorMain.jsp

Sets up a federation connectivity test. If you've set up a Federation Circle of Trust, this file is accessible from the "Test Federation Connectivity" option in the main OpenAM console.

validatorRpt.jsp

Opens a "Connectivity Test Results" window, specifying the status of a federation circle of trust. Tests relate to IdP authentication, SP authentication, account linking, single log out, single sign on, and account unlinking.

validatorStatus.jsp

Adds information to validator.jsp and validatorMain.jsp with federation status information as it relates to the currently configured circle of trust.

All of the validat*.jsp files near the end of this list relate to testing and verifying federation. It requires at least one identity provider (IDP) and one service provider (SP). At least one of these components must be configured remotely to set up a valid Circle of Trust (COT). If federation does not apply to your configuration, the validat*.jsp files are not essential to your configuration.

7.3. User Interface JSP Endpoints

The endpoints in this section can be found in several com_sun_web_ui/jsp/ subdirectories. These endpoints appear to relate to JavaHelp; per OPENAM-806, this functionality was removed from OpenAM, starting with version 9.5.3. Thus, the endpoints in this section, with one possible exception (Masthead.jsp in the com_sun_web_ui/jsp/version subdirectory) may no longer serve any purpose.

DateTimeWindow.jsp

The only endopint in the com_sun_web_ui/jsp/datetime subdirectory. May be a legacy endpoint; it calls a DateTimeWindowViewBean class; the corresponding .java file does not exist in the current trunk.

Help.jsp

One of two endpoints in the com_sun_web_ui/jsp/help subdirectory. May be a legacy endpoint; it calls a HelpViewBean class; the corresponding .java file does not exist in the current trunk.

Masthead.jsp

One of two endpoints in the com_sun_web_ui/jsp/help subdirectory. Also exists in a slightly different format in the com_sun_web_ui/jsp/help2 subdirectory, as well as the com_sun_web_ui/jsp/version subdirectory. May be a legacy endpoint; it calls a MastheadViewBean class; the Masthead.jsp file and the corresponding MastheadViewBean.java were last changed in 2004.

(However, the Masthead.jsp file in the com_sun_web_ui/jsp/version subdirectory includes a VersionViewBean.java file that is used by the Version.jsp endpoint used in the console/base subdirectory.

ButtonNav.jsp

Specifies an endpoint in the com_sun_web_ui/jsp/help2 directory. Points to a ButtonNavViewBean class; the associated .java file no longer exists in the trunk.

Help2Ie.jsp

Specifies an endpoint in the com_sun_web_ui/jsp/help2 directory. Points to a Help2ViewBean class; the associated .java file no longer exists in the trunk.

Help2Nav4.jsp

Specifies an endpoint in the com_sun_web_ui/jsp/help2 directory. Points to a Help2ViewBean class; the associated .java file no longer exists in the trunk.

Help2Nav6up.jsp

Specifies an endpoint in the com_sun_web_ui/jsp/help2 directory. Points to a Help2ViewBean class; the associated .java file no longer exists in the trunk.

Navigator.jsp

Specifies an endpoint in the com_sun_web_ui/jsp/help2 directory. Points to a NavigatorViewBean class; the associated .java file no longer exists in the trunk.

AdvancedSort.jsp

Specifies an endpoint in the com_sun_web_ui/jsp/table directory.

Table.jsp

Specifies an endpoint in the com_sun_web_ui/jsp/table directory. Points to a TableViewBean class; the associated .java file no longer exists in the trunk..

WizardWindow.jsp

Points to an endpoint in the com_sun_web_ui/jsp/wizard subdirectory. Points to a WizardWindowViewBean class, which appears to be unused by any other .jsp file.

7.4. Default Authentication JSP Endpoints

Many of the .jsp files in this category can be modified to help you modify the messages that appear to users in the OpenAM console. Standard messages for most of these endpoints can be found in the amAuth.properties and amAuthUI.properties files. You'll find the endpoints in this subsection in the config/auth/default subdirectory.

account_expired.jsp

Specifies an error page for account expiration. The message displayed to the user can be modified in the amAuthUI.properties file.

authException.jsp

Option to Exception.jsp; called if there is an existing resource bundle, as specified in AuthExceptionViewBean.java.

auth_error_template.jsp

Specifies an error page for authentication errors. The message displayed to the user can be modified in the amAuthUI.properties file.

disclaimer.jsp

Associated with the self-registration module, which can be configured in the OpenAM Console, under Access Control > Realm Name > Authentication > Module Instances. The default disclaimer is associated with the disclaimer.notice parameter, defined in the amAuthUI.properties file.

disclaimerDeclined.jsp

Associated with the self-registration module, which can be configured in the OpenAM Console, under Access Control > Realm Name > Authentication > Module Instances. The default disclaimer_denied message is associated with the disclaimer.declined parameter, defined in the amAuthUI.properties file.

Exception.jsp

Includes the following error message: "Authentication Service is not initialized." Cited by several other .java files in the code, so it should not be removed in a secure deployment..

invalidAuthlevel.jsp

Used to specify an issue with the authentication level. The default invalidauthlevel and contactadmin messages can be redefined in the amAuthUI.properties file.

invalidPCookieUserID.jsp

Notes a problem with a specified user name for a cookie, which presumably does not exist in the relevant domain. The default cookie.notpersistent and contactadmin messages can be modified in the amAuthUI.properties file.

invalid_domain.jsp

Displays a "No such Organization found" message when a domain is not defined in the OpenAM database. Refers to the nosuch.domain parameter in the amAuthUI.properties file.

login_denied.jsp

Defines the response of OpenAM to a user who enters an undefined profile. Uses the userhasnosuchprofile.org and contactadmin parameters in the amAuthUI.properties file.

login_failed_template.jsp

Provides a message in the event of a login failure. The message uses the auth.failed parameter in the amAuthUI.properties file.

Login.jsp

Specifies a regular authentication template. As noted in the *Administration Guide* entry on *Securing OpenAM Administration* in the *Administration Guide*, the Login.jsp file may be customized for different deployments.

Logout.jsp

The Logout.jsp file may also be customized for different deployments.

maxSessions.jsp

Specifies the message given to users when the number of sessions has hit the preconfigured limit. The default is 5000, defined in the OpenAM console under Configuration > Servers and Sites > Default Server Settings > Session. The message uses the session.max.limit parameter defined in the amAuthUI.properties file.

membership.jsp

Specifies information for the page associated with the self-registration module.

Message.jsp

Calls text messages related to the authentication process.

module_denied.jsp

Includes a message to a target user that he does not have access to a specified module. The message uses the authmodule.denied parameter defined in the amAuthUI.properties file..

module_template.jsp

Adds a page which can be used to help customize appropriate modules.

new_org.jsp

Includes a warning when a user is trying to access a different realm. The message uses the newOrg.agree parameter, as defined in the amAuthUI.properties file.

noConfig.jsp

Specifies the lack of a defined configuration module. The message uses the noconfig.found parameter, defined in the amAuthUI.properties file.

OAuthActivate.jsp

Shows a default template for entering an activation code. Used by OAuth.xml for password changes. As this file is not configured for OAuth2, the file is deprecated and may be removed from a future release.

OAuthPwd.jsp

Displays a password change screen, with an option for terms and conditions of service. As this file is not configured for OAuth2, it is deprecated and may be removed from a future release.

org_inactive.jsp

Transmits the message that the target organization is not active in the OpenAM database.

profileError.jsp

Specifies the message that is sent when there's a failure in the use of the self-registration module. Associated with the profile.error parameter, defined in the amAuthUI.properties file.

Redirect.jsp

Notes a file used by other code to redirect users for events such as login failures.

register.jsp

Identifies the page with the self-registration template.

session_timeout.jsp

Adds a message to a user when a session has gone past its allocated login time. Uses the session.timeout parameter, defined in the amAuthUI.properties file.

userDenied.jsp

Associated with role-based authentication. Tells a user when the required role has not been configured for that user. Message defined by the user.not.inrole parameter, defined in the amAuthUI.prooperties file.

user_inactive.jsp

Identifies a message sent to a user that is not currently active in the database. Message defined by the usernot.active parameter, as shown in the amAuthUI.properties file.

7.5. Default Federation JSP Endpoints

Many of the files in this config/federation/default subdirectory use the com.sun.liberty.LibertyManager interface. In general, you'll want to keep these files in a production

deployment, to support adding to and deleting users from different Circles Of Trust (COT). Many of these files are customizable for different organizational interfaces. Interfaces in different languages may be configured in slightly different subdirectories such as config/federation/default_fr.

`cdclogin.jsp`

Supports a non-blank page for cross-domain single sign-ons; associated with a Cross-Domain Controller (CDC) servlet.

`CommonLogin.jsp`

Supports links to login pages of trusted identity providers.

`Error.jsp`

Sets up an error message, using the com.sun.liberty.LibertyManager interface.

`Federate.jsp`

Supports a connection to providers that can be configured in a federation.

`FederationDone.jsp`

Specifies the status of a federation request; the default response is either "The user has cancelled account federation." or "Federation has been successfully completed with the remote provider.

`Footer.jsp`

Sets up code that you can use to include a custom footer on all pages.

`Header.jsp`

Sets up code that you can use to include a custom header on all pages; the default version is configured with the OpenAM logo.

`ListOfCOTs.jsp`

When a service provider (SP) belongs to more than one COT, this page prompts the user to select a preferred identity provider (IDP).

`LogoutDone.jsp`

Specifies success or failure during a logout operation. Where a user has an account on multiple providers, he may see the following message: "Unable to log the user out from one or more providers where the user may still have active sessions."

`NameRegistration.jsp`

Supports registration with a new remote provider; this endpoint is associated with NameRegistrationDone.jsp.

`NameRegistrationDone.jsp`

Displays different messages based on a registration attempt with a remote provider. The message varies depending on whether the request was successful, a failure, or cancelled.

`Termination.jsp`

Supports defederation from an existing remote provider; goes with TerminationDone.jsp.

`TerminationDone.jsp`

Displays different messages based on a defederation attempt with a remote provider. The message varies depending on whether the request was successful, a failure, or cancelled.

7.6. Console Agent Configuration JSP Endpoints

The JSP files in the console/agentconfig subdirectory relate to the configuration of Web Agents. To see what is done by each JSP file, log into the console as the administrator. Select Access Control > *[Some Realm]* > Agents. Several of the options that appear corresponds to the JSP files in the target subdirectory.

Some of the endpoints include messages from relevant sections of the amConsole.properties file. The agents in this directory are part of the com.sun.identity.console.agentconfig package.

Several endpoints relate to Web Service Client (WSC) policy agents, which secure outgoing requests and validate incoming requests from Web Service Providers (WSP). For more information, see the chapter on *Configuring Policy Agent Profiles* in the Administrative Guide in the *Administration Guide*.

If you are not using agent functionality such as that related to the Security Token Service (STS), the related endpoints listed in this section may not be essential in a production deployment.

`AgentAdd.jsp`

Includes a newly created web agent for a specified realm. The AgentAdd page appears in the OpenAM console after an agent is added to a realm.

`AgentConfigInherit.jsp`

Allows an administrator to review default settings for the agent, as configured in the Inheritance Settings page. Inheritance assumes that agent is part of a previously confiugred group. To access Inheritance Settings, refer to the *Creating Agent Profiles" section of the Administration Guide* in the *Administration Guide*.

`AgentDump.jsp`

Displays information about the current configuration of an agent or an agent group, and how it might be exported.

AgentExportPolicy.jsp

Shows how the information about an agent may be exported.

AgentGroup.jsp

Includes a newly created agent group for common web agents within a specified realm. The AgentGroup page appears in the OpenAM console after an agent is added to a realm.

AgentGroupMembers.jsp

Supports the display of agents that are members of a specified agent group.

Agents.jsp

Enables access to a form to specify a new agent to add. The same form is used for every category of new agents configured from the OpenAM console, when you navigate to Access Control -> [Realm name] -> Agents.

Home.jsp

Per comments in the HomeViewBean, this file should forward requests for other agents.

WebServiceClientEdit.jsp

Includes customizable options for web service clients. Accessible when you edit and then save or export the configuration for a specific web service client.

WebServiceProviderEdit.jsp

Includes customizable options for web service providers. Accessible when you edit and then save or export the configuration for a specific web service provider.

WebServiceSTSEdit.jsp

Includes customizable options for web service STS providers. Accessible when you edit and then save or export the configuration for a specific web service STS provider.

WebServiceUserCredAdd.jsp

Supports the configuration of an WSP agent username and password.

WebServiceUserCredEdit.jsp

Supports changes to an WSP agent username and password.

7.7. Console Ajax JSP Endpoints

The only JSP file that appears to be active in this subdirectory is AjaxProxy.jsp, which appears to be used by several other endpoints.

AjaxProxy.jsp

Specifies an element used by several other endpoints, including ConfigureGoogleApps.jsp and ConfigureSalesForceApps.jsp.

FileUpload.jsp

Used by the FileUploader.jsp endpoint, described in the section on Federation Console JSP Endpoints.

7.8. Console Authentication JSP Endpoints

You can find console authentication endpoints in the console/authentication subdirectory. The associated endpoints relate to authentication settings in a realm. To access these endpoints, navigate to Access Control > *[some realm]* > Authentication.

AuthConfig.jsp

Part of the creation of a New Authentication Chain; associated with the Authentication Chaining section of the Authentication tab for a realm.

AuthProperties.jsp

Specifies properties that might be configured under the authentication tab for a specific or top-level realm.

CoreAttributes.jsp

Associated with the Core section of the Authentication tab of a specific or the top-level realm. Includes options for Realm Attributes, Persistent Cookies, Account Lockout, and Post-Authentication Processing.

EditAuthType.jsp

Supports changes to Module Instances, under the Authentication tab of a specific or the top-level realm.

NewAuthConfig.jsp

Associated with the creation of a New Authentication Chain, an option available from the Authentication Chaining section of the Authentication tab.

NewAuthInstance.jsp

Supports the implementation of a new authentication module, available from the Module Instances section of the Authentication tab.

ReorderAuthChains.jsp

> Supports a change in sequence of authentication criteria; to access, select an existing Authentication Chaining service under the Authentication tab for a specified realm.

7.9. Base Console JSP Endpoints

The endpoints in this subdirectory (console/base) relate to options associated with the "home page" for the OpenAM GUI console; in essence, these are the options available when you log in as the administrative user (typically `amadmin`).

AMAdminFrame.jsp

> Defaults to the opening page for the OpenAM console.

AMInvalidURL.jsp

> Provides an "Invalid URL" error message.

AMLogin.jsp

> Redirects users to the default login page; assumes no user is currently logged into OpenAM.

AMPost.jsp

> Endpoint that either returns success of a post or an "Invalid or Missing Input" error.

AMUncaughtException.jsp

> Default uncaught exception error message endpoint: "An error occurred while processing this request. Contact your administrator."

Authenticated.jsp

> Displays a "You're logged in" information message.

CloseWindow.jsp

> Endpoint that closes existing windows.

Message.jsp

> Specifies a template endpoint used for messages.

Version.jsp

> Specifies current version information, copyright notice, and licensing.

7.10. Delegation Console JSP Endpoints

The two service endpoints under the console/delegation subdirectory relate to the privileges associated with configured realms.

`Delegation.jsp`

Associated with the privileges for a realm. The privileges can be assigned for different groups of users, as configured via Access Control > *[realm]* > Subjects > Group.

`DelegationProperties.jsp`

Supports changes in properties for group privileges, described in the Delegation.jsp endpoint. To get to these properties, select Access Control > *[some realm]* > Privileges > *[name of group]*.

7.11. Federation Console JSP Endpoints

The JSP files in this section relate to federation, specified in the console/federation subdirectory. Specifically, when you access the OpenAM GUI console and click the Federation tab, the variety of options that you select call the JSP files in this directory. References in each JSP file in that subdirectory are associated with the Federation tab.

Generally, the JSP files in this directory are essential if you want to add or modify federation partners in your Circles of Trust (COT), SAMLv2 / ID-FF / WS-Federation entity providers, and SAML 1.x configured partners.

If you're not using the legacy elements of federation, such as Liberty ID-FF, WS-Federation, and SAML 1.x, you may be able to delete related service endpoints in a more secure deployment.

Many of the endpoints in this section are accessible from the OpenAM console, under the Federation tab. Some of the endpoints are accessible only after you've created an appropriate entity provider, such as SAMLv2, ID-FF, or WS-Federation.

`CreateCOT.jsp`

When you create a Circle of Trust (COT) via Federation > New, you can access the COT Configuration window. You can then access all configured COTs.

`CreateSAML2MetaData.jsp`

Used when creating a new entity provider, configured with the SAML2 protocol.

`FSAuthDomainsEditViewBean.jsp`

Associated with an edit of a COT; to access, select a previously configured COT.

`FSSAMLSelectTrustedPartnerType.jsp`

Opened when you configure a new Trusted Partner under the SAML 1.x Configuration section.

FSSAMLService.jsp

Associated with FSSAMLServiceViewBean, which is used by a number of other JSP files in the console/federation subdirectory.

FSSAMLSetTrustedPartnerType.jsp

Associated with the FSSAMLSetTrustedPartnersEdit.jsp file; used when you select a configured SAML 1.x Configuration trusted partner.

FSSAMLSiteIDAdd.jsp

Supports the addition of a Site ID for a SAML-configured partner.

FSSAMLSiteIDEdit.jsp

Supports the modification of a Site ID for a SAML-configured partner.

FSSAMLTargetURLsAdd.jsp

Includes a new POST to a specified URL.

FSSAMLTargetURLsEdit.jsp

Supports editing of a POST to a specified URL.

FSSAMLTrustedPartnersAdd.jsp

Called when you create a new "trusted partner" in the SAML 1.x Configuration area of the Federation window.

FSSAMLTrustedPartersEdit.jsp

Called when you edit an existing "trusted partner" in the SAML 1.x Configuration area of the Federation window.

Federation.jsp

Cited when you click New in the "Circle of Trust" section of the Federation window.

FileUploader.jsp

Called by the ImportEntity.jsp file, to support uploads of metadata files associated with a previously configured entity provider.

IDFFAffiliate.jsp

Specifies an IDFF affiliate in a COT.

IDFFGeneral.jsp

Includes general parameters associated with an IDFF affiliate in a COT. The corresponding IDFFGeneralViewBean parameter is cited only in this and the IDFFGeneralViewBean.java files.

IDFFIDP.jsp

Associated with the Identity Provider (IDP) for IDFF.

ISFFSP.jsp

Associated with the Service Provider (SP) for IDFF.

ImportEntity.jsp

Supports the import of pre-existing metadata files which define an entity provider. Allows you to import metadata from a URL to a desired Realm.

SAMLv2Affiliate.jsp

Enables a view of SAML version 2 affiliates.

SAMLv2AttrAuthority.jsp

Associated with an IDP acting as an attribute authority.

SAMLv2AttrQuery.jsp

Supports queries and saves of SAML2 attribute metadata.

SAMLv2AuthnAuthority.jsp

Enables communication with an IDP acting as an authentication authority.

SAMLv2General.jsp

Identifies general properties of a SAML version 2 affiliate.

SAMLv2IDPAdvanced.jsp

Supports the configuration of advanced properties for a SAMLv2 IDP.

SAMLv2AssertionContent.jsp

Associated with the Assertion Content tab, accessible when you select Federation > Entity Providers > *Provider Name*.

SAMLv2AssertionProcessing.jsp

Associated with the Assertion Processing tab, accessible when you select Federation > Entity Providers > *Provider Name*.

SAMLv2IDPServices.jsp

Supports the configuration of IDP service properties for a SAML2 provider.

FORGEROCK

`SAMLv2PDP.jsp`

Enables the configuration of a SAMLv2-based Policy Decision Point (PDP).

`SAMLv2PEP.jsp`

Enables the configuration of a SAMLv2-based Policy Enforcement Point (PEP).

`SAMLv2SPAdvanced.jsp`

Supports the configuration of advanced properties for a SP. Accessible when you select Federation > Entity Providers > *Provider Name* > SP > Advanced.

`SAMLv2SPAssertionContent.jsp`

Associated with the Assertion Content tab; supports the configuration of such for SPs; It is accessible when you select Federation > Entity Providers > *Provider Name* > SP > Assertion Content.

`SAMLv2SPAssertionProcessing.jsp`

Associated with the Assertion Content tab; supports the configuration of assertion processing-related properties for SPs. It is accessible when you select Federation > Entity Providers > *Provider Name* > SP > Assertion Processing.

`SAMLv2SPServices.jsp`

Supports the configuration of services-related properties for an SP. It is accessible when you select Federation > Entity Providers > *Provider Name* > SP > Services.

`WSFedGeneral.jsp`

Associated with the configuration of a legacy WS-Federation entity provider.

`WSFedIDP.jsp`

Supports the configuration of an IDP under WS-Federation.

`WSFedSP.jsp`

Supports the configuration of an SP under WS-Federation.

7.12. Policy Console JSP Endpoints

The JSP service endpoints in the console/policy subdirectory relate to a policies under a specific realm. To v iew the options listed in this section, start the GUI console and navigate to Access Control > *[Name of Realm]* > Policies.

For more information, see the chapter on *Defining Authorization Policies OpenAM in the Administration Guide* in the *Administration Guide*.

AuthToRealm.jsp

Supports a policy that depends on the realm where the user authenticated.

AuthToRealmAdd.jsp

Adds a policy that depends on the realm where the user authenticated.

AuthToRealmEdit.jsp

Edits an existing policy that depends on the realm where the user authenticated.

AuthToServiceAdd.jsp

Enables a policy that depends on an authentication realm for a user.

AuthToServiceEdit.jsp

Edits a policy that depends on an authentication realm for a user.

ConditionAdd.jsp

Supports adding a condition to a policy realm. Associated with the SelectConditionType.jsp file.

ConditionEdit.jsp

Edits a condition that has been added to a policy realm. Associated with the SelectConditionType.jsp file.

ConditionProxy.jsp

Supports a proxy of a condition that has been added to a policy realm. Cited only by the ConditionProxyViewBean.java file.

IdentityMembershipConditionAdd.jsp

Supports a policy that depends on a list of selected OpenAM subjects, as well as group membership.

IdentityMembershipConditionEdit.jsp

Edits an existing policy that depends on a list of selected OpenAM subjects, as well as group membership.

IdentitySubject.jsp

Supports the configuration of a policy based on users or groups.

IdentitySubjectAdd.jsp

Adds a policy that configures a policy based on users or groups.

FORGEROCK

IdentitySubjectEdit.jsp

Edits an existing policy based on the configuration of users or groups.

IDRepoResponseProviderAdd.jsp

Identifies a response provider that provide additional information on policy enforcement, such as why a request was allowed or denied.

IDRepoResponseProviderEdit.jsp

Edits an ID response provider that provide additional information on policy enforcement, such as why a request was allowed or denied.

PMAuthenticatedUsersSubjectAdd.jsp

Supports the configuration of a new policy for authenticated users.

PMAuthenticatedUsersSubjectEdit.jsp

Supports the editing of an existing policy for authenticated users.

PMDefaultAuthLevelCondition.jsp

Supports a policy that depends on the realm where the user authenticated, with a minimum or maximum acceptable authentication level.

PMDefaultAuthLevelConditionAdd.jsp

Adds a policy that depends on the realm where the user authenticated, with a minimum or maximum acceptable authentication level.

PMDefaultAuthLevelConditionEdit.jsp

Edits an existing policy that depends on the realm where the user authenticated, with a minimum or maximum acceptable authentication level.

PMDefaultAuthSchemeCondition.jsp

Supports the configuration of a policy that depends on the realm where the user authenticated.

PMDefaultAuthSchemeConditionAdd.jsp

Adds a policy that depends on the realm where the user authenticated.

PMDefaultAuthSchemeConditionEdit.jsp

Edits an existing policy that depends on the realm where the user authenticated.

PMDefaultIPCondition.jsp

Supports a policy based on clients in a specific range of IP addresses or associated with a specific DNS domain name.

PMDefaultIPConditionAdd.jsp

Adds a policy based on clients in a specific range of IP addresses or associated with a specific DNS domain name.

PMDefaultIPConditionEdit.jsp

Edits an existing policy based on clients in a specific range of IP addresses or associated with a specific DNS domain name.

PMDefaultSessionCondition.jsp

Supports the configuration of an Active Session policy condition.

PMDefaultSessionConditionAdd.jsp

Adds a new policy related to an Active Session policy condition.

PMDefaultSessionConditionEdit.jsp

Edits an existing policy related to an Active Session policy condition.

PMDefaultTimeCondition.jsp

Relates to a policy associated with time restrictions on a user or group.

PMDefaultTimeConditionAdd.jsp

Adds a policy for time restrictions on a user or a group.

PMDefaultTimeConditionEdit.jsp

Edits an existing policy related to time restrictions on a user or a group.

PMDSAMERoleSubject.jsp

Used for user/group roles associated with the Directory Server Access Management Edition.

PMLDAPGroupSubject.jsp

Relates to a policy dependent on group membership within the LDAP database.

PMLDAPOrgSubject.jsp

Relates to a policy dependent on organizational (OU) membership within the LDAP database.

PMLDAPRoleSubject.jsp

Relates to a policy dependent on user roles configured within the LDAP database.

Policy.jsp

Displays currently configured policies for the target realm.

PolicyNormalAdd.jsp

Shows what policy has been added from the Policies tab, after configuring a new policy with the New Policy button.

PolicyNormalEdit.jsp

Supports the creation of a new policy rule, or the edit of an existing policy rule. To access, click New in any policy category, or select an existing policy.

PolicyReferralAdd.jsp

Displays a newly configured referral policy.

PolicyReferralEdit.jsp

Supports editing of an existing referral policy.

PolicySelectType.jsp

Supports selection of a policy, by name, in either a "normal" or a "referral" category.

ReferralAdd.jsp

Adds referrals to and from an existing policy.

ReferralEdit.jsp

Edits referrals associated with an existing policy.

ReferralProxy.jsp

Supports changes in referrals to and from an existing policy.

ResponseProviderAdd.jsp

Associated with IDRepoResponseProviderAdd.jsp.

ResponseProviderEdit.jsp

Associated with IDRepoResponseProviderEdit.jsp.

ResponseProviderProxy.jsp

Supports changes in response providers for an existing policy.

RuleAdd.jsp

Displays a newly created policy, in the Edit Policy window.

RuleEdit.jsp

Supports edits of an existing policy.

RuleWithPrefixAdd.jsp

Associated with the SelectServiceType.jsp endpoint.

RuleWithPrefixEdit.jsp

Associated with the SelectServiceType.jsp endpoint.

RuleNoResourceAdd.jsp

Associated with the SelectServiceType.jsp endpoint.

RuleNoResourceEdit.jsp

Associated with the SelectServiceType.jsp endpoint.

SelectConditionType.jsp

Enables a policy that depends on whether the information for a specific user can be found in the identity repository LDAP database.

SelectRealm.jsp

Opens a window that supports a selection from existing realms, based on available authentication modules.

SelectReferralType.jsp

Supports the configuration of a referral type for a sub-realm.

SelectResponseProviderType.jsp

Supports the configuration of a response provider type for an identity repository.

SelectServiceType.jsp

Supports the configuration of a policy service type; supports the customization of a new rule for configurable service types such as the Discovery Service.

SelectSubjectType.jsp

Enables creation of a policy for web service clients, associated with federated access management.

SessionPropertyAdd.jsp

Supports a policy that depends on attributes in a user's session.

SessionPropertyConditionAdd.jsp

Supports a policy that includes conditions based on attributes in a user's session.

SessionPropertyConditionEdit.jsp

Edits conditions in a policy based on attributes in a user's session.

SessionPropertyEdit.jsp

Edits attributes in a policy based on attributes in a user's session.

SubjectAdd.jsp

Supports the configuration of a new policy for authenticated users; associated with PMAuthenticatedUsersSubjectAdd.jsp.

SubjectEdit.jsp

Edits the configuration of a policy for authenticated users; associated with PMAuthenticatedUsersSubjectEdit.jsp.

SubjectNoneAdd.jsp

Associated with a policy for web service clients; related to SelectSubjectType.jsp.

SubjectNoneEdit.jsp

Supports the configuration of a new policy for authenticated users; associated with PMAuthenticatedUsersSubjectEdit.jsp.

SubjectProxy.jsp

Configures a proxy for web service client policies; associated with SelectSubjectType.jsp.

7.13. IDM Console JSP Endpoints

This group of service endpoints are associated with an identity management (IDM) interface from OpenAM. You can find these endpoints in the console/idm subdirectory. You may not need all of the functionality provided by the endpoints in this section.

Some of the endpoints in this section include references to UM*.jsp endpoints, User Console JSP Endpoints located in the console/user subdirectory, and described later in this chapter.

EndUser.jsp

Accesses the information page for the currently logged in user.

Entities.jsp

Opens the list of currently configured users, available via Access Control > *[selected realm]* > Subjects.

EntityAdd.jsp

Used when adding a new user or group.

EntityDiscoveryDescriptionAdd.jsp

Associated with the Discovery Service. To access that service, select a non-administrative user and select the Services tab. The EntityDiscoveryDescriptionAdd.jsp file is used when selecting a new Security Mechanism ID as a Service Description as a new Discovery Resource Offering.

EntityDiscoveryDescriptionEdit.jsp

Associated with an edit of an existing Security Mechanism ID.

EntityEdit.jsp

Called when saving changes to an existing user.

EntityMembers.jsp

Lists the members of a configured group.

EntityMembersFilteredIdentity.jsp

Lists the members of a configured group based on some filter.

EntityMembership.jsp

Accessed when a regular user is made a member of a previously configured group.

EntityResourceOffering.jsp

Supports custom resource offering entries for a previously configured user. Also seen when accessing the UMUserResourceOffering.jsp file.

EntityResourceOfferingAdd.jsp

Supports entries of new resource offerings for a previously configured user. Also seen when accessing the UMUserResourceOfferingAdd.jsp file.

EntityResourceOfferingEdit.jsp

Supports edits of existing resource offerings for a previously configured user. Also seen when accessing the UMUserResourceOfferingEdit.jsp file.

EntityServices.jsp

Supports a new service for a specific user. As of this writing, available services are: Dashboard, Discovery Service, Liberty Personal Profile Service, and Session.

Home.jsp

Opens a list of currently configured users.

ServicesAdd.jsp

Accessible after adding a new service for a currently configured user; associated with the
EntityServices.jsp file.

ServicesEdit.jsp

Accessible for editing services associated with a currently configured user.

ServicesNoAttribute.jsp

Used if a configured organization has no available attributes.

ServicesSelect.jsp

Opened when adding a service for a specific user.

7.14. Console Realm JSP Endpoints

If you want to know how to configure services and data stores within a realm, you'll want to
understand the workings of these service endpoints. If you want to customize realms in production,
you'll want to keep these endpoints available on an OpenAM console. You can find these endpoints in
the console/realm subdirectory.

HomePage.jsp

Associated with the main Access Control page in the OpenAM GUI console, which lists configured
realms. If you call realm/HomePage.jsp directly, it cites messages associated with changes for
a specific user, and functions more closely associated with JSP endpoints in the console/idm
subdirectory.

IDRepo.jsp

Enables links with directory server data stores within a realm. To access, select Access Control >
[some realm] > Data Stores > New. You should see a variety of supported directory server data
stores, such as Active Directory, OpenDJ, and Tivoli Directory Server.

IDRepoAdd.jsp

Appears when you add a data store; associated with the IDRepo.jsp service endpoint.

IDRepoEdit.jsp

Appears when you edit an existing data store; associated with the IDRepo.jsp service endpoint.

IDRepoSelectType.jsp

Includes a list of supported data stores, from Active Directory to OpenDJ; associated with the
IDRepo.jsp service endpoint.

FORGEROCK

RMRealm.jsp

Supports the configuration of a new realm, or editing of an existing realm.

RMRealmAdd.jsp

Supports the addition of a new realm; associated with the RMRealm.jsp service endpoint.

RealmDiscoveryDescriptionAdd.jsp

Supports a new description for a realm; associated with the RealmResourceOffering.jsp service endpoint.

RealmDiscoveryDescriptionEdit.jsp

Supports an edited description; associated with the RealmResourceOffering.jsp service endpoint.

RealmProperties.jsp

Works with the pages that allow you to edit an existing realm.

RealmResourceOffering.jsp

Supports the configuration of a security mechanism to a new realm resource offering. Requires the configuration of the discovery service, and the configuration of a directory resource offering for the specified realm.

RealmResourceOfferingAdd.jsp

Supports the addition of a security mechanism to a new realm resource offering. Requires the configuration of the discovery service, and the configuration of a directory resource offering for the specified realm.

RealmResourceOfferingEdit.jsp

Supports the editing of a security mechanism for an existing realm resource offering. Requires the configuration of the discovery service, and the configuration of a directory resource offering for the specified realm.

Services.jsp

Supports the configuration of a service within a specified realm.

ServicesAdd.jsp

Supports the addition of a service to a specified realm; available services to add include Administration, Dashboard, Discovery, Globalization Settings, OAuth2 Provider, Password Reset, Session, and User.

ServicesCannotAssignService.jsp

If a desired service is not compatible with directory data available from an organization, it is rejected.

ServicesEdit.jsp

Supports the editing of an existing service; associated with the Services.jsp endpoint.

ServicesNoAttribute.jsp

Supports the editing of an existing service; called if the attribute cannot be found or changed.

ServicesSelect.jsp

Implements step 1 of the addition of a new service; associated with the Services.jsp endpoint.

7.15. Service Console JSP Endpoints

You can find the JSP files in this category in the console/service subdirectory. Most of the endpoints are accessible in the console, from various options associated with the Configuration menu. If you don't use some of the functionality described such as Liberty ID-FF or SOAP binding, you may be able to delete the associated endpoints.

G11NCharsetAliasAdd.jsp

Supports the configuration of a new character set alias. Accessible from the Globalization Settings > Charset Aliases submenu.

G11NCharsetAliasEdit.jsp

Supports the editing of an existing character set alias. Accessible from the Globalization Settings > Charset Aliases submenu.

G11NSupportedCharsetAdd.jsp

Supports the configuration of a new character set supported by a locale. Accessible from the Globalization Settings > Charsets Supported by Each Locale submenu.

G11NCharsetAliasEdit.jsp

Supports the editing of an existing character set supported by a locale. Accessible from the Globalization Settings > Charsets Supported by Each Locale submenu.

MAPClientManager.jsp

Supports a list of client types. Associated with the Default Client Type option available via Configuration > System > Client Detection.

MAPCreateDevice.jsp

Supports creation of client devices.

MAPCreateDeviceTwo.jsp

Supports creation of client devices.

MAPDeviceProfile.jsp

Supports step 1 of creating a new client device.

MAPDuplicationDevice.jsp

Used with duplicate client devices.

SCConfig.jsp

Associated with basic Service Configuration data, and the other endpoints accessible from the Configuration menu.

SCConfigAuth.jsp

Supports the configuration of available authentication databases. You can get to this window by selecting Configuration > Authentication.

SCConfigConsole.jsp

Supports the configuration of administrative an globalization console properties. You can get to this window by selecting Configuration > Console.

SCConfigGlobal.jsp

Supports the configuration of OpenAM global properties. You can get to this window by selecting Configuration > Global.

SCConfigSystem.jsp

Supports the configuration of OpenAM system properties. You can get to this window by selecting Configuration > System.

SCPlatform30.jsp

Accesses current global attributes and cookie domain settings. To get to this window, select Configuration > System > Platform.

SCPolicy.jsp

Supports a view of the current policy configuration. To access this window, select Configuration > Global > Policy Configuration.

SCPolicyResourceComparatorAdd.jsp

Supports the addition of a new resource comparator to the current policy configuration. To access the relevant window, select Configuration > Global > Policy Configuration.

SCPolicyResourceComparatorEdit.jsp

Supports the editing of an existing resource comparator in the current policy configuration. To access the relevant window, select Configuration > Global > Policy Configuration.

SCSAML2SOAPBinding.jsp

Enables a review of current SAMLv2 SOAP binding request handlers. Associated with SOAP-based communications, using SAMLv2 requests, between a client and a server. To access the relevant screen, select Configuration > Global > SAMLv2 SOAP Binding.

SCSAML2SOAPBindingRequestHandlerListAdd.jsp

Allows you to add a new SAMLv2 SOAP binding request handler. To access the relevant screen, select Configuration > Global > SAMLv2 SOAP Binding.

SCSAML2SOAPBindingRequestHandlerListDup.jsp

Allows you to duplicate an existing SAMLv2 SOAP binding request handler. To access the relevant screen, select Configuration > Global > SAMLv2 SOAP Binding.

SCSAML2SOAPBindingRequestHandlerListEdit.jsp

Allows you to edit an existing SAMLv2 SOAP binding request handler. To access the relevant screen, select Configuration > Global > SAMLv2 SOAP Binding.

SCSOAPBinding.jsp

Enables a review of current SOAP binding request handlers. Associated with the Liberty Alliance Project Identity Federation Framework (Liberty ID-FF).

SCSOAPBindingRequestHandlerListAdd.jsp

Allows you to add a new SOAP binding request handler. Associated with the Liberty Alliance Project Identity Federation Framework (Liberty ID-FF).

SCSOAPBindingRequestHandlerListDup.jsp

Allows you to duplicate an existing SOAP binding request handler. Associated with the Liberty Alliance Project Identity Federation Framework (Liberty ID-FF).

SCSOAPBindingRequestHandlerListEdit.jsp

Allows you to edit an existing SOAP binding request handler. Associated with the Liberty Alliance Project Identity Federation Framework (Liberty ID-FF).

SecurityTokenService.jsp

Supports the configuration of tokens associated with the Security Token Service (STS). To access the associated screen, select Configuration > Global > Security Token Service.

ServerAdd.jsp

Supports the addition of an OpenAM server to work behind a load balancer in support of Session Failover (SFO). Available from Configuration > Servers and Sites, in the Servers subsection.

ServerClone.jsp

Supports the cloning of an existing OpenAM server to work behind a load balancer in support of Session Failover (SFO). Available from Configuration > Servers and Sites, in the Servers subsection.

ServerConfigInherit.jsp

Supports the inheritance of the default configuration for servers, as it relates to SFO.

ServerConfigXMLAddServer.jsp

Enables the configuration fo a new server; relates to SFO.

ServerConfigXML.jsp

Supports the review of the XML settings of an existing server, as it relates to SFO.

ServerEditAdvanced.jsp

Supports the editing of advanced properties for default servers, in the configuration of servers for SFO. To access, select Configuration > Severs and Sites > Default Server Settings, and click Advanced.

ServerEditGeneral.jsp

Supports the editing of general properties for default servers, such as the base directory, default locale, debug level, mail server for notifications, and more. Relates to the configuration of servers for SFO. To access, select Configuration > Severs and Sites > Default Server Settings, and click General.

ServerEditSDK.jsp

Supports the editing of SDK-related properties for default servers, associated with SFO. Supports editing of settings such as datastore notifications, event service connection retries, LDAP connections, Time To Live (TTL) for user entries, and more. To access, select Configuration > Severs and Sites > Default Server Settings, and click SDK.

ServerEditSecurity.jsp

Supports the editing of security properties for default servers; associated wtih SFO. Includes default security settings such as encryption keys, cookie encoding, key stores, and certificate management. To access, select Configuration > Severs and Sites > Default Server Settings, and click Security.

ServerEditSession.jsp

Supports the editing of session properties for default servers; associated with SFO. Note the Session Limit default specifies a maximum of 5000, well short of the 100,000 sessions that can be

handled by a standard 3GB dual-core production system. To access, select Configuration > Severs and Sites > Default Server Settings, and click Session.

`ServerSite.jsp`

Associated with the addition or editing of a load balancer that distributes requests to other OpenAM servers. Available from the Configuration > Servers and Sites, in the Servers subsection.

`SiteAdd.jsp`

Enables the configuration of a load balancer to distribute requests to other existing OpenAM servers. Available from the Configuration > Servers and Sites, in the Sites subsection.

`SiteEdit.jsp`

Enables changes to a configured load balancer in how it distributes requests to other existing OpenAM servers. Available from the Configuration > Servers and Sites, in the Sites subsection.

`SMDiscoveryBootstrapRefOffAdd.jsp`

Includes new resource offerings for the discovery service, bootstrapped using a standard such as SAML2.

`SMDiscoveryBootstrapRefOffEdit.jsp`

Supports the editing of existing resource offerings for the discovery service, bootstrapped with a standard such as SAML2.

`SMDiscoveryDescriptionAdd.jsp`

Includes the addition of of new options for the discovery service.

`SMDiscoveryDescriptionEdit.jsp`

Supports the editing of existing options for the discovery service.

`SMDiscoveryProviderResourceIdMapperAdd.jsp`

Supports the mapping of a new resource ID for the discovery service.

`SMDiscoveryProviderResourceIdMapperEdit.jsp`

Supports the editing of an existing resource ID for the discovery service.

`SMDiscoveryService.jsp`

Supports a review and configuration of the Discovery Server, for global attributes, the ResourceID Mapper plug-in, and bootstrapping.

SMG11N.jsp

> Allows you to configure globalization settings for OpenAM; accessible via Configuration > Console > Globalization Settings.

SMG11N.jsp

> Allows you to configure globalization settings for OpenAM; accessible via Configuration > Console > Globalization Settings.

STSExportPolicy.jsp

> Allows you to review and copy STS policies for export, input, and output. You can review this via Configuration > Global > Security Token Service > Export Policy.

SubConfigAdd.jsp

> Allows you to configure a secondary configuration instance; accessible via Configuration > Global > Session.

SubConfigEdit.jsp

> Allows you to edit an existing secondary configuration instance; accessible via Configuration > Global > Session.

SubSchemaTypeSelect.jsp

> Allows you to configure a schema assocaited with breadcrumbs.

7.16. Session Console JSP Endpoints

There are currently two service endpoints configured in the console/session subdirectory, related to login sessions.

SMProfile.jsp

> Provides information on current login session statistics. Available from the Sessions tab from the main console.

SessionHAStatistics.jsp

> Supports session high availability statistics collection.

7.17. Task Console JSP Endpoints

The service endpoints in the console/task subdirectory relate to the options available from the default start page when an administrator logs into the OpenAM console. If you don't use Google Apps or Salesforce, you may not need some of the functionality in the associated endpoints.

CompleteCreateHostedIDP.jsp

Provides information on what the administrator can do after configuring an Identity Provider (IDP). Options listed include registering a remote Service Provider (SP), creating a fedlet, configuring Google Apps, and configuring Salesforce CRM. Includes links to such functionality, which depend on the configuration of a Circle of Trust (CoT).

ConfigureGoogleApps.jsp

Supports the configuration of Google Apps for Single-sign on (SSO). Requires a CoT configured with an IDP.

ConfigureGoogleAppsComplete.jsp

Enables entries to configure the SP. Includes steps "To Enable Access to the Google Apps API."

ConfigureGoogleAppsWarning.jsp

Includes a default warning message related to the ConfigureGoogleApps.jsp endpoint. The message is self-explanatory, though grammatically questionable: "Unable to configure because there are no circle of trust with Identity Provider."

ConfigureOAuth2.jsp

Supports the configuration of OAuth2 Authorization. For more information, see the the chapter on *Managing OAuth2 Authorization in the Administration Guide* in the *Administration Guide*.

ConfigureSalesForceApps.jsp

Accessible when you select the Configure Salesforce CRM link shown in the main GUI console. Requires IDP and SP information for an appropriate CoT, where OpenAM is the IDP and Salesforce is configured as the SP.

ConfigureSalesForceAppsComplete.jsp

Supports the configuration of SSO with a Salesforce CRM account. Includes instructions on the settings to add to an applicable Salesforce account.

ConfigureSalesForceAppsFinishWarning.jsp

Sets up a warning message related to a need for a Salesforce Login URL for the configuration.

CreateFedlet.jsp

A fedlet supports federation for a SP that does not already have its own federation solution. For more information, see the the chapter on *Using Fedlets in Java Web Applications in the Development Guide* in the *Developer's Guide*.

CreateFedletWarning.jsp

Sets up a warning message related to the prerequisite for a CoT with the IDP.

`CreateHostedIDP.jsp`

Supports the configuration of a SAMLv2 IDP on the local instance of OpenAM.

`CreateHostedSP.jsp`

Supports the configuration of a SAMLv2 SP on the local instance of OpenAM.

`CreateRemoteIDP.jsp`

Supports the configuration of a SAMLv2 IDP on a remote system, within a configured CoT.

`CreateRemoteSP.jsp`

Supports the configuration of a SAMLv2 SP on a remote system, within a configured CoT.

`Home.jsp`

Endpoint that redirects the client to the startup page for OpenAM.

`ValidateSAML2Setup.jsp`

Supports the test of a federation connection between an IDP and SP in a CoT.

7.18. User Console JSP Endpoints

Endpoints in the console/user subdirectory support account configuration tasks. Many of these endpoints are accessible by realm. From the home page screen, select Access Control > *[realm]* > Subjects > *[name of user]*. This should open up an Edit User screen

`UMChangeUserPassword.jsp`

This service endpoint is normally opened in a separate window to enable a user (or administrator) to change their login password. Accessible from the Edit User screen. All you need to do from the screen is click Edit next to the Password entry.

`UMUserDiscoveryDescriptionAdd.jsp`

Relates to the security mechanism identifier associated wih a user. To access from the screen for an individual user, select Services > Discovery Service > Add > scroll down to the Service Description box > New Description > select and Add a Security Mechanism ID. Example IDs include urn:liberty:security:2003-08:ClientTLS:SAML, which relates to the former Liberty Alliance project, using Transaction Layer Security (TLS) on the client, with SAML assertions.

`UMUserDiscoveryDescriptionEdit.jsp`

Supports editing of the security mechanism identifier associated with a user. Closely related to the UMUserDiscoveryDescriptionAdd.jsp endpoint.

UMUserPasswordResetOptions.jsp

Allows you to "Force Change Password on Next Login". Accessible from the Edit User screen for a specific user, via the "Password Reset Options" entry near the bottom of the window.

UMUserResourceOffering.jsp

Accessible as an option to the Discovery Service for a specific user. To access from the Edit User screen for a specific user, select Services > Discovery Service > Add.

UMUserResourceOfferingAdd.jsp

Accessible as an option to the Discovery Service for a specific user. To access from the Edit User screen for a specific user, select Services > Discovery Service > Add.

UMUserResourceOfferingEdit.jsp

Accessible as an option to the Discovery Service for a specific user. To edit an existing resource offering, navigate to the Edit User screen for a specific user, select Services > Discovery Service > *[some previously configured service]*.

7.19. Web Services Console JSP Endpoints

Web services include endpoints in the console/webservices subdirectory. You can use them to define legacy options for services such as the Liberty Identity Federation Framework (ID-FF). As such, these endpoints may be less essential to your implementation of OpenAM. For more information, see the *OpenAM Wiki on Web Services* .

WSAuthNServices.jsp

Supports the configuration of various mechanism handlers for authentication, including CRAM-MD5, PLAIN, and SSOToken.

WSAuthNServicesHandlersAdd.jsp

Supports the addition of a new mechanism handler for authentication.

WSAuthNServicesHandlersEdit.jsp

Supports changes to an existing mechanism handler for authentication.

WSPPServiceDSAttributeMapListAdd.jsp

Enables the addition of a new LDAP attribute, with a name prefix.

WSPPServiceDSAttributeMapListEdit.jsp

Enables the editing of an existing LDAP attribute, with a name prefix.

`WSPPServiceSupportedContainerAdd.jsp`

Enables the creation of a new supported container for ID-FF.

`WSPPServiceSupportedContainerEdit.jsp`

Enables the editing of an existing container.

`WSPersonalProfileService.jsp`

Allows you to configure ID-FF for global attributes, supported containers, PPLDAP attributes and alternative security mechanisms.

7.20. OAuth JSP Endpoints

Includes endpoints in the oauth, oauth2, and oauth2c subdirectories. Some of the service endpoints in the oauth subdirectory are based on OAuth 1.0, which may be deprecated in an upcoming release.

`deleteconsumer.jsp`

This endpoint is used to delete consumer systems, which get resources from service providers (SPs) based on OAuth 1.0 tokens.

`deletetoken.jsp`

This endpoint is used to delete an existing OAuth 1.0 token.

`index.jsp`

Specifies an endpoint used to register and delete service consumers, which get resources from SPs. Provides access to registerconsumer.jsp and deleteconsumer.jsp. Associated with OAuth 1.0.

`registerconsumer.jsp`

Defines an endpoint used to register a consumer of services from SPs. Associated with OAuth 1.0.

`userconsole.jsp`

Allows a user to authorize or revoke a request for an OAuth 1.0 token..

`registerClient.jsp`

Enables registration of an OAuth 2.0 client with the OpenAM OAuth 2.0 authorization service. For details, see the Administration Guide chatper on *Managing OAuth 2.0 Authorization* in the *Administration Guide*.

`OAuthLogout.jsp`

Used to log out the resource owner with teh OAuth 2.0 provider. For more information, see the Administration Guide chapter on *Defining Authentication Services* in the *Administration Guide*.

OAuthProxy.jsp

Endpoint used for redirection. For more information, see the Administration Guide chapter on *Managing OAuth 2.0 Authorization* in the *Administration Guide*.

7.21. Password JSP Endpoints

The endpoints in this section can be found in the password/ui subdirectory. Each of these endpoints use the PWResetViewBeanBase.java file, as a class to set up messages. You can view some of these endpoints by omitting the `password`. For example, to view the effect of the PWResetUserValidation.jsp endpoint on an OpenAM system using an URL of openam.example.org in a standard Tomcat container, navigate to http://openam.exmaple.org/openam/ui/PWResetUserValidation.jsp. You can set associated options from the main console by selecting Configuration > Global > Password Reset. For more information on the process, see the chapter on *Configuring Password Reset in the Administration Guide* in the *Administration Guide*.

PWResetBase.jsp

This simple endpoint includes a redirection of the ServiceURI, and specifies OpenAM as the ProductName. It's cited by the other endpoints in the password/ui subdirectory.

PWResetInvalidURL.jsp

This endpoint is called with the PWResetInvalidURLViewBean class, when a module servlet gets an invalid URL.

PWResetQuestion.jsp

Starts the password reset process by propmting for the User ID. For more information on the process, see the method for the associated `PWResetQuestionModel`, available from the Interface PWResetQuestionModel specification page.

PWResetSuccess.jsp

Specifies the endpoint that is called when an account password is successfully reset.

PWResetUncaughtException.jsp

Specifies a "Contact your administrator" message when there is an error in a related endpoint.

PWResetUserValidation.jsp

Opens a screen that prompts for a user ID (UID). If that UID is found in the database, configured with an accessible email address, on a system connected to a mail server, a reset link is sent to that address.

7.22. SAML2 JSP Endpoints

You can find the endpoints described in this section in the saml2/jsp subdirectory. As of this writing, some of these endpoints are not used in the current implementation of OpenAM. Active endpoints in this category are discussed in the chapter on *Managing SAML2 Federation in the Administration Guide* in the *Administration Guide*.

default.jsp

> May be used by other files to return a success or failure message. While the default.jsp name is common in the trunk, the jsp/default.jsp filename is used only by SPSingleLogout.java, which is not commonly used.

exportmetadata.jsp

> Supports the export of XML-based metadata with other providers within a circle of trust (CoT). Currently used. For more information, see the chapter on *Managing SAML2 Federation in the Administration Guide* in the *Administration Guide*.

fedletAttrQuery.jsp

> Supports the configuration of SAML attribute query headers.

fedletAttrResp.jsp

> Supports the configuration of SAML attribute response headers.

fedletSSOInit.jsp

> Previously used to start single sign-on at the Fedlet.

fedletSampleApp.jsp

> Specifies a sample fedlet application that can be removed in production.

fedletXACMLQuery.jsp

> Enables a sample SAML XACML query handler; used for testing, to prompt users to specify a resource URL along with an action (GET, POST).

fedletXACMLResp.jsp

> Retrieves a sample SAML XACML resource URL for a yes, no, or maybe decision (PERMIT, DENY, or INDETERMINATE).

idpMNIPOST.jsp

> The MNI in several JSP files relate to ManageNameID, which sets up corresponding accounts on IDPs and SPs. This particular JSP file processes a request from an IDP through an HTTP redirect.

idpMNIRedirect.jsp

> The MNI in several JSP files relate to ManageNameID, which sets up corresponding accounts on IDPs and SPs. This particular JSP file processes a request from an IDP through an HTTP redirect.

It uses a metadata-based alias, an entity ID for the service provider, and the type of MNI request; examples include `NewID` and `terminate`.

idpMNIRequestInit.jsp

The MNI in several JSP files relate to ManageNameID, which sets up corresponding accounts on IDPs and SPs. As described in the *Managing SAML2 Federation in the Administration Guide* in the *Administration Guide* chapter of the Administration Guide, it allows you to change federation of persistently linked accounts. The chapter also includes an example of this endpoint at work.

idpSSOFederate.jsp

Specifies an endpoint that takes authentication requests from an SP, with a `SAMLRequest` data, a `metaAlias` and a `RelayState` with information from the target URL.

idpSSOInit.jsp

Specifies an endpoint that starts SSO, either from cache, or by verifying `metaAlias` and SP identifier data.For more information, see the chapter on *Managing SAML2 Federation in the Administration Guide* in the *Administration Guide*.

idpSingleLogoutInit.jsp

Starts a `LogoutRequest` from the identity provider.For more information, see the chapter on *Managing SAML2 Federation in the Administration Guide* in the *Administration Guide*.

idpSingleLogoutPOST.jsp

Specifies an endpoint that receives logout requests from IDPs and receives logout responses from SPs. Also sends logout responses to SPs.

idpSingleLogoutRedirect.jsp

Takes the `SAMLRequest` and `SAMLResponse` messages for logouts from the SP. May also handle the `RelayState` directive.

SA_IDP.jsp

Used for SAML authentication for communication with identity providers (IDPs).

SA_SP.jsp

Used for SAML authentication for communication with service providers (SPs).

saeerror.jsp

Returns an error message related to Secure Attribute Exchange (SAE). Currently used only by the SA_IDP.jsp and SA_SP.jsp endpoints.

saml2error.jsp

Endpoint that may return one of many error codes, specified in the comments of the file.

spAssertionConsumer.jsp

Used on a SP, to interpret information from an IDP. The request to the IDP is an `AuthnRequest`; the response from the IDP is read by this endpoint.

spMNIPOST.jsp

The MNI in several JSP files relate to ManageNameID, which sets up corresponding accounts on IDPs and SPs. This particular endpoint takes the associated request, using an HTTP Redirect, from a SP. Less commonly used.

spMNIRedirect.jsp

This particular endpoint handles the `ManageNameIDRequest` and `ManageNameIDRespnose` messages with the help of HTTP Redirect. Less commonly used.

spMNIRequestInit.jsp

This particular endpoint supports changes to federation of persistently linked accounts, in a fashion similar to idpMNIRequestInit.jsp. For an example of this endpoint in work, see the chapter on *Managing SAML2 Federation in the Administration Guide* in the *Administration Guide*.

spSSOInit.jsp

Supports SSO messages from the SP. For more information and an example of how this endpoint is used, see the chapter on *Managing SAML2 Federation in the Administration Guide* in the *Administration Guide*.

spSingleLogoutInit.jsp

Supports SSO messages from the SP. For more information, see the chapter on *Managing SAML2 Federation in the Administration Guide* in the *Administration Guide*.

spSingleLogoutPOST.jsp

Specifies an endpoint that receives logout requests from SPs and receives logout responses from IDPs. Also sends logout responses to IDPs. Converse endpoint to idpSingleLogoutPOST.jsp.

spSingleLogoutRedirect.jsp

Takes the `SAMLRequest` and `SAMLResponse` messages for logouts from the IDP. May also handle the `RelayState` directive. Converse endpoint to idpSingleLogoutRedirect.jsp.

7.23. WS Federation JSP Endpoints

The endpoints described in this section, in the wsfederation/jsp subdirectory, relate to Kantera Alliance standards that originated with the Liberty Alliance Project Identity Federation Framework.

logout.jsp

Shows a page after a successful logout.

multi.jsp

Used for multi-federation protocol configurations.

post.jsp

Sets up a form for single sign-on (SSO) responses sent from the IDP to the SP.

realmSelection.jsp

Default display if no realms are defined.

7.24. WEB-INF Endpoints

The OpenAM WAR archive includes pointers to different URL patterns in the web.xml file. The following section includes a description of each of the identified URL patterns.

Many of the endpoints in this section are based on what you would add to an OpenAM URL. Many of the endpoints described in the web.xml file are not directly related to the .jsp files described in other parts of this chapter.

The endpoints in this chapter are taken from all items tagged with the `url-pattern` label. These endpoints are listed in that they appear in the web.xml file available at the time of this writing; the list is changed frequently. If you want to disable one or more of these endpoints, you may be able to delete them from the web.xml file.

Each of the `url-pattern`s shown in the web.xml file is associated with elements such as a `filter-name` or a `servlet-name`. The definitions that follow use those elements to help identify the function of each endpoint listed in the web.xml file. Many of these elements can be directly related to a .java file.

The endpoints in this section are in the order found in the list of `url-pattern` entries shown in the web.xml file at the time of this writing.

/*

This entry is more of a filter for all endpoints. It's associated with the ResponseValidationFilter, which checks for valid URLs. It's also associated with the AMSetupFilter.java file; on systems not yet configured, it redirects users to the setup wizard.

ws/*

Specifies a group of URLs related to authentication endpoints, as it is associated with the AuthNFilter.java and AuthZFilter.java files. However, those files (and the associated RestServiceManager.java file) are not called by any other files in the trunk.

/login

With the help of the LoginLogoutMapping.java file, this would forward to the /UI/Login.jsp endpoint.

/logout

With the help of the LoginLogoutMapping.java file, this would forward to the /UI/Logout.jsp endpoint.

/UI/*

With the help of the LoginServlet.java file, this forwards to the default login page for an OpenAM system.

/config/configurator

Uses the AMSetupServlet, which as noted in the associated .java file, "is the first class to get loaded by the Servlet * container"

/setup/setSetupProgress

Used by the installation wizard to display the progress.

/upgrade/setUpgradeProgress

Used by the upgrade wizard to display progress.

/ui/*

Associated with the servlet naemd PWResetServlet, associated with password resets.

/gateway

Used with the servlet named GatewayServlet. Associated with the Gateway.java file, which takes an authentication module and forwards it to a login URL.

/GetHttpSession

The associated .java file is associated with Session Failover (SFO).

/sessionservice, /profileservice, /policyservice, /namingservice, /loggingservice, /authservice, / notificationservice

All of these endpoints are associated with OpenAM Security Advisory #201203. As suggested in the advisory, if you're using OpenAM version 9.5.4 or 10.0.0, you should be sure to apply the updates required to upgrade your systems to versions 9.5.5 or 10.0.1 (or higher).

/jaxrpc/*, /identityservices/*

These endpoints provide information on configured web services, including the port name, status, URL, and implementation class. Both endpoints show the same data. The IdentityServices servlet name points to the following description: "Web Service Endpoint - Identity Services".

/SMSServlet

Includes system configuration information when available, as documented in the comments to the AMSystemConfig.java file.

/notification

The associated servlet named notificationservlet appears to be commonly used. When the URL is entered, the default output is 200, associated with an URL success message.

/entitlementmonitor

Used by the NetworkMonitor.java file, which is essential to the monitoring of OpenAM services.

/identity/*

Possibly a legacy endpoint. While the associated IdentityServicesHandler servlet is identified as "REST Endpoint - Identity Services", it is only cited in the IdentityServicesHandler.java file.

/resources/*

Linked to an oauth servlet. The associated com.sun.identity.oauth.service.RestService class is rarely used.

/authentication/*

Associated with the servlet named AuthServlet. The associated AuthServer.java file is the controller servlet for realm authentication pages. When the URL is entered prior to login, it defaults to the standard login page.

/base/*

Associated with the servlet named AMBaseServlet. While the associated AMBaseServlet.java file is rarely used, the URL prior to login defaults to the standard login page.

/service/*

Associated with the servlet named SCServlet. While the associated SCServlet.java file is rarely used, the URL prior to login defaults to the standard login page.

/session/*

Associated with the servlet named SMServlet. While the associated SMServlet.java file is rarely used, the URL prior to login defaults to the standard login page.

/realm/*

Associated with the servlet named RMServlet. While the associated RMServlet.java file is rarely used, the URL prior to login defaults to the standard login page.

/policy/*

Associated with the servlet named PMServlet. While the associated PMServlet.java file is rarely used, the URL prior to login defaults to the standard login page.

/idm/*

Associated with the servlet named IDMServlet. While the associated IDMServlet.java file is rarely used, the URL prior to login defaults to the standard login page.

/user/*

Associated with the servlet named UMServlet. While the associated UMServlet.java file is rarely used, the URL prior to login defaults to the standard login page.

/delegation/*

Associated with the servlet named DelegationServlet. While the associated DelegationServlet.java file is rarely used, the URL prior to login defaults to the standard login page.

/task/*

Associated with the servlet named TaskServlet. While the associated TaskServlet.java file is rarely used, the URL prior to login defaults to the standard login page.

/agentconfig/*

Associated with the servlet named AgentConfigurationServlet. The associated AgentConfigurationServlet class is called by the amAccessControl.xml file, which suggests that it can be configured from the GUI console, through the Agents section of the Access Control menu. It is rarely used otherwise. The URL prior to login defaults to the standard login page.

/ccversion/*

Associated with the servlet named click-servlet. There is no associated click-servlet.java or ClickServlet.java file.

/federation/*

Associated with the servlet named FSServlet. While the associated FSServlet.java file is rarely used, the URL prior to login defaults to the standard login page.

/webservices

Used by the WSServlet.java and SecurityTokenService.java files. If you're using web services and/or the Security Token Service (STS), you may want to keep this in place.

/sts

Associated with the STS. Be aware, this endpoint exposes basic service and port information for STS, Metadata Exchange (MEX), Simple Object Access Protocol 1.1 (SOAP11), and Web Service Definition Language (WSDL) endpoints without logons.

/sts/mex

Associated with the STS. Be aware, this endpoint exposes basic service and port information for STS, Metadata Exchange (MEX), Simple Object Access Protocol 1.1 (SOAP11), and Web Service Definition Language (WSDL) endpoints without logons.

/sts/soap11

Associated with the STS. Be aware, this endpoint exposes basic service and port information for STS, Metadata Exchange (MEX), Simple Object Access Protocol 1.1 (SOAP11), and Web Service Definition Language (WSDL) endpoints without logons.

/sts/mexsoap11

Associated with the STS. Unlike related STS endpoints, it returns a 404 message by default.

/SPMniSoap/*

Used by a servlet named SPMniSoap; associated with a com.sun.identity.saml2.servlet.SPManageNameIDServiceSOAP servlet class. The associated .java file works with Manage Name ID communications using SOAP binding from the SP. As the former spMNISOAP.jsp file no longer exists in the trunk, this may be a legacy endpoint.

/SPMniPOST/*

Used by a servlet named spMNIPOST.jsp; previously defined in the SAML2 JSP Endpoints section.

/SPMniRedirect/*

Used by a servlet named spMNIRedirect.jsp; previously defined in the SAML2 JSP Endpoints section.

/SPMniInit/*

Used by a servlet named spMNIRequestInit.jsp; previously defined in the SAML2 JSP Endpoints section.

/SPECP/*

The associated SPECPService class receives and processes single logout (SLO) requests, using SOAP bindings on the SP.

/SPSloSoap/*

The associated SPSingleLogoutServiceSOAP class receives and processes single logout (SLO) requests, using SOAP bindings on the SP.

/SPSloPOST/*

Used by a servlet named spSingleLogoutPOST.jsp; previously defined in the SAML2 JSP Endpoints section.

/SPSloRedirect/*

Used by a servlet named spSingleLogoutRedirect.jsp; previously defined in the SAML2 JSP Endpoints section.

/SPSloInit/*

Used by a servlet named spSingleLogoutInit.jsp; previously defined in the SAML2 JSP Endpoints section.

/Consumer/*, /SSORedirect/*

Used by a servlet named spAssertionConsumer.jsp; previously defined in the SAML2 JSP Endpoints section.

/SSOPOST/*, /SSORedirect/*

Used by a servlet named idpSSOFederate.jsp; previously defined in the SAML2 JSP Endpoints section.

/SSORedirect/*

Used by a servlet named idpSSOFederate.jsp; previously defined in the SAML2 JSP Endpoints section.

/NIMSoap/*

Used by a servlet named NameIDMappingServiceSOAP.

/AIDReqUri/*

Used by a servlet named AssertionIDRequestServiceSoap.

/AIDReqSoap/*

Used by a servlet named AssertionIDRequestServiceSoap.

/AuthnQuerySerivceSoap/*

Used by a servlet named AuthnQueryServiceSoap.

/AttributeServiceSoap/*

Used by a servlet named AttributeServiceSoap.

/SSOSoap/*

Used by a servlet named SSOSoap.

/IDPMniSoap/*

Used by a servlet named IDPMniSoap.

/IDPMniPOST/*

Used by a servlet named idpMNIPOST.jsp; previously defined in the SAML2 JSP Endpoints section.

/IDPMniRedirect/*

Used by a servlet named idpMNIRedirect.jsp; previously defined in the SAML2 JSP Endpoints section.

/IDPMniInit/*

Used by a servlet named idpMNIRequestInit.jsp; previously defined in the SAML2 JSP Endpoints section.

/IDPSloSoap/*

Used by a servlet named IDPSloSoap.

/IDPSloPOST/*

Used by a servlet named idpSingleLogoutPOST.jsp; previously defined in the SAML2 JSP Endpoints section.

/IDPSloRedirect/*

Used by a servlet named idpSingleLogoutRedirect.jsp; previously defined in the SAML2 JSP Endpoints section.

/IDPSloInit/*

Used by a servlet named idpSingleLogoutInit.jsp; previously defined in the SAML2 JSP Endpoints section.

/ArtifactResolver/*

Used by a servlet named IDPArtifactResolver.

/spssoinit

Used by a servlet named spSSOInit.jsp; previously defined in the SAML2 JSP Endpoints section.

/idpssoinit

Used by a servlet named idpSSOInit.jsp; previously defined in the SAML2 JSP Endpoints section.

/idpSSOFederate

Used by a servlet named idpSSOFederate.jsp; previously defined in the SAML2 JSP Endpoints section.

/idpsaehandler/*

Used by a servlet named SA_IDP.jsp; previously defined in the SAML2 JSP Endpoints section.

/spsaehandler/*

Used by a servlet named IDP_SP.jsp; previously defined in the SAML2 JSP Endpoints section.

/idpfinder

Used by a servlet named IDPFinderService; The associated FSIDPFinderService.java file can be used to find a preferred IDP with a common domain cookie.

/cdcservlet

Used by a servlet named CDCServlet. It is associated with a Cross Domain Controller Servlet, as described in the the chapter on *Configuring Cross-Domain Single Sign On in the Administration Guide* in the *Administration Guide*.

/SAMLAwareServlet

Used by a servlet named SAMLAwareServlet. It is associated with communications between a client, an SP, and an IDP. The transfer service on the IDP is the SAML Aware Servlet, and is part of the client web browser artifact profile. It validates a session token from a request run through the IDP.

/SAMLPOSTProfileServlet

Used by a servlet named SAMLPOSTProfileServlet. It is associated with communications between a client, an SP, and an IDP. The transfer service on the IDP is the SAML Aware Servlet, and is part of the client web browser POST profile, which supplies assertion IDs, and returns the response to the client browser.

/SAMLSOAPReceiver

Used by a servlet named SAMLSOAPReceiver. The servlet extracts a SAML request from a message sent in SOAP format. That message can be a query for authorization, attributes, or authentication. It supports POST messages only.

/AssertionManagerServlet/*

Used by a servlet named AssertionManagerServlet. It supports dynamic substitution, using the host name, port number, and the deployment location.

/FSAssertionManagerServlet/*

Used by a servlet named FSAssertionManagerServlet. It provides remote interfaces for the assertion manager class.

/SecurityTokenManagerServlet/*

Used by a servlet named SecurityTokenManagerServlet. It supports dynamic substitution, using session parameters.

/preLogin

Used by a servlet named preLoginHandler. As there is no associated .java or .jsp file, it may be a legacy endpoint.

/postLogin/*

Used by a servlet named postLoginHandler. As there is no associated .java or .jsp file, it may be a legacy endpoint.

/federation

Used by a servlet named FederationServlet. Associated with the com.sun.identity.federation.login.FSFederationHandler class. The matching FSFederationHandler.java file processes requests to initiate a federation.

/consentHandler

Used by a servlet named consentHandler. Associated with the com.sun.identity.federation.login.FSConsentHandler class. The matching FSConsentHandler.java file processes redirect requests in an existing federation.

/ProcessLogout/*

Used by a servlet named ProcessLogout. Associated with the FSProcessLogoutServlet class. It is designed to handle single logout requests related to Kantera / Liberty ID-FF processes.

/ReturnLogout/*

Used by a servlet named ReturnLogout. Associated with the FSReturnLogoutServlet class. It is designed to handle single logout responses related to Kantera / Liberty ID-FF processes. (Note the subtle difference with the ProcessLogout endpoint which handles logout requests.)

/liberty-logout

Used by a servlet named LogoutServlet. Associated with the FSSingleLogoutServlet class. It is designed to start single logout requests related to Kantera / Liberty ID-FF processes.

/SingleSignOnService/*

Used by a servlet named SingleSignOnService. Associated with the FSSSOAndFedService class. Configured for SSO on the IDP.

/IntersiteTransferService

Used by a servlet named IntersiteTransferService. Associated with the FSIntersiteTransferService class. It is designed to send a `AuthnRequest` to an IDP.

/AssertionConsumerService/*

Used by a servlet named AssertionConsumerService. Associated with the FSAssertionConsumerService class. For more information, see the chapter on *Managing SAML 2.0 Federation in the Administration Guide* in the *Administration Guide*.

/SOAPReceiver/*

Used by a servlet named SOAPReceiver. Associated with the FSSOAPReceiver class. SOAP endpoint that handles federation and specifies a URI to the SP.

/federation-terminate

Used by a servlet named FederationTerminationServlet. Associated with the FSTerminationInitiationServlet.java file, used to initiate termination of a federation connection. The IDP will send the termination request to the associated URL.

/ProcessTermination/*

Used by a servlet named ProcessTermination. Associated with the FSTerminationRequestServlet class. The associated .java file is used when a request is received by a remote SP.

/ReturnTermination/*

Used by a servlet named ReturnTermination. Associated with the FSTerminationReturnServlet class. The associated .java file is used to define a URL used by an IP to send termination responses.

/InitiateRegistration/*

Used by a servlet named InitiateRegistration. Associated with the FSRegistrationInitiationServlet class. The associated .java file is used to handle the registration request from a remote IDP.

/ProcessRegistration/*

Used by a servlet named ProcessRegistration. Associated with the FSRegistrationRequestServlet class. Processes registration requests from remote SPs.

/ReturnRegistration/*

Used by a servlet named ReturnRegistration. Associated with the FSRegistrationReturnServlet class. Defines a URL for IDPs to send registration responses.

/Liberty/*

Used by a servlet named WSSOAPReceiver. Associated with the SOAPReceiver class. Defines an endpoint that handles SOAP requests.

/WSPRedirectHandler/*

Used by a servlet named WSPRedirectHandler. Associated with the WSPRedirectHandlerServlet class. Used by the SP for user redirects.

/idffwriter, /saml2writer

Used by a servlet with a matching name (idffwriter, saml2writer). Associated with the CookieWriterServlet class. Used by the IDP to help the web container find app-specific info such as Java classes or Java Archives (JARs).

/idffreader, /saml2reader

Used by a servlet with a matching name (idffreader, saml2reader). Associated with the CookieReaderServlet class. Used by the SP to help find the preferred IDP.

/multiprotocolrelay

Used by a servlet named MultiProtocolRelayServlet. Associated with the MultiProtocolRelayServlet class. Used as a RelayState to continue to the next protocol; associated with a federation.

/WSFederationServlet/*, /FederationMetadata/*

Used by a servlet named WSFederationServlet. Associated with the WSFederationServlet class. Used as a service endpoint for WS-Federation.

/RealmSelection/*

Used by am endpoint named realmSelection.jsp. Previously defined in the WS-Federation JSP Endpoints section.

/saml2query/*

Used by a servlet named saml2query. Associated with the QueryHandlerServlet class. The corresponding .java file receives and processes SAML2 queries.

/federationws/*

Used by a servlet named federationrest. Associated with the ServletContainer class. Does not appear to be included in any current .java or .jsp file, so it may be a legacy endpoint.

/xacml/*

Used by a servlet named XACMLContentAdapter. Associated with the XacmlContentHandlerService class. Provides the main endpoint for all XACML requests.

/frrest/oauth2/*

Used by a servlet named OAuth2Rest. Associated with the RestTokenDispatcher class. class. For more information, see the the chapter on *Using RESTful Web Services* in the *Developer's Guide*.

/oauth2/registerClient.jsp

Used by a servlet named OAuth2RegisterClient. For more information, see the the Administration Guide chapter on *Managing OAuth 2.0 Authorization* in the *Administration Guide*.

`/oauth2/*`

Used by a servlet named OAuth2RestletAdapter. Associated with the RestTokenDispatcher class. For more information, see the chapter on the chapter on *Using RESTful Web Services* in the *Developer's Guide*.

`/json/*`

Used by a servlet named ForgeRockRest. Associated with the HttpServlet class. For more information, see the chapter on *Using RESTful Web Services* in the *Developer's Guide*. In addition, you can read more about associated REST endpoints in Section 7.25, "JSON REST Endpoints".

7.25. JSON REST Endpoints

The endpoints in this section document the REST-based JSON interfaces used for authentication and authorization.

/json/agents

Authorization: Supports the PassThroughAuthorizationFilter. No authorization logic is performed in the filter. Information is logged. The authorization logic is performed by the underlying identity services.

/json/authenticate

Authentication: Supports HTTP GET and POST methods. Can handle Integrated Windows Authentication.

Authorization: No filter.

/json/dashboard

Authorization: Supports the PassThroughAuthorizationFilter. No authorization logic is performed in the filter. Information is logged.

/json/groups

Authorization: Supports the PassThroughAuthorizationFilter. No authorization logic is performed in the filter. Information is logged. The authorization logic is performed by the underlying identity services.

/json/serverinfo

Authorization: Supports the PassThroughAuthorizationFilter. No authorization logic is performed in the filter. Information is logged. One sub-endpoint, `/json/serverinfo/cookieDomains`, supports HTTP GET.

/json/sessions

Authorization: Supports the SessionResourceAuthZFilter. Allows POST _action=logout for all users. Other functionality is limited to the administrative amadmin superuser.

/json/tokens

Authorization: Supports the AdminAuthorizationFilter. Access limited to the amadmin superuser.

/json/users

Authentication: Supports HTTP POST. Uses the _action query parameter with the following allowed values: register, confirm, forgotPassword, forgotPasswordReset.

Authorization: Supports the PassThroughAuthorizationFilter. No authorization logic is performed in the filter. Information is logged. The authorization logic is performed by the underlying identity services.

7.26. Well-Known Endpoints

The endpoints described in this section are Well-Known URIs supported by OpenAM.

`/.well-known/openid-configuration`

Exposes OpenID Provider configuration by HTTP GET as specified by OpenID Connect Discovery 1.0. No query string parameters are required.

`/.well-known/webfinger`

Allows a client to retrieve the provider URL for an end user by HTTP GET as specified by OpenID Connect Discovery 1.0.

For an example, see *Configuring OpenAM For OpenID Connect Discovery* in the *Administration Guide*.

Chapter 8
XUI Configuration Parameters

The configuration of the XUI is based on settings in the `themeConfig.json` file. When OpenAM is installed, this file can be found in the `/path/to/webapps/XUI` directory.

Interface Stability: Internal in the *Administration Guide*

XUI is not supported for production use.

The following table depicts the parameters found in this file. All color codes are standard CSS Hex colors. If there is more than one theme, they may inherit parameters from the `default` theme.

- `themes`: Title; also represents an array of theme objects.

  - `name`: Theme title.

  - `path`: Relative path to CSS files.

  - `realms`: For a realm named test, enter ["test.*"].

  - `regex`: true or false.

  - `icon`: Filename of icon.

  - `settings`: Includes `logo, lessVars, footer`.

    - `logo`: Parameters for the logo, including `src,title, alt, height, width`.

      - `src`: Filename with logo.

      - `title`: Title attribute, shown behind the graphic.

      - `alt`: Text that appears upon cursor hover.

      - `height`: Logo height.

      - `width`: Logo width.

    - `lessVars`: Settings for variables used in LESS CSS stylesheets.

      - `background-color`: Standard background color; use hex or standard color words.

      - `background-image`: URL or relative path to file image

- `background-repeat`: If set to `repeat`, fills screen with multiple copies of the image.

- `background-position`: Position of the background image, in a format such as `left top` or `right bottom`.

- `footer-background-color`: Background color of the footer area; hex or standard color words accepted.

- `column-padding`: Distance between columns.

- `login-container-width`: Width of view box with login text boxes

- `login-container-label-align`: Alignment of labels in the login container, such as `left`, `right`, or `center`.

- `message-background-color`: Login message background color.

- `content-background`: Login container background color.

- `font-color`: Login container font color.

- `font-size`: Despite the name, this is the distance between login labels and text boxes

- `font-family`: Available fonts.

- `site-width`: Total width available for the login screen.

- `line-height`: Height of text lines.

- `color-active`: Border color of active text box and menu option.

- `color-inactive`: Border color of inactive text box.

- `active-menu-color`: Color of active menu option.

- `active-menu-font-color`: Color of the font used in the active menu option.

- `inactive-menu-color`: Color of inactive menu options.

- `inactive-menu-font-color`: Color of font used in the inactive menu options.

- `active-menu-color`: Color of active menu option.

- `button-hover-lightness`: Reduction in color, in percent.

- `href-color`: Color of text links.

- `href-color-hover`: Color of text links of the optiom currently being hovered over by the pointer

- `color-error`: Color of error text.

- `color-warning`: Color of warning text.

- `color-success`: Color of text of a success message.

- `color-info`: Color of information message.

- `color-inactive`: Text color of inactive messages.

- `input-border-basic`: Border color of active input text box.

- `header-border-color`: Border color of the header.

- `footer-height`: Height of the footer.

- `footer`: Parameters in the footer, typically `mailto` and `phone`.

  - `mailto`: Email address.

  - `phone`: Telephone number.

Index

C

Configuration, 134
  Authentication, 134
  Console, 135
  Global, 144
  Servers and Sites, 167
  System, 137

D

Default ports, 586

E

Endpoints, 593
  JSP, 594
    Base Console, 605
    Console Agent Configuration, 602
    Console Ajax, 603
    Console Authentication, 604
    Console Realm, 617
    Default Authentication Configuration, 597
    Default Console, 600
    Delegation Console, 605
    Federation Console, 606
    IDM Console, 615
    Main Directory, 594
    OAuth, 628
    Password, 629
    Policy Console, 609
    SAML2, 629
    Service Console, 619
    Session Console, 624
    Task Console, 624
    User Console, 626
    User Interface, 596
    Web Services Console, 627
    WS Federation, 632
  WEB-INF, 633
  Well-Known, 645
Error messages
  Authentication, 582
  Console, 584

L

Languages supported, 587
Locales supported, 587
Logs
  Administrative Files, 189
  Debug Files, 192

O

OpenID Connect, 645

P

Ports used, 586

R

REST
  JSON, 644

S

Supported languages, 587
Supported locales, 587
Supported standards
  Liberty ID-FF, 592
  OAuth 2.0, 591
  OpenID Connect 1.0, 591
  REST, 592
  SAML, 592
  SOAP, 592
  WS-Federation, 592
  WSDL, 592
  XACML, 592