Sun Java System Access Manager 7.1 Administration Reference

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

Part No: 819–4671–10

Copyright 2007 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2007 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux Etats-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certaines composants de ce produit peuvent être dérivées du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, le logo Solaris, le logo Java Coffee Cup, docs.sun.com, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la legislation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la legislation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement designés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

070226@16599

Contents

Preface 9

Part I Command Line Interface Reference 15

1 The amadmin Command Line Tool 17
The amadmin Command Line Executable 17
The amadmin Syntax 18
Using amadmin for Federation Management 21
Using amadmin for Resource Bundles 23

2 The ampassword Command Line Tool 25
The ampassword Command Line Executable 25
▼ To Run ampassword with Access Manager in SSL mode 25

3 The VerifyArchive Command Line Tool 27
The VerifyArchive Command Line Executable 27
VerifyArchive Syntax 27

4 The amsecuridd Helper 29
The amsecuridd Helper Command Line Executable 29
amsecuridd Syntax 30
Running the amsecuridd helper 30

Part II Configuration Attribute Reference 33

5 Configuration Attributes 35
Authentication 36
Anonymous 36
Active Directory 38
Authentication Configuration 42
Certificate 42
Core 47
Data Store 54
HTTP Basic 55
JDBC 55
▼ To Configure a Connection Pool — Example 57
LDAP 58
Membership 62
MSISDN 66
RADIUS 69
SafeWord 71
SAML 73
SecurID 73
UNIX 74
Windows Desktop SSO 76
Windows NT 77
Supported Language Locales 79
Console Properties 80
Administration 80
Globalization Settings 93
Global Properties 95
Password Reset 95
Policy Configuration 98
Session 104
▼ To Add a Sub Configuration 107
User 107
System Properties 108
Client Detection 109

▼ To Add a New Client 111
Logging 111
Naming 115
Platform 118
▼ To Create a New Site Name 120
▼ To Create a New Instance Name 120
▼ To Create a New Character Set 121

Part III File Reference 123

6 amConfig.properties Reference 125
About the `AMConfig.properties` File 126
Access Manager Console 126
Access Manager Server Installation 126
am.util 128
amSDK 128
Application Server Installation 128
Authentication 129
Certificate Database 130
Cookies 130
Debugging 131
Directory Server Installation 132
Event Connection 132
Global Services Management 133
Helper Daemons 133
Identity Federation 134
JSS Proxy 135
LDAP Connection 136
Liberty Alliance Interactions 136
Logging Service 140
Logging Properties You Can Add to AMConfig.properties 140
Naming Service 141
Notification Service 142
Policy Agents 142
Policy Client API 144

Profile Service 144
Replication 145
SAML Service 145
Security 146
Session Service 147
SMTP 148
Statistics Service 148

7 serverconfig.xml Reference 149
Overview 149
Proxy User 149
Admin User 150
server-config Definition Type Document 150
iPlanetDataAccessLayer Element 151
ServerGroup Element 151
Server Element 151
User Element 151
BaseDN Element 152
MiscConfig Element 152
Failover Or Multimaster Configuration 153

Part IV Error Codes and Log File Reference 155

8 Access Manager Component Error Codes 157
Access Manager Console Errors 157
Authentication Error Codes 159
Policy Error Codes 162
amadmin Error Codes 163

9 Access Manager Log File Reference 169
Log Reference for amadmin Command Line Utility 169
Log Reference for Authentication 186
Access Manager Console 201
Federation 295

Liberty 299
Policy 302
SAML 304
Session 310

Preface

The Sun Java System Access Manager 7.1 Administration Guide describes how to use the Sun Java™ System Access Manager console as well as manage user and service data via the command line interface.

Access Manager is a component of the Sun Java Enterprise System (Java ES), a set of software components that provide services needed to support enterprise applications distributed across a network or Internet environment.

Who Should Use This Book

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

Before You Read This Book

Readers should be familiar with the following components and concepts:

- Access Manager technical concepts as described in the *Sun Java System Access Manager 7.1 Technical Overview*
- Deployment platform: Solaris™ or Linux operating system
- Web container that will run Access Manager: Sun Java System Application Server, Sun Java System Web Server, BEA WebLogic, or IBM WebSphere Application Server
- Technical concepts: Lightweight Directory Access Protocol (LDAP), Java technology, JavaServer Pages™ (JSP) technology, HyperText Transfer Protocol (HTTP), HyperText Markup Language (HTML), and eXtensible Markup Language (XML)

Related Books

Related documentation is available as follows:

Access Manager Core Documentation

The Access Manager core documentation set contains the following titles:

- The *Sun Java System Access Manager 7.1 Release Notes* will be available online after the product is released. It gathers an assortment of last-minute information, including a description of what is new in this current release, known problems and limitations, installation notes, and how to report issues with the software or the documentation.
- The *Sun Java System Access Manager 7.1 Technical Overview* provides an overview of how Access Manager components work together to consolidate access control functions, and to protect enterprise assets and web-based applications. It also explains basic Access Manager concepts and terminology.
- The *Sun Java System Access Manager 7.1 Deployment Planning Guide* provides planning and deployment solutions for Sun Java System Access Manager based on the solution life cycle
- The *Sun Java System Access Manager 7.1 Postinstallation Guide* provides information on configuring Access Manager after installation.
- The *Sun Java System Access Manager 7.1 Performance Tuning Guide* provides information on how to tune Access Manager and its related components for optimal performance.
- The *Sun Java System Access Manager 7.1 Administration Guide* describes how to use the Access Manager console as well as manage user and service data via the command line interface.
- The *Sun Java System Access Manager 7.1 Federation and SAML Administration Guide* provides information about the Federation module based on the Liberty Alliance Project specifications. It includes information on the integrated services based on these specifications, instructions for enabling a Liberty-based environment, and summaries of the application programming interface (API) for extending the framework.
- The *Sun Java System Access Manager 7.1 Developer's Guide* offers information on how to customize Access Manager and integrate its functionality into an organization's current technical infrastructure. It also contains details about the programmatic aspects of the product and its API.
- The *Sun Java System Access Manager 7.1 C API Reference* provides summaries of data types, structures, and functions that make up the public Access Manager C APIs.
- The *Java API Reference*provides information about the implementation of Java packages in Access Manager.
- The *Sun Java System Access Manager Policy Agent 2.2 User's Guide* provides an overview of the policy functionality and the policy agents available for Access Manager.

Updates to the *Release Notes* and links to modifications of the core documentation can be found on the Access Manager page at the Sun Java Enterprise System documentation web site. Updated documents will be marked with a revision date.

Sun Java Enterprise System Product Documentation

Useful information can be found in the documentation for the following products:

- Directory Server
- Web Server
- Application Server
- Web Proxy Server

Related Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Documentation, Support, and Training

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

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

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX® system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–2 Shell Prompts

Shell	Prompt
C shell	`machine_name%`
C shell for superuser	`machine_name#`
Bourne shell and Korn shell	`$`
Bourne shell and Korn shell for superuser	`#`

Sun Welcomes Your Comments

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

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

For example, the title of this book is *Sun Java System Access Manager 7.1 Administration Guide*, and the part number is 819-4176.

PART I

Command Line Interface Reference

CHAPTER 1

The amadmin Command Line Tool

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

The amadmin Command Line Executable

The primary purposes of the command line executable `amadmin` is to load XML service files into the data store and to perform batch administrative tasks on the DIT. `amadmin` can be found in `AccessManager-base/SUNWam/bin` and is used to:

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

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

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

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

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

The amadmin Syntax

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

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

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

---

amadmin Options

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

--runasdn (-u)

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

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

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

--password (-w)

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

--locale (-l)

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

--continue (-c)

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

--session (-m)

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

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

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

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

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

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

While using the following option:

`amadmin -m | --session` servername pattern

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

--debug (-d)

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

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

--verbose (-v)

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

--data (-t)

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

--schema (-s)

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

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

--addattributes (-a)

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

--deleteservice (-r)

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

--serviceName

`--serviceName` is an option that takes a value equal to the service name which is defined under the `Service name=...` tag of an XML service file. This portion is displayed in "--serviceName" on page 20.

EXAMPLE 1–1 Portion of `sampleMailService.xml`

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

EXAMPLE 1–1 Portion of `sampleMailService.xml` *(Continued)*

```
...
```

--help (-h)

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

--version (-n)

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

Using amadmin for Federation Management

This section lists the parameters of amadmin for use with Federation Management. For more information on Federation Management, see the Access Manager Federation Management Guide.

Loading the Liberty meta compliance XML into Directory Server

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

--runasdn (-u)

The user's DN

--password (-w)

The user's password.

--passwordfile (-f)

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

--entityname (-e)

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

--import (-g)

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

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

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

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

--runasdn (-u)

The user's DN

--password (-w)

The user's password.

--passwordfile (-f)

The name of file that contains user's password.

--entityname (--e)

The name of Entity that resides in the Directory Server

--export (-o)

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

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

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

--runasdn (-u)

The user's DN

--password (-w)

The user's password.

--passwordfile (-f)

The name of file that contains user's password.

--entityname (--e)

The name of Entity that resides in the Directory Server

--export (-o)

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

--xmlsig (-x)

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

Using amadmin for Resource Bundles

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

Add resource bundle.

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

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

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

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

Get resource strings.

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

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

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

Remove resource bundle.

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

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

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

CHAPTER 2

The ampassword Command Line Tool

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

- "The ampassword Command Line Executable" on page 25

The ampassword Command Line Executable

Access Manager contains an `ampassword` utility under `/opt/SUNWam/bin` on SPARC systems and `/opt/sun/Identity/bin` on Linux systems. This utility allows you change the Directory Server password for the administrator or user.

To Run ampassword with Access Manager in SSL mode

1. **Modify the `serverconfig.xml` file, located in the following directory:**

   `AccessManager-base/SUNWam/config/`

2. **Change `port` the server attribute to the SSL port which Access Manager is running.**

3. **Change the `type` attribute to SSL.**

   For example:

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

```
                    AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
        </DirPassword>
 </User> ...
```

`ampassword` only changes the password in Directory Server. You will have to manually change passwords in the `ServerConfig.xml` and all authentication templates for Access Manager.

CHAPTER 3

The VerifyArchive Command Line Tool

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

- "The VerifyArchive Command Line Executable" on page 27

The VerifyArchive Command Line Executable

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

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

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

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

VerifyArchive Syntax

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

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

VerifyArchive Options

logName

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

path

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

uname

`uname` is the user id of the Access Manager administrator.

password

`password` is the password of the Access Manager adminstrator.

CHAPTER 4

The amsecuridd Helper

This chapter provides information on the `amsecuiridd` helper and contains the following section:

- "The amsecuridd Helper Command Line Executable" on page 29
- "Running the amsecuridd helper" on page 30

The amsecuridd Helper Command Line Executable

The Access Manager SecurID authentication module is implemented using the Security Dynamic ACE/Client C API and the `amsecruidd` helper, which communicates between the Access Manager SecurID authentication module and the SecurID Server. The SecurID authentication module invokes the `amsecuridd` daemon by opening a socket to `localhost:57943` to listen for SecurID authentication requests.

Note – `57943` is the default port number. If this port number is already used, you can specify a different port number in the SecurID Helper Authentication Port attribute in the SecurID Authentication module. This port number must be unique accross all organizations.

Because the interface to `amsecuridd` is in clear text through `stdin`, only local host connections are permitted. `amsecuridd` uses the SecurID remote API (version 5.x) on the back end for data encryption.

The `amsecuridd` helper listens on port number `58943` (by default) to receive its configuration information. If this port is already used, you can change it in the `securidHelper.ports` attribute in the `AMConfig.properties` file (by default, located in AccessManager-base `/SUNWam/config/`). The `securidHelp.ports` attribute contains a space-separated list of the ports for each `amsecuridd` helper instance. Restart Access Manager once the changes to `AMConfig.properties` are saved.

Note – A separate instance of `amsecuridd` should run for each organization that communicates with a separate ACE/Server (containing different `sdconf.rec` files).

---

amsecuridd Syntax

The syntax is as follows:

```
amsecuridd [-v] [-c portnum]
```

amsecuridd Options

verbose (-v)

Turns on verbose mode and logs to `/var/opt/SUNWam/debug/securidd_client.debug`.

configure portnumber (-c portnm)

Configures the listening port number. The default is 58943.

Running the amsecuridd helper

`amsecuridd` is located, by default, in *AccessManager-base* `/SUNWam/share/bin`. To run the helper on the default ports, enter the following command (without options):

```
./amsecuridd
```

To run the helper on non-default port, enter the following command:

```
./amsecuridd [-v] [-c portnm]
```

`amsecuridd` can also be run through the `amserver` command line utitility, but it will only run on the default ports.

Required Libraries

In order to run the helper, the following libraries are required (most can be found in the operating system in `/usr/lib/`):

- `libnsl.so.1`
- `libthread.so.1`
- `libc.so.1`
- `libdl.so.1`

- `libmp.so.2`
- `librt.so.1`
- `libaio.so.1`
- `libmd5.so.1`

Note – Set `LD_LIBRARY_PATH` to *AccessManager-base* `/Sunwam/lib/` to find `libaceclnt.so`.

PART II

Configuration Attribute Reference

CHAPTER 5

Configuration Attributes

The Configuration page contains all of the attributes to configure Access Manager's default services. The attributes that comprise an Access Manager service are classified as one of the following types (some services may have more than one type):

Global – Applied across the Access Manager configuration. They cannot be applied to users, roles or realms as the goal of global attributes is to customize the Identity Server application.

Realm – Realm attributes are only assigned to realms. No object classes are associated with realm attributes. Attributes listed in the authentication services are defined as realm attributes because authentication is done at the realm level rather than at a subtree or user level.

Dynamic – Assigned to an Access Manager configured role or realm. When the role is assigned to a user or a user is created in an realm, the dynamic attribute then becomes a characteristic of the user.

User – Assigned directly to each user. They are not inherited from a role or an realm and, typically, are different for each user.

The Configuration properties you can modify are:

- "Authentication" on page 36
- "Console Properties" on page 80
- "Global Properties" on page 95
- "System Properties" on page 108

Authentication

Access Manager is installed with a set of default authentication module types. An authentication module instance is a plug-in that collects user information such as a user ID and password, checks the information against entries in a database, and allows or denies access to the user. Multiple instances of the same type can be created and configured separately.

This section provides attribute descriptions that configure the default authentication module types.

- "Anonymous" on page 36
- "Active Directory" on page 38
- "Authentication Configuration" on page 42
- "Certificate" on page 42
- "Core" on page 47
- "Data Store" on page 54
- "HTTP Basic" on page 55
- "JDBC" on page 55
- "LDAP" on page 58
- "Membership" on page 62
- "MSISDN" on page 66
- "RADIUS" on page 69
- "SafeWord" on page 71
- "SAML" on page 73
- "SecurID" on page 73
- "UNIX" on page 74
- "Windows Desktop SSO" on page 76
- "Windows NT" on page 77
- "Supported Language Locales" on page 79

Anonymous

This module type allows a user to log in without specifying credentials. You can create an Anonymous user so that anyone can log in as Anonymous without having to provide a password. Anonymous connections are usually customized by the Access Manager administrator so that Anonymous users have limited access to the server. The Anonymous authentication attributes are realm attributes. The attributes are:

- "Valid Anonymous Users" on page 37
- "Default Anonymous User Name" on page 37
- "Case Sensitive User IDs" on page 37
- "Authentication Level" on page 37

Valid Anonymous Users

Contains a list of user IDs that have permission to login without providing credentials. If a user's login name matches a user ID in this list, access is granted and the session is assigned to the specified user ID.

If this list is empty, accessing the following default module instance login URL will be authenticated as the Default Anonymous User Name:

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?
module=Anonymous&org=org_name
```

If this list is not empty, accessing Default module instance login URL (same as above) will prompt the user to enter any valid Anonymous user name. If this list is not empty, the user can log in without seeing the login page by accessing the following URL:

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?
module=Anonymous&org=org_name&IDToken1=<valid Anonymous username>
```

Default Anonymous User Name

Defines the user ID that a session is assigned to if Valid Anonymous User List is empty and the following default module instance login URL is accessed:

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?
module=Anonymous&org=org_name
```

The default value is anonymous. An Anonymous user must also be created in the realm.

Note – If Valid Anonymous User List is not empty, you can login without accessing the login page by using the user defined in Default Anonymous User Name. This can be done by accessing the following URL:

`protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name&IDToken1=` *DefaultAnonymous User Name*

Case Sensitive User IDs

If enabled, this option allows for case-sensitivity for user IDs. By default, this attribute is not enabled.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the

user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

Active Directory

This module type works similarly to the LDAP authentication module type, but uses the Microsoft Active Directory instead of an LDAP directory. Using this module type makes it possible to have both LDAP and Active Directory coexist under the same realm. The Active Directory authentication attributes are realm attributes. The attributes are:

- "Primary Active Directory Server" on page 38
- "Secondary Active Directory Server" on page 39
- "DN to Start User Search" on page 39
- "DN for Root User Bind" on page 39
- "Password for Root User Bind" on page 40
- "Password for Root User Bind (confirm)" on page 40
- "Attribute Used to Retrieve User Profile" on page 40
- "Attributes Used to Search for a User to be Authenticated" on page 40
- "User Search Filter" on page 40
- "Search Scope" on page 40
- "SSL Access to Active Directory Server" on page 41
- "Return User DN to Authenticate" on page 41
- "Active Directory Server Check Interval" on page 41
- "User Creation Attributes" on page 41
- "Authentication Level" on page 42

Primary Active Directory Server

Specifies the host name and port number of the primary Active Directory server specified during Access Manager installation. This is the first server contacted for Active Directory authentication. The format is*hostname:port*. If there is no port number, assume `389`.

If you have Access Manager deployed with multiple domains, you can specify the communication link between specific instances of Access Manager and Directory Server in the following format (multiple entries must be prefixed by the local server name):

```
local_servername|server:port local_servername2|server2:port2 ...
```

For example, if you have two Access Manager instances deployed in different locations (L1-machine1-IS and L2- machine2-IS) communicating with different instances of Directory Server (L1-machine1-DS and L2-machine2-DS), it would look the following:

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389

L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

Secondary Active Directory Server

Specifies the host name and port number of a secondary Active Directory server available to the Access Manager platform. If the primary Active Directory server does not respond to a request for authentication, this server would then be contacted. If the primary server is up, Access Manager will switch back to the primary server. The format is also *hostname:port*. Multiple entries must be prefixed by the local server name.

Caution – When authenticating users from a Directory Server that is remote from the Access Manager enterprise, it is important that both the Primary and Secondary LDAP Server Ports have values. The value for one Directory Server location can be used for both fields.

DN to Start User Search

Specifies the DN of the node where the search for a user would start. (For performance reasons, this DN should be as specific as possible.) The default value is the root of the directory tree. Any valid DN will be recognized. If OBJECT is selected in the Search Scope attribute, the DN should specify one level above the level in which the profile exists. Multiple entries must be prefixed by the local server name. The format is *servername*|*search dn*.

For multiple entries:

servername1|*search dn servername2*|*search dn servername3*|*search dn* . . .

If multiple entries exist under the root organization with the same user ID, then this parameter should be set so that the only one entry can be searched for or found in order to be authenticated. For example, in the case where the agent ID and user ID is same under root org, this parameter should be `ou=Agents` for the root organization to authenticate using Agent ID and `ou=People,` for the root organization to authenticate using User ID.

DN for Root User Bind

Specifies the DN of the user that will be used to bind to the Directory Server specified in the Primary LDAP Server and Port field as administrator. The authentication service needs to bind as this DN in order to search for a matching user DN based on the user login ID. The default is `amldapuser.` Any valid DN will be recognized.

Make sure that password is correct before you logout. If it is incorrect, you will be locked out. If this should occur, you can login with the super user DN in the *com.iplanet.authentication.super.user* property in the `AMConfig.Properties` file. By default, this the `amAdmin` account with which you would normally log in, although you will use the full DN. For example:

`uid_amAdmin,ou=People,`*AccessManager-base*

Password for Root User Bind

Carries the password for the administrator profile specified in the DN for Root User Bind field. There is no default value. Only the administrator's valid Active Directory password is recognized.

Password for Root User Bind (confirm)

Confirm the password.

Attribute Used to Retrieve User Profile

Specifies the attribute used for the naming convention of user entries. By default, Access Manager assumes that user entries are identified by the uid attribute. If your Directory Server uses a different attribute (such as *givenname*) specify the attribute name in this field.

Attributes Used to Search for a User to be Authenticated

Lists the attributes to be used to form the search filter for a user that is to be authenticated, and allows the user to authenticate with more than one attribute in the user's entry. For example, if this field is set to *uid*, *employeenumber* , and *mail*, the user could authenticate with any of these names.

User Search Filter

Specifies an attribute to be used to find the user under the DN to Start User Search field. It works with the User Naming Attribute. There is no default value. Any valid user entry attribute will be recognized.

Search Scope

Indicates the number of levels in the Directory Server that will be searched for a matching user profile. The search begins from the node specified in DN to Start User Search. The default value is SUBTREE. One of the following choices can be selected from the list:

OBJECT	Searches only the specified node.
ONELEVEL	Searches at the level of the specified node and one level down.
SUBTREE	Search all entries at and below the specified node.

SSL Access to Active Directory Server

Enables SSL access to the Directory Server specified in the Primary and Secondary Server and Port field. By default, the box is not checked and the SSL protocol will not be used to access the Directory Server.

If the Active Directory server is running with SSL enabled (LDAPS), you must make sure that Access Manager is configured with proper SSL trusted certificates so that AM could connect to Directory server over LDAPS protocol

Return User DN to Authenticate

When the Access Manager directory is the same as the directory configured for Active Directory, this option may be enabled. If enabled, this option allows the Active Directory authentication module instance to return the DN instead of the User ID, and no search is necessary. Normally, an authentication module instance returns only the User ID, and the authentication service searches for the user in the local Access Manager instance. If an external Active Directory is used, this option is typically not enabled.

Active Directory Server Check Interval

This attribute is used for Active Directory Server failback. It defines the number of minutes in which a thread will "sleep" before verifying that the primary Active Directory server is running.

User Creation Attributes

This attribute is used by the Active Directory authentication module instance when the Active Directory server is configured as an external Active Directory server. It contains a mapping of attributes between a local and an external Directory Server. This attribute has the following format:

attr1|*externalattr1*

attr2|*externalattr2*

When this attribute is populated, the values of the external attributes are read from the external Directory Server and are set for the internal Directory Server attributes. The values of the external attributes are set in the internal attributes only when the `User Profile`attribute (in the Core Authentication module type) is set to Dynamically Created and the user does not exist in local Directory Server instance. The newly created user will contain the values for internal attributes, as specified in User Creation Attributes List, with the external attribute values to which they map.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

Authentication Configuration

Once an authentication module instance is defined, the instance can be configured for authentication module chaining, to supply redirect URLs, and a post-processing Java class specification based on a successful or failed authentication process. Before an authentication module instance can be configured, the Core authentication attribute "Organization Authentication Configuration" on page 51 must be modified to include the specific authentication module instance name.

Certificate

This module enables a user to log in through a personal digital certificate (PDC). The module instance can require the use of the Online Certificate Status Protocol (OCSP) to determine the state of a certificate. Use of the OCSP is optional. The user is granted or denied access to a resource based on whether or not the certificate is valid. The Certificate authentication attributes are realm attributes. The attributes are:

- "Match Certificate in LDAP" on page 43
- "Subject DN Attribute Used to Search LDAP for Certificates" on page 43
- "Match Certificate to CRL" on page 43
- "Issuer DN Attribute Used to Search LDAP for CRLs" on page 44
- "HTTP Parameters for CRL Update" on page 44
- "OCSP Validation" on page 44
- "LDAP Server Where Certificates are Stored" on page 44
- "LDAP Start Search DN" on page 45
- "LDAP Server Principal User" on page 45
- "LDAP Server Principal Password" on page 45
- "LDAP Server Principal Password (confirm)" on page 45

- "LDAP Attribute for Profile ID" on page 45
- "Use SSL for LDAP Access" on page 46
- "Certificate Field Used to Access User Profile" on page 46
- "Other Certificate Field Used to Access User Profile" on page 46
- "Trusted Remote Hosts" on page 46
- "SSL Port Number" on page 46
- "Authentication Level" on page 47

Match Certificate in LDAP

Specifies whether to check if the user certificate presented at login is stored in the LDAP Server. If no match is found, the user is denied access. If a match is found and no other validation is required, the user is granted access. The default is that the Certificate Authentication service does not check for the user certificate.

Note – A certificate stored in the Directory Server is not necessarily valid; it may be on the certificate revocation list. See "Match Certificate to CRL" on page 43. However, the web container may check the validity of the user certificate presented at login.

Subject DN Attribute Used to Search LDAP for Certificates

Specifies the attribute of the certificate's *SubjectDN* value that will be used to search LDAP for certificates. This attribute must uniquely identify a user entry. The actual value will be used for the search. The default is `cn`.

Match Certificate to CRL

Specifies whether to compare the user certificate against the Certificate Revocation List (CRL) in the LDAP Server. The CRL is located by one of the attribute names in the issuer's *SubjectDN*. If the certificate is on the CRL, the user is denied access; if not, the user is allowed to proceed. This attribute is, by default, not enabled.

Certificates should be revoked when the owner of the certificate has changed status and no longer has the right to use the certificate or when the private key of a certificate owner has been compromised.

When the Certificate authentication module possesses a client certificate for authentication, it checks the configured option first. If CRL validation is enabled, it accesses the CRL from the local Directory Server. If the CRL is valid, it validates the client certificate with the current CRL from the local Directory Server.

If the CRL is not valid or needs to be updated, it retrieves CRLDP information from the client certificate and gets a new CRL from the CRLDP and replaces the old CRL with a new one. If the CRL is not valid or needs to be updated but the client certificate does not have CRLDP, it

retrieves IssuingDP information from the current CRL and gets the new CRL from the IssuingDP and replaces the old CRL with a new one. It then validates the client certificate with this new CRL.

Issuer DN Attribute Used to Search LDAP for CRLs

Specifies the attribute of the received certificate's issuer *subjectDN* value that will be used to search LDAP for CRLs. This field is used only when the Match Certificate to CRL attribute is enabled. The actual value will be used for the search. The default is `cn`.

HTTP Parameters for CRL Update

Specifies the HTTP parameters for obtaining a CRL from a servlet for a CRL update. Contact the administrator of your CA for these parameters.

OCSP Validation

Enables OCSP validation to be performed by contacting the corresponding OCSP responder. The OCSP responder is decided as follows during runtime:

- If `com.sun.identity.authentication.ocspCheck` is true and the OCSP responder is set in the *com.sun.identity.authentication.ocsp.repsonder.url* attribute, the value of the attribute will be used as the OCSP responder.
- If `com.sun.identity.authentication.ocspCheck` is set to true and If the value of the attribute is not set in the `AMConfig.properties` file, the OCSP responder presented in your client certificate is used as the OCSP responder.
- If `com.sun.identity.authentication.ocspCheck` is set to false or if *com.sum.identity.authentication.ocspCheck* is set to true and if an OCSP responder can not be found, no OCSP validation will be performed.

Before enabling OCSP Validation, make sure that the time of the Access Manager machine and the OCSP responder machine are in sync as close as possible. Also, the time on the Access Manager machine must not be behind the time on the OCSP responder. For example:

```
OCSP responder machine - 12:00:00 pm

Access Manager machine - 12:00:30 pm
```

LDAP Server Where Certificates are Stored

Specifies the name and port number of the LDAP server where the certificates are stored. The default value is the host name and port specified when Access Manager was installed. The host name and port of any LDAP Server where the certificates are stored can be used. The format is `hostname:port`.

LDAP Start Search DN

Specifies the DN of the node where the search for the user's certificate should start. There is no default value. The field will recognize any valid DN.

Multiple entries must be prefixed by the local server name. The format is as follows:

```
servername|search dn
```

For multiple entries:

```
servername1|search dn servername2|search dn servername3|search dn...
```

If multiple entries exist under the root organization with the same user ID, then this parameter should be set so that the only one entry can be searched for or found in order to be authenticated. For example, in the case where the agent ID and user ID is same under root org, this parameter should be `ou=Agents` for the root organization to authenticate using Agent ID and `ou=People,` for the root organization to authenticate using User ID.

LDAP Server Principal User

This field accepts the DN of the principal user for the LDAP server where the certificates are stored. There is no default value for this field which will recognize any valid DN. The principal user must be authorized to read, and search certificate information stored in the Directory Server.

LDAP Server Principal Password

This field carries the LDAP password associated with the user specified in the LDAP Server Principal User field. There is no default value for this field which will recognize the valid LDAP password for the specified principal user. This value is stored as readable text in the directory.

LDAP Server Principal Password (confirm)

Confirm the password.

LDAP Attribute for Profile ID

Specifies the attribute in the Directory Server entry that matches the certificate whose value should be used to identify the correct user profile. There is no default value for this field which will recognize any valid attribute in a user entry (*cn*, *sn*, and so forth) that can be used as the UserID.

Use SSL for LDAP Access

Specifies whether to use SSL to access the LDAP server. The default is that the Certificate Authentication service does not use SSL for LDAP access.

Certificate Field Used to Access User Profile

Specifies which field in the certificate's Subject DN should be used to search for a matching user profile. For example, if you choose email address, the certificate authentication service will search for the user profile that matches the attribute *emailAddr* in the user certificate. The user logging in then uses the matched profile. The default field is *subject CN*. The list contains:

- email address
- subject CN
- subject DN
- subject UID
- other

Other Certificate Field Used to Access User Profile

If the value of the Certificate Field Used to Access User Profile attribute is set to other, then this field specifies the attribute that will be selected from the received certificate's *subjectDN* value. The authentication service will then search the user profile that matches the value of that attribute.

Trusted Remote Hosts

Defines a list of trusted hosts that can be trusted to send certificates to Access Manager. Access Manager must verify whether the certificate emanated from one of these hosts. This attribute is only used for SSL termination.

none	Disables the attribute. This is set by default.
all	Accepts Portal Server Gateway-style certificate authentication from any client IP address.
IP ADDR	Lists the IP addresses from which to accept Portal Server Gateway-style certificate authentication requests (the IP Address of the Gateway(s)). The attribute is configurable on an realm basis.

SSL Port Number

Specifies the port number for the secure socket layer. Currently, this attribute is only used by the Gateway servlet. Before you add or change an SSL Port Number, see the "Policy-Based Resource Management" section in the Access Manager Administration Guide.

HTTP Header Name for Client Certificate

This attribute is used only when the Trusted Remote Hosts attribute is set to all or has a specific host name defined. The administrator must specify the http header name for the client certificate that is inserted by the load balancer or SRA.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core authentication attribute "Default Authentication Level" on page 54.

Core

This module is the general configuration base for the Access Manager authentication services. It must be registered and configured to use any of the specific authentication module instances. It enables the administrator to define default values that will be picked up for the values that are not specifically set in the Access Manager default authentication modules. The Core attributes are global and realm. The attributes are:

- "Pluggable Authentication Module Classes" on page 48
- "Supported Authentication Module for Clients" on page 48
- "LDAP Connection Pool Size" on page 48
- "Default LDAP Connection Pool Size" on page 49
- "User Profile" on page 49
- "Administrator Authentication Configuration" on page 49
- "User Profile Dynamic Creation Default Roles" on page 49
- "Persistent Cookie Mode" on page 50
- "Persistent Cookie Maximum Time" on page 50
- "Alias Search Attribute Name" on page 50
- "Default Authentication Locale" on page 50
- "Organization Authentication Configuration" on page 51
- "Login Failure Lockout Mode" on page 51
- "Login Failure Lockout Count" on page 51
- "Login Failure Lockout Interval" on page 51
- "Email Address to Send Lockout Notification" on page 51

- "Warn User After N Failures" on page 51
- "Login Failure Lockout Duration" on page 52
- "Lockout Attribute Name" on page 52
- "Lockout Attribute Value" on page 52
- "Default Success Login URL" on page 52
- "Default Failure Login URL" on page 52
- "Authentication Post Processing Class" on page 52
- "Generate UserID Mode" on page 53
- "Pluggable User Name Generator Class" on page 53
- "Identity Types" on page 53
- "Pluggable User Status Event Classes" on page 53
- "Store Invalid Attempts in Data Store" on page 53
- "Module-based Authentication" on page 53
- "Default Authentication Level" on page 54

Pluggable Authentication Module Classes

Specifies the Java classes of the authentication modules available to any realm configured within the Access Manager platform. You can write custom authentication modules by implementing the AMLoginModule SPI or the JAAS LoginModule SPI. For more information, see the Access Manager Developer's Guide. To define new services, this field must take a text string specifying the full class name (including package name) of each new authentication service.

Supported Authentication Module for Clients

Specifies a list of supported authentication modules for a specific client. The format is as follows:

```
clientType | module1,module2,module3
```

This attribute is in effect when Client Detection is enabled.

LDAP Connection Pool Size

Specifies the minimum and maximum connection pool to be used on a specific LDAP server and port. This attribute is for LDAP and Membership authentication services only. The format is as follows:

```
host:port:min:max
```

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

Default LDAP Connection Pool Size

Sets the default minimum and maximum connection pool to be used with all LDAP authentication module configurations. If an entry for the host and port exists in the LDAP Connection Pool Size attribute, the minimum and maximum settings will not be used from LDAP Connection Default Pool Size.

User Profile

This option enables you to specify options for a user profile. The options are:

Required This specifies that on successful authentication, the user needs to have a profile in the local Directory Server installed with Access Manager for the authentication service to issue an SSOToken.

Dynamic This specifies that on successful authentication, the authentication service will create the user profile if one does not already exist. The SSOToken will then be issued. The user profile is created in the local Directory Server installed with Access Manager.

Dynamic With User Alias This specifies that on successful authentication, the authentication services will create the user profile with the User Alias List attribute.

Ignore This specifies that the user profile is not required by the authentication service to issue the SSOToken for a successful authentication.

Administrator Authentication Configuration

Defines the authentication service for administrators only. This attribute can be used if the authentication module for administrators needs to be different from the module for end users. The modules configured in this attribute are picked up when the Access Manager console is accessed. For example:

`http://`*servername.port/console_deploy_uri*

User Profile Dynamic Creation Default Roles

This field specifies the roles assigned to a new user whose profiles are created if Dynamic Creation is selected through the User Profile. There is no default value. The administrator must specify the DNs of the roles that will be assigned to the new user.

Note – The role specified must be under the realm for which authentication is being configured. This role can be either an Access Manager or LDAP role, but it cannot be a filtered role.

If you wish to automatically assign specific services to the user, you have to configure the Required Services attribute in the User Profile.

Persistent Cookie Mode

This option determines whether users can restart the browser and still return to their authenticated session. User sessions can be retained by enabling Enable Persistent Cookie Mode. When Enable Persistent Cookie Mode is enabled, a user session does not expire until its persistent cookie expires, or the user explicitly logs out. The expiration time is specified in Persistent Cookie Maximum Time. The default value is that Persistent Cookie Mode is not enabled and the authentication service uses only memory cookies.

Note – A persistent cookie must be explicitly requested by the client using the *iPSPCookie=yes* parameter in the login URL.

Persistent Cookie Maximum Time

Specifies the interval after which a persistent cookie expires. The interval begins when the user's session is successfully authenticated. The maximum value is 2147483647 (time in seconds). The field will accept any integer value less than the maximum.

Alias Search Attribute Name

After successful authentication by a user, the user's profile is retrieved. This field specifies a second LDAP attribute to search from if a search on the first LDAP attribute fails to locate a matching user profile. Primarily, this attribute will be used when the user identification returned from an authentication module is not the same as that specified in User Naming Attribute. For example, a RADIUS server might return `abc1234` but the user name is `abc`. There is no default value for this attribute.

The field will take any valid LDAP attribute (for example, cn).

Default Authentication Locale

Specifies the default language subtype to be used by the authentication service. The default value is en_US. See "Supported Language Locales" on page 79 for a listing of valid language subtypes.

In order to use a different locale, all authentication templates for that locale must first be created. A new directory must then be created for these templates. See "Login URL Parameters" in the Administration Guide for more information.

Organization Authentication Configuration

Sets the authentication module for the organization. The default authentication module is LDAP.

Login Failure Lockout Mode

Specifies whether a user can attempt a second authentication if the first attempt failed. Selecting this attribute enables a lockout and the user will have only one chance at authentication. By default, the lockout feature is not enabled. This attribute works in conjunction with Lockout-related and notification attributes.

Login Failure Lockout Count

Defines the number of attempts that a user may try to authenticate, within the time interval defined in Login Failure Lockout Interval, before being locked out.

Login Failure Lockout Interval

Defines (in minutes) the time between two failed login attempts. If a login fails and is followed by another failed login that occurs within the lockout interval, then the lockout count is incremented. Otherwise, the lockout count is reset.

Email Address to Send Lockout Notification

Specifies an email address that will receive notification if a user lockout occurs. To send email notification to multiple addresses, separate each email address with a space. For non-English locales, the format is:

```
email_address|locale|charset
```

Warn User After N Failures

Specifies the number of authentication failures that can occur before Access Manager sends a warning message that the user will be locked out.

Login Failure Lockout Duration

Enables memory locking. By default, the lockout mechanism will inactivate the User Profile (after a login failure) defined in *Lockout Attribute Name*. If the value of Login Failure Lockout Duration is greater than 0, then its memory locking and the user account will be locked for the number of minutes specified.

Lockout Attribute Name

Designates any LDAP attribute that is to be set for lockout. The value in Lockout Attribute Value must also be changed to enable lockout for this attribute name. By default, Lockout Attribute Name is empty in the Access Manager Console. The default implementation values are *inetuserstatus* (LDAP attribute) and *inactive* when the user is locked out and Login Failure Lockout Duration is set to 0.

Lockout Attribute Value

This attribute specifies whether lockout is enabled or disabled for the attribute defined in Lockout Attribute Name. By default, the value is set to inactive for *inetuserstatus*.

Default Success Login URL

This field accepts a list of multiple values that specify the URL to which users are redirected after successful authentication. The format of this attribute is `clientType|URL`, although you can specify only the value of the URL which assumes a default type of HTML. The default value is */amserver/console* .

Default Failure Login URL

This field accepts a list of multiple values that specify the URL to which users are redirected after an unsuccessful authentication. The format of this attribute is `clientType|URL`, although you can specify only the value of the URL which assumes a default type of HTML.

Authentication Post Processing Class

Specifies the name of the Java class used to customize post authentication processes for successful or unsuccessful logins. Example:

```
com.abc.authentication.PostProcessClass
```

The Java class must implement the following Java interface:

```
com.sun.identity.authentication.spi.AMPostAuthProcessInterface
```

Additionally, you must add the path to where the class is located to the Web Server's Java Classpath attribute.

Generate UserID Mode

This attribute is used by the Membership authentication module. If this attribute field is enabled, the Membership module is able to generate user IDs, during the Self Registration process, for a specific user if the user ID already exists. The user IDs are generated from the Java class specified in Pluggable User Name Generator Class.

Pluggable User Name Generator Class

Specifies the name of the Java class is used to generate User IDs when Enable Generate UserID Mode is used.

Identity Types

Lists the type or types of identities for which Access Manager will search.

Pluggable User Status Event Classes

Extends the authentication SPIs to provide a callback mechanism for user status changes during the authentication process. The following status changes are supported:

`account lockout` The account lockout event is available for any authentication module. The features is configurable through the "Login Failure Lockout Mode" on page 51 attribute.

`password change` Only available through the LDAP authentication module type, as the password change feature is only available for that module.

Store Invalid Attempts in Data Store

If enabled, this attribute allows the sharing of login failure attempts in a identity repository that is shared by multiple Access Manager instances. For example, if the identity repository that is used for a specific deployment is Directory Server, the invalid attempts are stored in the `sunAMAuthInvalidAttemptsData` (which belongs to `sunAMAuthAccountLockout`objectclass). The format of the data is stored as:

```
<InvalidPassword><InvalidCount></InvalidCount><LastInvalidAt></LastInvalidAt><Lockedo
```

This information is maintained in the Directory Server for each user. As the invalid attempts occur, `<InvalidCount>` is increased.

Module-based Authentication

If enabled, this attribute allows users to authenticate through module-based authentication. If this attribute is not enabled, module-based login is not allowed. All login attempts with `module=<` *module_instance_name*> will result in login failure.

Default Authentication Level

The authentication level value indicates how much to trust authentications. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application can use the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level.

The authentication level should be set within the realm's specific authentication template. The Default Authentication Level value described here will apply only when no authentication level has been specified in the Authentication Level field for a specific realm's authentication template. The Default Authentication Level default value is 0. (The value in this attribute is not used by Access Manager but by any external application that may chose to use it.)

Data Store

The Data Store authentication module allows a login using the Identity Repository of the realm to authenticate users. Using the Data Store module removes the requirement to write an authentication plug- in module, load, and then configure the authentication module if you need to authenticate against the same data store repository. Additionally, you do not need to write a custom authentication module where flat-file authentication is needed for the corresponding repository in that realm.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

HTTP Basic

The HTTP authentication module allows a login using the HTTP basic authentication with no data encryption. A user name and password are requested through the use of a web browser. Credentials are validated internally using the LDAP authentication module.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

JDBC

The Java Database Connectivity (JDBC) authentication module allows Access Manager to authenticate users through any Structured Query Language (SQL) databases that provide JDBC-enabled drivers. The connection to the SQL database can be either directly through a JDBC driver or through a JNDI connection pool. The JDBC attributes are realm attributes. The attributes are:

- "Connection Type" on page 56
- "Connection Pool JNDI Name" on page 56
- "JDBC Driver" on page 56
- "JDBC URL" on page 56
- "Connect This User to Database" on page 56
- "Password for Connecting to Database" on page 56
- "Password for Connecting to Database Confirm" on page 56
- "Password Column String" on page 56
- "Prepared Statement" on page 57
- "Class to Transform Password Syntax" on page 57
- "Authentication Level" on page 57

Connection Type

Specifies the connection type to the SQL database, using either a JNDI (Java Naming and Directory Interface) connection pool or JDBC driver. The options are:

- Connection pool is retrieved via JDNI
- Non-persistent JDBC connection

The JNDI connection pool utilizes the configuration from the underlying web container.

Connection Pool JNDI Name

If JNDI is selected in Connection Type, this field specifies the connection pool name. Because JDBC authentication uses the JNDI connection pool provided by the web container, the setup of JNDI connection pool may not be consistent among other web containers. See the Access Manager Administration Guide for examples

JDBC Driver

If JDBC is selected in "Connection Type" on page 56, this field specifies the JDBC driver provided by the SQL database. For example, `com.mysql.jdbc.Driver`.

JDBC URL

Specifies the database URL if JDBC is select in "Connection Type" on page 56. For example, the URL for mySQL is `jdbc.mysql://hostname:port/databaseName`.

Connect This User to Database

Specifies the user name from whom the database connection is made for the JDBC connection.

Password for Connecting to Database

Defines the password for the user specified in User to Connect to Database.

Password for Connecting to Database Confirm

Confirm the password.

Password Column String

Specifies the password column name in the SQL database.

Prepared Statement

Specifies the SQL statement that retrieves the password of the user that is logging in. For example:

```
select Password from Employees where USERNAME = ?
```

Class to Transform Password Syntax

Specifies the class name that transforms the password retrieved from the database, to the format of the user input, for password comparison. This class must implement the `JDBCPasswordSyntaxTransform` interface.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

▼ To Configure a Connection Pool — Example

The following example shows how to set up a connection pool for Web Server and MySQL 4.0:

1. **In the Web Server console, create a JDBC connection pool with the following attributes:**

poolName	`samplePool`
DataSource Classname	`com.mysql.jdbc.jdbc2.optional.MysqlDatacSource`
serverName	Server name of the mySQL server.
port	Port number on which mySQL server is running.
user	User name of the database password.
password	The password of the user.
databaseName	The name of the database.

Note – The jar file which contain the DataSource class and the JDBC Driver class mentioned in the following steps should be added to the application class path

---

2 **Configure the JDBC Resources. In the Web Server console, create a JDBC resource with the following attributes:**

JNDI name	*jdbc/samplePool*
Pool name	*samplePool*
Data Resource Enabled	*on*

3 **Add the following lines to the `sun-web.xml` file of the application:**

```
<resource-ref>
      <res-ref-name>jdbc/mySQL</res-ref-name>
      <jndi-name>jdbc/samplePool</jndi-name>
</resource-ref>
```

4 **Add the following lines to the web.xml file of the application:**

```
<resource-ref>
       <description>mySQL Database</description>
       <res-ref-name>jdbc/mySQL</res-ref-name>
       <res-type>javax.sql.DataSource</res-type>
       <res-auth>Container</res-auth>
</resource-ref>
```

5 **Once you have completed the settings the value for this attribute is becomes** *java:comp/env/jdbc/mySQL***.**

LDAP

This module enables authentication using LDAP bind, a Directory Server operation which associates a user ID password with a particular LDAP entry. You can define multiple LDAP authentication configurations for a realm. The LDAP authentication attributes are realm attributes. The attributes are:

- "Primary LDAP Server" on page 59
- "Secondary LDAP Server" on page 59
- "DN to Start User Search" on page 59
- "DN for Root User Bind" on page 60
- "Password for Root User Bind" on page 60
- "Password for Root User Bind (confirm)" on page 60
- "Attribute Used to Retrieve User Profile" on page 60
- "Attributes Used to Search for a User to be Authenticated" on page 60

- "User Search Filter" on page 61
- "Search Scope" on page 61
- "Enable SSL to Access LDAP Server" on page 61
- "Return User DN to Authenticate" on page 61
- "LDAP Server Check Interval" on page 61
- "User Creation Attribute List" on page 62
- "Authentication Level" on page 62

Primary LDAP Server

Specifies the host name and port number of the primary LDAP server specified during Access Manager installation. This is the first server contacted for authentication. The format is*hostname:port*. If there is no port number, assume `389`.

If you have Access Manager deployed with multiple domains, you can specify the communication link between specific instances of Access Manager and Directory Server in the following format (multiple entries must be prefixed by the local server name):

```
local_servername|server:port local_servername2|server2:port2 ...
```

For example, if you have two Access Manager instances deployed in different locations (L1-machine1-IS and L2- machine2-IS) communicating with different instances of Directory Server (L1-machine1-DS and L2-machine2-DS), it would look the following:

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389

L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

Secondary LDAP Server

Specifies the host name and port number of a secondary LDAP server available to the Access Manager platform. If the primary LDAP server does not respond to a request for authentication, this server would then be contacted. If the primary server is up, Access Manager will switch back to the primary server. The format is also *hostname:port*. Multiple entries must be prefixed by the local server name.

Caution – When authenticating users from a Directory Server that is remote from the Access Manager enterprise, it is important that both the Primary and Secondary LDAP Server Ports have values. The value for one Directory Server location can be used for both fields.

DN to Start User Search

Specifies the DN of the node where the search for a user would start. (For performance reasons, this DN should be as specific as possible.) The default value is the root of the directory tree. Any

valid DN will be recognized. If OBJECT is selected in the Search Scope attribute, the DN should specify one level above the level in which the profile exists. Multiple entries must be prefixed by the local server name. The format is *servername*|*search dn*.

For multiple entries:

servername1|*search dn servername2*|*search dn servername3*|*search dn* . . .

If multiple entries exist under the root organization with the same user ID, then this parameter should be set so that the only one entry can be searched for or found in order to be authenticated. For example, in the case where the agent ID and user ID is same under root org, this parameter should be `ou=Agents` for the root organization to authenticate using Agent ID and `ou=People,` for the root organization to authenticate using User ID.

DN for Root User Bind

Specifies the DN of the user that will be used to bind to the Directory Server specified in the Primary LDAP Server and Port field as administrator. The authentication service needs to bind as this DN in order to search for a matching user DN based on the user login ID. The default is `amldapuser.` Any valid DN will be recognized.

Password for Root User Bind

Carries the password for the administrator profile specified in the DN for Root User Bind field. There is no default value. Only the administrator's valid LDAP password will be recognized.

Password for Root User Bind (confirm)

Confirm the password.

Attribute Used to Retrieve User Profile

Specifies the attribute used for the naming convention of user entries. By default, Access Manager assumes that user entries are identified by the uid attribute. If your Directory Server uses a different attribute (such as *givenname*) specify the attribute name in this field.

Attributes Used to Search for a User to be Authenticated

Lists the attributes to be used to form the search filter for a user that is to be authenticated, and allows the user to authenticate with more than one attribute in the user's entry. For example, if this field is set to *uid*, *employeenumber* , and *mail*, the user could authenticate with any of these names.

User Search Filter

Specifies an attribute to be used to find the user under the DN to Start User Search field. It works with the User Naming Attribute. There is no default value. Any valid user entry attribute will be recognized.

Search Scope

Indicates the number of levels in the Directory Server that will be searched for a matching user profile. The search begins from the node specified in the "DN to Start User Search" on page 59 attribute. The default value is SUBTREE. One of the following choices can be selected from the list:

OBJECT	Searches only the specified node.
ONELEVEL	Searches at the level of the specified node and one level down.
SUBTREE	Search all entries at and below the specified node.

Enable SSL to Access LDAP Server

Enables SSL access to the Directory Server specified in the Primary and Secondary LDAP Server and Port field. By default, the box is not checked and the SSL protocol will not be used to access the Directory Server.

If the LDAP Server is running with SSL enabled (LDAPS), you must make sure that Access Manager is configured with proper SSL trusted certificates so that AM could connect to Directory server over LDAPS protocol

Return User DN to Authenticate

When the Access Manager directory is the same as the directory configured for LDAP, this option may be enabled. If enabled, this option allows the LDAP authentication module to return the DN instead of the User ID, and no search is necessary. Normally, an authentication module returns only the User ID, and the authentication service searches for the user in the local Access Manager LDAP. If an external LDAP directory is used, this option is typically not enabled.

LDAP Server Check Interval

This attribute is used for LDAP Server failback. It defines the number of minutes in which a thread will "sleep" before verifying that the LDAP primary server is running.

User Creation Attribute List

This attribute is used by the LDAP authentication module when the LDAP server is configured as an external LDAP server. It contains a mapping of attributes between a local and an external Directory Server. This attribute has the following format:

attr1|*externalattr1*

attr2|*externalattr2*

When this attribute is populated, the values of the external attributes are read from the external Directory Server and are set for the internal Directory Server attributes. The values of the external attributes are set in the internal attributes only when the `User Profile`attribute (in the Core Authentication module) is set to Dynamically Created and the user does not exist in local Directory Server instance. The newly created user will contain the values for internal attributes, as specified in User Creation Attributes List, with the external attribute values to which they map.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

Membership

The Membership Authentication module is implemented for personalized sites. When membership authentication is enabled, a user can self-register. This means the user can create an account, personalize it, and access it as a registered user without the help of an administrator. The attributes are realm attributes. The attributes are:

- "Minimum Password Length" on page 63
- "Default User Roles" on page 63
- "User Status After Registration" on page 63
- "Primary LDAP Server" on page 63
- "Secondary LDAP Server" on page 64

- "DN to Start User Search" on page 64
- "DN for Root User Bind" on page 65
- "Password for Root User Bind" on page 65
- "Password for Root User Bind (confirm)" on page 65
- "Attribute Used to Retrieve User Profile" on page 65
- "Attributes Used to Search for a User to be Authenticated" on page 65
- "User Search Filter" on page 65
- "Search Scope" on page 65
- "Enable SSL to Access LDAP Server" on page 66
- "Return User DN to Authenticate" on page 66
- "Authentication Level" on page 66

Minimum Password Length

Specifies the minimum number of characters required for a password set during self-registration. The default value is 8.

If this value is changed, it should also be changed in the registration and error text in the following file:

AcessManager-base/`locale/amAuthMembership.properties` (*PasswdMinChars* entry)

Default User Roles

Specifies the roles assigned to new users whose profiles are created through self-registration. There is no default value. The administrator must specify the DNs of the roles that will be assigned to the new user.

Note – The role specified must be under the realm for which authentication is being configured. Only the roles that can be assigned to the user will be added during self-registration. All other DNs will be ignored. The role can be either an Access Manager role or an LDAP role, but filtered roles are not accepted.

User Status After Registration

Specifies whether services are immediately made available to a user who has self-registered. The default value is Active and services are available to the new user. By selecting Inactive, the administrator chooses to make no services available to a new user.

Primary LDAP Server

Specifies the host name and port number of the primary LDAP server specified during Access Manager installation. This is the first server contacted for authentication. The format is*hostname:port*. If there is no port number, assume `389`.

If you have Access Manager deployed with multiple domains, you can specify the communication link between specific instances of Access Manager and Directory Server in the following format (multiple entries must be prefixed by the local server name):

```
local_servername|server:port local_servername2|server2:port2 ...
```

For example, if you have two Access Manager instances deployed in different locations (L1-machine1-IS and L2- machine2-IS) communicating with different instances of Directory Server (L1-machine1-DS and L2-machine2-DS), it would look the following:

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389

L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

Secondary LDAP Server

Specifies the host name and port number of a secondary LDAP server available to the Access Manager platform. If the primary LDAP server does not respond to a request for authentication, this server would then be contacted. If the primary server is up, Access Manager will switch back to the primary server. The format is also *hostname:port*. Multiple entries must be prefixed by the local server name.

Caution – When authenticating users from a Directory Server that is remote from the Access Manager enterprise, it is important that both the Primary and Secondary LDAP Server Ports have values. The value for one Directory Server location can be used for both fields.

DN to Start User Search

Specifies the DN of the node where the search for a user would start. (For performance reasons, this DN should be as specific as possible.) The default value is the root of the directory tree. Any valid DN will be recognized. If OBJECT is selected in the Search Scope attribute, the DN should specify one level above the level in which the profile exists. Multiple entries must be prefixed by the local server name. The format is *servername*|*search dn*.

For multiple entries:

servername1|*search dn servername2*|*search dn servername3*|*search dn* . . .

If multiple entries exist under the root organization with the same user ID, then this parameter should be set so that the only one entry can be searched for or found in order to be authenticated. For example, in the case where the agent ID and user ID is same under root org, this parameter should be `ou=Agents` for the root organization to authenticate using Agent ID and `ou=People,` for the root organization to authenticate using User ID.

DN for Root User Bind

Specifies the DN of the user that will be used to bind to the Directory Server specified in the Primary LDAP Server and Port field as administrator. The authentication service needs to bind as this DN in order to search for a matching user DN based on the user login ID. The default is `amldapuser.` Any valid DN will be recognized.

Password for Root User Bind

Carries the password for the administrator profile specified in the DN for Root User Bind field. There is no default value. Only the administrator's valid LDAP password will be recognized.

Password for Root User Bind (confirm)

Confirmation of the password.

Attribute Used to Retrieve User Profile

Specifies the attribute used for the naming convention of user entries. By default, Access Manager assumes that user entries are identified by the uid attribute. If your Directory Server uses a different attribute (such as *givenname*) specify the attribute name in this field.

Attributes Used to Search for a User to be Authenticated

Lists the attributes to be used to form the search filter for a user that is to be authenticated, and allows the user to authenticate with more than one attribute in the user's entry. For example, if this field is set to *uid*, *employeenumber* , and *mail*, the user could authenticate with any of these names.

User Search Filter

Specifies an attribute to be used to find the user under the DN to Start User Search field. It works with the User Naming Attribute. There is no default value. Any valid user entry attribute will be recognized.

Search Scope

Indicates the number of levels in the Directory Server that will be searched for a matching user profile. The search begins from the node specified in the attribute "DN to Start User Search" on page 315. The default value is SUBTREE. One of the following choices can be selected from the list:

OBJECT	Searches only the specified node.
ONELEVEL	Searches at the level of the specified node and one level down.

SUBTREE Search all entries at and below the specified node.

Enable SSL to Access LDAP Server

Enables SSL access to the Directory Server specified in the Primary and Secondary LDAP Server and Port field. By default, the box is not checked and the SSL protocol will not be used to access the Directory Server.

If the LDAP Server is running with SSL enabled (LDAPS), you must make sure that Access Manager is configured with proper SSL trusted certificates so that AM could connect to Directory server over LDAPS protocol

Return User DN to Authenticate

When the Access Manager directory is the same as the directory configured for LDAP, this option may be enabled. If enabled, this option allows the LDAP authentication module to return the DN instead of the User ID, and no search is necessary. Normally, an authentication module returns only the User ID, and the authentication service searches for the user in the local Access Manager LDAP. If an external LDAP directory is used, this option is typically not enabled.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

MSISDN

The Mobile Station Integrated Services Digital Network (MSISDN) authentication module enables authentication using a mobile subscriber ISDN associated with a device such as a cellular telephone. It is a non-interactive module. The module retrieves the subscriber ISDN and validates it against the Directory Server to find a user that matches the number. The MSISDN Authentication attributes are realm attributes. The MSISDN Authentication attributes are:

- "Trusted Gateway IP Address" on page 67
- "MSISDN Number Argument" on page 67
- "LDAP Server and Port" on page 67
- "LDAP Start Search DN" on page 68
- "Attribute To Use To Search LDAP" on page 68
- "LDAP Server Principal User" on page 68
- "LDAP Server Principal Password" on page 68
- "LDAP Server Principal Password (confirm)" on page 68
- "Enable SSL for LDAP Access" on page 68
- "LDAP Attribute Used to Retrieve User Profile" on page 69
- "Return User DN on Authentication" on page 69
- "Authentication Level" on page 69

Trusted Gateway IP Address

Specifies a list of IP addresses of trusted clients that can access MSIDSN modules. You can set the IP addresses of all clients allows to access the MSISDN module by entering the address (for example, `123.456.123.111`) in the entry field and clicking Add. By default, the list is empty. If the attribute is left empty, then all clients are allowed. If you specify none, no clients are allowed.

MSISDN Number Argument

Specifies a list of parameter names that identify which parameters to search in the request header or cookie header for the MSISDN number. For example, if you define *x-Cookie-Param*, *AM_NUMBER*, and *COOKIE-ID*, the MSISDN authentication services will search those parameters for the MSISDN number.

LDAP Server and Port

Specifies the host name and port number of the Directory Server in which the search will occur for the users with MSISDN numbers. The format is*hostname:port*. If there is no port number, assume `389`.

If you have Access Manager deployed with multiple domains, you can specify the communication link between specific instances of Access Manager and Directory Server in the following format (multiple entries must be prefixed by the local server name):

```
local_servername|server:port local_servername2|server2:port2 ...
```

For example, if you have two Access Manager instances deployed in different locations (L1-machine1-IS and L2- machine2-IS) communicating with different instances of Directory Server (L1-machine1-DS and L2-machine2-DS), it would look the following:

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389
```

```
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

LDAP Start Search DN

Specifies the DN of the node where the search for the user's MSISDN number should start. There is no default value. The field will recognize any valid DN. Multiple entries must be prefixed by the local server name. The format is *servername|search dn*.

For multiple entries:

servername1|search dn servername2|search dn servername3|search dn . . .

If multiple entries exist under the root organization with the same user ID, then this parameter should be set so that the only one entry can be searched for or found in order to be authenticated. For example, in the case where the agent ID and user ID is same under root org, this parameter should be `ou=Agents` for the root organization to authenticate using Agent ID and `ou=People,` for the root organization to authenticate using User ID.

Attribute To Use To Search LDAP

Specifies the name of the attribute in the user's profile that contains the MSISDN number to search for a particular user. The default value is *sunIdentityMSISDNNumber*. This value should not be changed, unless you are certain that another attribute in the user's profile contains the same MSISDN number.

LDAP Server Principal User

Specifies the LDAP bind DN to allow MSISDN searches in the Directory Server. The default bind DN is `cn=amldapuser,ou=DSAME Users,dc=sun,dc=com .`

LDAP Server Principal Password

Specifies the LDAP bind password for the bind DN, as defined in LDAP Server Principal User.

LDAP Server Principal Password (confirm)

Confirm the password.

Enable SSL for LDAP Access

Enables SSL access to the Directory Server specified in the LDAP Server and Port attribute. By default, this is not enabled and the SSL protocol will not be used to access the Directory Server. However, if this attribute is enabled, you can bind to a non-SSL server.

LDAP Attribute Used to Retrieve User Profile

Specifies the headers to use for searching the request for the MSISDN number. The supported values are as follows:

Cookie Header	Performs the search in the cookie.
RequestHeader	Performs the search in the request header.
RequestParameter	Performs the search in the request parameter. By default, all options are selected.

Return User DN on Authentication

When the Access Manager directory is the same as the directory configured for MSDISN, this option may be enabled. If enabled, this option allows the authentication module to return the DN instead of the User ID, and no search is necessary. Normally, an authentication module returns only the User ID, and the authentication service searches for the user in the local Access Manager. If an external directory is used, this option is typically not enabled.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

RADIUS

This module allows for authentication using an external Remote Authentication Dial-In User Service (RADIUS) server. The RADIUS Authentication attributes are realm attributes. The attributes are:

- "Server 1" on page 70
- "Server 2" on page 70
- "Shared Secret" on page 70
- "Shared Secret Confirm" on page 70
- "Port Number" on page 70

- "Timeout" on page 70
- "Authentication Level" on page 70

Server 1

Displays the IP address or fully qualified host name of the primary RADIUS server. The default IP address is 127.0.0.1. The field will recognize any valid IP address or host name. Multiple entries must be prefixed by the local server name as in the following syntax:

```
local_servername|ip_address local_servername2|ip_address ...
```

Server 2

Displays the IP address or fully qualified domain name (FQDN) of the secondary RADIUS server. It is a failover server which will be contacted if the primary server could not be contacted. The default IP address is 127.0.0.1. Multiple entries must be prefixed by the local server name as in the following syntax:

```
local_servername|ip_address local_servername2|ip_address ...
```

Shared Secret

Carries the shared secret for RADIUS authentication. The shared secret should have the same qualifications as a well-chosen password. There is no default value for this field.

Shared Secret Confirm

Confirmation of the shared secret for RADIUS authentication.

Port Number

Specifies the port on which the RADIUS server is listening. The default value is 1645.

Timeout

Specifies the time interval in seconds to wait for the RADIUS server to respond before a timeout. The default value is 3 seconds. It will recognize any number specifying the timeout in seconds.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is

sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

SafeWord

This module allows for users to authenticate using Secure Computing's SafeWord or SafeWord PremierAccess authentication servers. The SafeWord Authentication Attributes are realm attributes. The attributes are:

- "Server" on page 71
- "Server Verification Files Directory" on page 71
- "Logging Enable" on page 71
- "Logging Level" on page 72
- "Log File" on page 72
- "Authentication Connection Timeout" on page 72
- "Client Type" on page 72
- "EASSP Version" on page 72
- "Minimum Authenticator Strength" on page 72
- "Authentication Level" on page 72

Server

Specifies the SafeWord or SafeWord PremiereAccess server name and port. Port 7482 is set as the default for a SafeWord server. The default port number for a SafeWord PremierAccess server is 5030.

Server Verification Files Directory

Specifies the directory into which the SafeWord client library places its verification files. The default is as follows:

```
/var/opt/SUNWam/auth/safeword/serverVerification
```

If a different directory is specified in this field, the directory must exist before attempting SafeWord authentication.

Logging Enable

Enables SafeWord logging. By default, SafeWord logging is enabled.

Logging Level

Specifies the SafeWord logging level. Select a level in the Drop-down menu. The levels are DEBUG, ERROR, INFO and NONE .

Log File

Specifies the directory path and log file name for SafeWord client logging. The default path is`/var/opt/SUNWam/auth/safeword/safe.log`.

If a different path or filename is specified, it must exist before attempting SafeWord authentication. If more than one realm is configured for SafeWord authentication, and different SafeWord servers are used, then different paths must be specified or only the first realm where SafeWord authentication occurs will work. Likewise, if an realm changes SafeWord servers, the `swec.dat` file in the specified directory must be deleted before authentications to the newly configured SafeWord server will work.

Authentication Connection Timeout

Defines the timeout period (in seconds) between the SafeWord client (Access Manager) and the SafeWord server. The default is 120 seconds.

Client Type

Defines the Client Type that the SafeWord server uses to communicate with different clients, such as Mobile Client, VPN, Fixed Password, Challenge/Response, and so forth.

EASSP Version

This attribute specifies the Extended Authentication and Single Sign-on Protocol (EASSP) version. This field accepts either the standard (101), SSL-encrypted premier access (200), or premier access (201) protocol versions.

Minimum Authenticator Strength

Defines the minimum authenticator strength for the client/SafeWord server authentication. Each client type has a different authenticator value, and the higher the value, the higher the authenticator strength. 20 is the highest value possible. 0 is the lowest value possible.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is

sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

SAML

The Security Assertion Markup Language (SAML) authentication module receives and validates SAML Assertions on a target server. The SAML attribute is a realm attribute.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

SecurID

This module allows for authentication using RSA ACE/Server software and RSA SecurID authenticators. the SecurID authentication module is not available for the Linux or Solaris x86 platforms and this should not be registered, configured, or enabled on these two platforms. It is only available for Solaris. The SecurID authentication attributes are realm attributes. The attributes are:

- "ACE/Server Configuration Path" on page 74
- "Helper Configuration Port" on page 74
- "Helper Authentication Port" on page 74
- "Authentication Level" on page 74

ACE/Server Configuration Path

Specifies the directory in which the SecurID ACE/Server `sdconf.rec` file is located, by default in `/opt/ace/data` If you specify a different directory in this field, the directory must exist before attempting SecurID authentication.

Helper Configuration Port

Specifies the port on which the SecurID helper 'listens' upon startup for the configuration information contained in the SecurID Helper Authentication Port attribute. The default is 58943.

If this attribute is changed, you must also change the *securidHelper.ports* entry in the `AMConfig.properties` file, and restart Access Manager. The entry in the `AMConfig.properties` file is a space-separated list of the ports for the instances of SecurID helpers. For each realm that communicates with a different ACE/Server (which has a different `sdconf.rec` file), there must be a separate SecurID helper.

Helper Authentication Port

Specifies the port that the realm's SecurID authentication module will configure its SecurID helper instance to 'listen' for authentication requests. This port number must be unique across all realms using SecurID or UNIX authentication. The default port is 57943.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

UNIX

This Solaris only module allows for authentication using a user's UNIX identification and password. If any of the UNIX authentication attributes are modified, both Access Manager and the amunixd helper must be restarted. The UNIX authentication attributes are global and realm attributes. The attributes are:

- "Configuration Port" on page 75
- "Authentication Port" on page 75
- "Timeout" on page 75
- "Threads" on page 75
- "Authentication Level" on page 75
- "PAM Service Name" on page 76

Configuration Port

This attribute specifies the port to which the UNIX Helper 'listens' upon startup for the configuration information contained in the UNIX Helper Authentication Port, UNIX Helper Timeout, and UNIX Helper Threads attributes. The default is 58946.

If this attribute is changed, you must also change the *unixHelper.port* entry in the `AMConfig.properties` file, and restart Access Manager.

Authentication Port

This attribute specifies the port to which the UNIX Helper 'listens' for authentication requests after configuration. The default port is 57946.

Timeout

This attribute specifies the number of minutes that users have to complete authentication. If users surpass the allotted time, authentication automatically fails. The default time is set to 3 minutes.

Threads

This attribute specifies the maximum number of permitted simultaneous UNIX authentication sessions. If the maximum is reached at a given moment, subsequent authentication attempts are not allowed until a session is freed up. The default is set to 5.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

PAM Service Name

Defines the PAM (Pluggable Authentication Module) configuration or stack that is shipped for you operating system and is used for UNIX authentication. For Solaris, the name is usually `other` and for Linux, the name is `password`.

Windows Desktop SSO

This module is specific to Windows and is also known as Kerberos authentication. The user presents a Kerberos token to Access Manager through the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) protocol. The Windows Desktop SSO authentication plug-in module provides a client (user) with desktop single sign-on. This means that a user who has already authenticated with a key distribution center can be authenticated with Access Manager without having to provide the login information again. The Windows Desktop SSO attributes are global attributes. The attributes are:

- "Service Principal" on page 76
- "Keytab File Name" on page 76
- "Kerberos Realm" on page 77
- "Kerberos Server Name" on page 77
- "Return Principal with Domain Name" on page 77
- "Authentication Level" on page 77

Service Principal

Specifies the Kerberos principal that is used for authentication. Use the following format:

`HTTP/`*hostname.domainname@dc_domain_name*

hostname and *domainame* represent the hostname and domain name of the Access Manager instance. *dc_domain_name* is the Kerberos domain in which the Windows 2000 Kerberos server (domain controller) resides. It is possibly different from the domain name of the Access Manager.

Keytab File Name

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

*hostname***`.HTTP.keytab`**

hostname is the hostname of the Access Manager instance.

Kerberos Realm

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

Kerberos Server Name

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

Return Principal with Domain Name

If enabled, this attributes allows Access Manager to automatically return the Kerberos principal with the domain controller's domain name during authentication.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

Windows NT

The Windows NT Authentication module allows for authentication against a Microsoft Windows NT server. The attributes are realm attributes. The values applied to them under Service Configuration become the default values for the Windows NT Authentication template. The service template needs to be created after registering the service for the realm. The default values can be changed after registration by the realm's administrator. realm attributes are not inherited by entries in the subtrees of the realm.

In order to activate the Widows NT Authentication module, Samba Client 2.2.2 must be downloaded and installed to the following directory:

AcessManager-base/`SUNWam/bin`

The Samba Client is a file and print server for blending Windows and UNIX machines without requiring a separate Windows NT/2000 Server.

Red Hat Linux ships with a Samba client, located in the`/usr/bin` directory.

In order to authenticate using the Windows NT Authentication service for Linux, copy the client binary to*AccessManager-base* `/identity/bin`.

The Windows NT attributes are:

- "Authentication Domain" on page 78
- "Authentication Host" on page 78
- "Samba Configuration File Name" on page 78
- "Authentication Level" on page 78

Authentication Domain

Defines the Domain name to which the user belongs.

Authentication Host

Defines the Windows NT authentication hostname. The hostname should be the netBIOS name, as opposed to the fully qualified domain name (FQDN). By default, the first part of the FQDN is the netBIOS name.

If the DHCP (Dynamic Host Configuration Protocol) is used, you would put a suitable entry in the HOSTS file on the Windows 2000 machine.

Name resolution will be performed based on the netBIOS name. If you do not have any server on your subnet supplying netBIOS name resolution, the mappings should be hardcoded. For example, the hostname should be `example1` not `example1.company1.com`.

Samba Configuration File Name

Defines the Samba configuration filename and supports the `-s` option in the `smbclient` command. The value must be the full directory path where the Samba configuration file is located. For example: `/etc/opt/SUNWam/config/smb.conf`

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication mechanism. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is

sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is 0.

Note – If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute "Default Authentication Level" on page 54.

Supported Language Locales

The following table lists the language locales that Access Manager supports:

Language Tag	Language
af	Afrikaans
be	Byelorussian
bg	Bulgarian
ca	Catalan
cs	Czechoslovakian
da	Danish
de	German
el	Greek
en	English
es	Spanish
eu	Basque
fi	Finnish
fo	Faroese
fr	French
ga	Irish
gl	Galician
hr	Croatian
hu	Hungarian
id	Indonesian

is	Icelandic
it	Italian
ja	Japanese
ko	Korean
nl	Dutch
no	Norwegian
pl	Polish
pt	Portuguese
ro	Romanian
ru	Russian
sk	Slovakian
sl	Slovenian
sq	Albanian
sr	Serbian
sv	Swedish
tr	Turkish
uk	Ukrainian
zh	Chinese

Console Properties

The Console properties contain services that enable you to configure the Access Manager console and to define console properties for different locales and character sets. The Console properties contain the following:

- "Administration" on page 80
- "Globalization Settings" on page 93

Administration

The Administration service enables you to configure the Access Manager console at both the application level as well as at a configured realm level (Preferences or Options specific to a configured realm). The Administration service attributes are global and realm attributes. The attributes are:

- "Federation Management" on page 82
- "User Management" on page 82
- "People Containers" on page 82
- "Organizational Unit Containers" on page 82
- "Group Containers" on page 82
- "Managed Group Type" on page 82
- "Default Role Permissions" on page 83
- "Domain Component Tree" on page 83
- "Administrative Groups" on page 84
- "Compliance User Deletion" on page 84
- "Dynamic Administrative Roles ACIs" on page 84
- "User Profile Service Classes" on page 86
- "DC Node Attribute List" on page 86
- "Search Filters for Deleted Objects" on page 86
- "Default People Container" on page 86
- "Default Groups Container" on page 86
- "Default Agents Container" on page 87
- "Groups Default People Container" on page 87
- "Groups People Container List" on page 87
- "User Profile Display Class" on page 87
- "End User Profile Display Class" on page 87
- "Show Roles on User Profile Page" on page 87
- "Show Groups on User Profile Page" on page 88
- "User Self Subscription to Group" on page 88
- "User Profile Display Options" on page 88
- "User Creation Default Roles" on page 88
- "Administrative Console Tabs" on page 88
- "Maximum Results Returned From Search" on page 88
- "Timeout For Search" on page 89
- "JSP Directory Name" on page 90
- "Online Help Documents" on page 90
- "Required Services" on page 90
- "User Search Key" on page 90
- "User Search Return Attribute" on page 90
- "User Creation Notification List" on page 91
- "User Deletion Notification List" on page 91
- "User Modification Notification List" on page 91
- "Maximum Entries Displayed per Page" on page 92
- "Event Listener Classes" on page 92
- "Pre and Post Processing Classes" on page 92
- "External Attributes Fetch" on page 93
- "Invalid User ID Characters" on page 93
- "UserID and Password Validation Plug-in Class" on page 93

Federation Management

Enables Federation Management. It is selected by default. To disable this feature, deselect the field The Federation Management tab will not appear in the console.

User Management

Enables User Management. This is enabled by default. This attribute is applicable when Access Manager is installed in legacy mode.

People Containers

This attribute is deselected by default and is applicable only when Access Manager is installed in legacy mode. Selecting this attribute will display people containers under the Directory Management tab. It is recommended that you use a single people container in your DIT and then use roles to manage accounts and services. The default behavior of the Access Manager console is to hide the People Containers. However, if you have multiple people containers in your DIT, select this attribute to display People Containers as managed objects.

Organizational Unit Containers

This attribute is deselected by default and is applicable when Access Manager is installed in legacy mode. Selecting this attribute will display containers in the Directory Management tab.

Group Containers

This attribute is deselected by default and is applicable when Access Manager is installed in legacy mode. Selecting this attribute will display group containers in the Directory Management tab.

Managed Group Type

Specifies whether subscription groups created through the console are static or dynamic. The console will either create and display subscription groups that are static or dynamic, not both. (Filtered groups are always supported regardless of the value given to this attribute.) The default value is dynamic.

- A static group explicitly lists each group member using the `groupOfNames` or `groupOfUniqueNames` object class. The group entry contains the *uniqueMember* attribute for each member of the group. Members of static groups are manually added; the user entry itself remains unchanged. Static groups are suitable for groups with few members.
- A dynamic group uses a `memberOf` attribute in the entry of each group member. Members of dynamic groups are generated through the use of an LDAP filter which searches and returns all entries which contain the `memberOf` attribute. Dynamic groups are suitable for groups that have a very large membership.

- A filtered group uses an LDAP filter to search and return members that meet the requirement of the filter. For instance, the filter can generate members with a specific uid (`uid=g*`) or email address (`mail=*@example.com`).

In the examples above, the LDAP filter would return all users whose uid begins with `g` or whose email address ends with `example.com`, respectively. Filtered groups can only be created within the User Management view by choosing Membership by Filter.

An administrator can select one of the following:

- Dynamic - Groups created through the Membership By Subscription option will be dynamic.
- Static - Groups created through the Membership By Subscription option will be static.

Default Role Permissions

Defines a list of default access control instructions (ACIs) or *permissions* that are used to grant administrator privileges when creating new roles. Select one of these ACIs for the level of privilege you wish. Access Manager ships with four default role permissions:

No Permissions — No permissions are to be set on the role.

Organization Admin — The Organization Administrator has read and write access to all entries in the configured organization.

Organization Help Desk Admin — The Organization Help Desk Administrator has read access to all entries in the configured organization and write access to the `userPassword` attribute.

Organization Policy Admin — The Organization Policy Administrator has read and write access to all policies in the realm. The Organization Policy Administrator can not create a referral policy.

Domain Component Tree

The Domain Component tree (DC tree) is a specific DIT structure used by many Sun Java System components to map between DNS names and realm entries.

When this option is enabled, the DC tree entry for an realm is created, provided that the DNS name of the realm is entered at the time the realm is created. The DNS name field will appear in the realm Create page. This option is only applicable to top-level realms, and will not be displayed for subrealms.

Any status change made to the *inetdomainstatus* attribute through the Access Manager SDK in the realm tree will update the corresponding DC tree entry status. (Updates to status that are not made through the Access Manager SDK will not be synchronized.) For example, if a new realm, sun, is created with the DNS name attribute `sun.com`, the following entry will be created in the DC tree:

```
dc=sun,dc=com,o=internet,root suffix
```

The DC tree may optionally have its own root suffix configured by setting `com.iplanet.am.domaincomponent` in `AMConfig.properties`. By default, this is set to the Access Manager root. If a different suffix is desired, this suffix must be created using LDAP commands. The ACIs for administrators that create realms required modification so that they have unrestricted access to the new DC tree root.

Administrative Groups

Specifies whether to create the DomainAdministrators and DomainHelpDeskAdministrators groups. If enabled, these groups are created and associated with the Organization Admin Role and Organization Help Desk Admin Role, respectively. Once created, adding or removing a user to one of these associated roles automatically adds or removes the user from the corresponding group. This behavior, however, does not work in reverse. Adding or removing a user to one of these groups will not add or remove the user in the user's associated roles.

The DomainAdministrators and DomainHelpDeskAdministrators groups are only created in realms that are created after this option is enabled.

Note – This option does not apply to subrealms, with the exception of the root realm. At the root realm, the ServiceAdministrators and ServiceHelpDesk Administrators groups are created and associated with the Top-level Admin and Top-level Help Desk Admin roles, respectively. The same behavior applies.

Compliance User Deletion

Specifies whether a user's entry will be deleted, or just marked as deleted, from the directory. This attribute is only applicable when Access Manager is installed in legacy mode.

When a user's entry is deleted and this option is selected (true), the user's entry will still exist in the directory, but will be marked as deleted. User entries that are marked for deletion are not returned during Directory Server searches. If this option is not selected, the user's entry will be deleted from the directory.

Dynamic Administrative Roles ACIs

This attribute defines the access control instructions for the administrator roles that are created dynamically when a group or realm is configured using Access Manager. These roles are used for granting administrative privileges for the specific grouping of entries created. The default ACIs can be modified only under this attribute listing.

Note – Administrators at the realm level have a wider scope of access than do group administrators. But, by default, when a user is added to a group administrator role, that user can change the password of anyone in the group. This would include any realm administrator who is a member of that group.

The Container Help Desk Admin role has read access to all entries in a realm and write access to the *userPassword* attribute in user entries only in this container unit.

The Realm Help Desk Admin has read access to all entries in a realm and write access to the *userPassword* attribute. When a sub—realm is created, remember that the administration roles are created in the sub-realm, not in the parent realm.

The Container Admin role has read and write access to all entries in an LDAP organizational unit. In Access Manager, the LDAP organizational unit is often referred to as a container.

The Organization Policy Administrator has read and write access to all policies, and can create, assign, modify, and delete all policies within that realm.

ThePeople Container Admin is by default, any user entry in an newly created realm is a member of that realm's People Container. The People Container Administrator has read and write access to all user entries in the realm's People Container. Keep in mind that this role DOES NOT have read and write access to the attributes that contain role and group DNs therefore, they cannot modify the attributes of, or remove a user from, a role or a group.

Other containers can be configured with Access Manager to hold user entries, group entries or even other containers. To apply an Administrator role to a container created after the realm has already been configured, the Container Admin Role or Container Help Desk Admin defaults would be used.

The Group Admin has read and write access to all members of a specific group, and can create new users, assign users to the groups they manage, and delete the users the that they have created. When a group is created, the Group Administrator role is automatically generated with the necessary privileges to manage the group. The role is not automatically assigned to a group member. It must be assigned by the group's creator, or anyone that has access to the Group Administrator Role.

The Top-level Admin has read and write access to all entries in the top-level realm. In other words, this Top-level Admin role has privileges for every configuration principal within the Access Manager application.

The Organization Administrator has read and write access to all entries in a realm. When a realm is created, the Organization Admin role is automatically generated with the necessary privileges to manage the realm.

User Profile Service Classes

Lists the services that will have a custom display in the User Profile page. The default display generated by the console may not be sufficient for some services. This attribute creates a custom display for any service, giving full control over what and how the service information is displayed. The syntax is as follows:

```
service name | relative url()
```

Services that are listed in this attribute will not display in the User Create pages. Any data configuration for a custom service display must be performed the User Profile pages.

DC Node Attribute List

Defines the set of attributes that will be set in the DC tree entry when an object is created. The default parameters are:

maildomainwelcomemessage
preferredmailhost
mailclientattachmentquota
mailroutingsmarthost
mailaccessproxyreplay
preferredlanguage
domainuidseparator
maildomainmsgquota
maildomainallowedserviceaccess
preferredmailmessagestore
maildomaindiskquota
maildomaindiskquota
objectclass=maildomain
mailroutinghosts

Search Filters for Deleted Objects

Defines the search filters for objects to be removed when User Compliance Deletion mode is enabled.

Default People Container

Specifies the default people container into which the user is created.

Default Groups Container

Specifies the default groups container into which the group is created.

Default Agents Container

Specifies the default agent container into which the agent is created. The default is `Agents`.

Groups Default People Container

Specifies the default People Container where users will be placed when they are created. There is no default value. A valid value is the DN of a people container. See the note under Groups People Container List attribute for the People Container fallback order.

Groups People Container List

Specifies a list of People Containers from which a Group Administrator can choose when creating a new user. This list can be used if there are multiple People Containers in the directory tree. (If no People Containers are specified in this list or in the Groups Default People Container field, users are created in the default Access Manager people container, `ou=people`.) There is no default value for this field.

The syntax for this attribute is:

dn of group | *dn of people container*

When a user is created, this attribute is checked for a container in which to place the entry. If the attribute is empty, the Groups Default People Container attribute is checked for a container. If the latter attribute is empty, the entry is created under `ou=people` .

This attribute is only applicable when Access Manager is installed in legacy mode. There is no default value.

User Profile Display Class

Specifies the Java class used by the Access Manager console when it displays the User Profile pages.

End User Profile Display Class

Specifies the Java class used by the Access Manager console when it displays the End User Profile pages.

Show Roles on User Profile Page

Specifies whether to display a list of roles assigned to a user as part of the user's User Profile page. If the parameter is not enabled (the default), the User Profile page shows the user's roles only for administrators.

Show Groups on User Profile Page

Specifies whether to display a list of groups assigned to a user as part of the user's User Profile page. If this parameter is not enabled (the default), the User Profile page shows the user's groups only for administrators.

User Self Subscription to Group

This parameter specifies whether users can add themselves to groups that are open to subscription. If the parameter is not enabled (the default), the user profile page allows the user's group membership to be modified only by an administrator. This parameter applies only when the Show Groups on User Profile Page option is selected.

User Profile Display Options

This menu specifies which service attributes will be displayed in the user profile page. An administrator can select from the following:

UserOnly	Display viewable User schema attributes for services assigned to the user. User service attribute values are viewable by the user when the attribute contains the keyword Display. See the Access Manager Developer's Guide for details.
Combined	Display viewable User and Dynamic schema attributes for services assigned to the user.

User Creation Default Roles

This listing defines roles that will be assigned to newly created users automatically. There is no default value. An administrator can input the DN of one or more roles.

This field only takes a full Distinguished Name address, not a role name. The roles can only be Access Manager roles, not LDAP (Directory Server) roles.

Administrative Console Tabs

This field lists the Java classes of modules that will be displayed at the top of the console. The syntax is `i18N key | java class name`.

The i18N key is used for the localized name of the entry in the console.

Maximum Results Returned From Search

This field defines the maximum number of results returned from a search. The default value is 200.

Do not set this attribute to a large value (greater than 1000) unless sufficient system resources are allocated.

Note – Access Manager is preconfigured to return a maximum size of 4000 search entries. This value can be changed through the console or by using `ldapmodify`. If you wish to change it using `ldapmodify`, create a `newConfig.xml`, with the following values (in this example, `nsSizeLimit`: -1 means unlimited):

```
dn: cn=puser,ou=DSAME Users,ORG_ROOT_SUFFIX
changetype: modify
replace:nsSizeLimit
nsSizeLimit: -1
```

Then, run `ldapmodify`. For example:

```
setenv LD_LIBRARY_PATH /opt/SUNWam/lib/:/opt/SUNWam/ldaplib/ldapsdk:/usr/lib/mps:/usr/sh
$LD_LIBRARY_PATH

./ldapmodify -D "cn=Directory Manager" -w "iplanet333" -c -a -h hostname.domain -p 389 -f  newCo
```

Modifications to this attribute done through `LDAPModify` will take precedence to those made through the Access Manager Console.

Timeout For Search

Defines the amount of time (in number of seconds) that a search will continue before timing out. It is used to stop potentially long searches. After the maximum search time is reached, the search terminates and returns an error. The default is 5 seconds.

Note – Directory Server is been preconfigured with a timeout value of 120 seconds. This value can be changed through the Directory Server console or by using `ldapmodify.` If you wish to change it using `ldapmodify`, create a `newConfig.xml`, with the following values (this example changes the timeout from 120 seconds to 3600 seconds):

```
dn: cn=config
changetype: modify
replace:nsslapd-timelimit
nsslapd-timelimit: 3600
```

Then, run `ldapmodify`. For example:

```
setenv LD_LIBRARY_PATH /opt/SUNWam/lib/:/opt/SUNWam/ldaplib/ldapsdk:/usr/lib/mps:/usr/sh
$LD_LIBRARY_PATH

./ldapmodify -D "cn=Directory Manager" -w "iplanet333" -c -a -h hostname.domain -p 389 -f  newCo
```

JSP Directory Name

Specifies the name of the directory that contains the JSP files for a realm. It allows administrator to have different appearance (customization) for different realm. The default value for this attribute is `console`. This attribute is applicable only when Access Manager is installed in legacy mode.

Online Help Documents

This field lists the online help links that will be created on the main Access Manager help page. This allows other applications to add their online help links in the Access Manager page. The format for this attribute is:

```
linki18nkey | html page to load | i18n properties file | remote server
```

The remote server attribute is an optional argument that allows you to specify the remote server on which the online help document is located. The default value is:

```
DSAME Help|/contents.html|amAdminModlueMsgs
```

This attribute is only applicable when Access Manager is installed in legacy mode.

Required Services

This field lists the services that are dynamically added to the users' entries when they are created. Administrators can choose which services are added at the time of creation. This attribute is not used by the console, but by the Access Manager SDK. Users that are dynamically created by the `amadmin` command line utility will be assigned the services listed in this attribute.

User Search Key

This attribute defines the attribute name that is to be searched upon when performing a simple search in the Navigation page. The default value for this attribute is `cn`.

For example, if you enter `j*` in the Name field in the Navigation frame, users whose names begins with "j" or "J" will be displayed.

User Search Return Attribute

This field defines the attribute name used when displaying the users returned from a simple search. The default of this attribute is uid cn. This will display the user ID and the user's full name.

The attribute name that is listed first is also used as the key for sorting the set of users that will be returned. To avoid performance degradation, use an attribute whose value is set in a user's entry.

User Creation Notification List

This field defines a list of email addresses that will be sent notification when a new user is created. Multiple email addresses can be specified, as in the following syntax:

```
e-mail|locale|charset

e-mail|locale|charset

e-mail|locale|charset
```

The notification list also accepts different locales by using the `-|locale` option.

See "Supported Language Locales" on page 79for a list of locales.

The sender email ID can be changed by modifying property 497 in `amProfile.properties`, which is located, by default, at *AccessManager-base*/`SUNWam/locale`.

User Deletion Notification List

This field defines a list of email addresses that will be sent notification when a user is deleted. Multiple email addresses can be specified, as in the following syntax:

```
e-mail|locale|charset

e-mail|locale|charset

e-mail|locale|charset
```

The notification list also accepts different locales by using the `-|locale` option.

See for a list of local"Supported Language Locales" on page 79.

The sender email ID can be changed by modifying property 497 in `amProfile.properties`, which is located, by default, at *AccessManager-base*/`SUNWam/locale`.

The default sender ID is `DSAME`.

User Modification Notification List

Defines a list of attributes and email addresses associated with the attribute. When a user modification occurs on an attribute defined in the list, the email address associated with the attribute will be sent notification. Each attribute can have a different set of addresses associated to it. Multiple email address can be specified, as in the following syntax:

`attrName` *e-mail*`|` *locale*`|`*charset* *e-mail* `|`*locale*`|`*charset* `.....`

`attrName` *e-mail*`|` *locale*`|`*charset* *e-mail* `|`*locale*`|`*charset* `.....`

The `-self` keyword may be used in place of one of the addresses. This sends mail to the user whose profile was modified. For example, assume the following:

```
manager someuser@sun.com|self|admin@sun.com
```

Mail will be sent to the address specified in the manager attribute, `someuser@sun.com`, `admin@sun`, the person who modified the user (self).

The notification list also accepts different locales by using the `-|locale` option. For example, to send the notification to an administrator in France:

`manager someuser@sun.com|self|admin@sun.com|fr` See"Supported Language Locales" on page 79 for a list of locales.

The attribute name is the same as it appears in the Directory Server schema, and not as the display name in the console.

Maximum Entries Displayed per Page

This attribute allows you to define the maximum rows that can be displayed per page. The default is 25. For example, if a user search returns 100 rows, there will be 4 pages with 25 rows displayed in each page.

Event Listener Classes

This attribute contains a list of listeners that receive creation, modification and deletion events from the Access Manager console.

Pre and Post Processing Classes

This field defines a list of implementation classes through plug-ins that extend the `com.iplanet.am.sdk.AMCallBack` class to receive callbacks during pre and post processing operations for users, realm, roles and groups. The operations are:

- create
- delete
- modify
- add users to roles/groups
- delete users from roles/groups

You must enter the full class name of the plug-in and then change the class path of your web container (from the Access Manager installation base) to include the full path to the location of the plug-in class

External Attributes Fetch

This option enables callbacks for plug-ins to retrieve external attributes (any external application-specific attribute). External attributes are not cached in the Access Manager SDK, so this attribute allows you enable attribute retrieval per realm level. By default, this option is not enabled

Invalid User ID Characters

This attribute defines a list of characters that are not allowed in a user's name. Each character must be separated by the | character. For example:

```
*|(|)|&|!
```

UserID and Password Validation Plug-in Class

This class provides a userID and password validation plug-in mechanism. The methods of this class need to be overridden by the implementation plug-in modules that validate the userID and/or password for the user. The implementation plug-in modules will be invoked whenever a userID or password value is being added or modified using the Access Manager console, the `amadmin` command line interface, or using the SDK.

The plug-ins that extend this class can be configured per realm. If a plug-in is not configured for an realm, then the plug-in configured at the global level will be used.

If the validation of the plug-in fails, the plug-in module can throw an exception to notify the application to indicate the error in the userID or password supplied by the user.

Globalization Settings

The Globalization Settings service contains global attributes that enable you to configure Access Manager for different locales and character sets. The attributes are:

- "Charsets Supported By Each Locale" on page 93
- "Charset Aliases" on page 94
- "Auto Generated Common Name Format" on page 94

Charsets Supported By Each Locale

This attribute lists the character sets supported for each locale, which indicates the mapping between locale and character set. The format is as follows:

To add a New Supported Charset, click Add and define the following parameters:

Locale	The new locale you wish to add. See"Supported Language Locales" on page 79 for more information.
Supported Charsets	Enter the supported charset for the specified locale. Charsets are delimited by a semicolon. For example, `charset=charset1;charset2;charset3;...;charsetn`

To edit any existing Supported Charset, click the name in the Supported Charset table. Click OK when you are finished.

Charset Aliases

This attribute lists the codeset names (which map to IANA names) that will be used to send the response. These codeset names do not need to match Java codeset names. Currently, there is a hash table to map Java character sets into IANA charsets and vice versa.

To add a New Charset Alias, click Add button and define the following parameters:

MIME name	The IANA mapping name. For example, `Shift_JIS`
Java Name	The Java character set to map to the IANA character set.

To edit any existing Charset Alias, click the name in the table. Click OK when you are finished.

Auto Generated Common Name Format

This display option allows you to define the way in which a name is automatically generated to accommodate name formats for different locales and character sets. The default syntax is as follows (please note that including commas and/or spaces in the definition will display in the name format):

```
en_us = {givenname} {initials} {sn}
```

For example, if you wanted to display a new name format for a user (User One) with a uid (11111) for the Chinese character set, define:

```
zh = {sn}{givenname}({uid})
```

The display is:

```
OneUser 11111
```

Global Properties

Global Properties contain services that enable to define password reset functionality and policy configuration for Access Manager. The services you can configure are:

- "Password Reset" on page 95
- "Policy Configuration" on page 98
- "Session" on page 104

Password Reset

Access Manager provides a Password Reset service to allow users to receive an email message containing a new password or to reset their password for access to a given service or application protected by Access Manager. The Password Reset attributes are realm attributes. The attributes are:

- "User Validation" on page 95
- "Secret Question" on page 96
- "Search Filter" on page 96
- "Base DN" on page 96
- "Bind DN" on page 96
- "Bind Password" on page 96
- "Password Reset Option" on page 96
- "Password Change Notification Option" on page 96
- "Password Reset" on page 96
- "Personal Question" on page 97
- "Maximum Number of Questions" on page 97
- "Force Change Password on Next Login" on page 97
- "Password Reset Failure Lockout" on page 97
- "Password Reset Failure Lockout Count" on page 97
- "Password Reset Failure Lockout Interval" on page 97
- "Email Address to Send Lockout Notification" on page 97
- "Warn User After N Failure" on page 97
- "Password Reset Failure Lockout Duration" on page 98
- "Password Reset Lockout Attribute Name" on page 98
- "Password Reset Lockout Attribute Value" on page 98

User Validation

This attribute specifies the value that is used to search for the user whose password is to be reset.

Secret Question

This field allows you to add a list of questions that the user can use to reset his/her password. To add a question, type it in the Secret Question filed and click Add. The selected questions will appear in the user's User Profile page. The user can then select a question for resetting the password. Users may create their own question if the Personal Question Enabled attribute is selected.

Search Filter

This attribute specifies the search filter to be used to find user entries.

Base DN

This attribute specifies the DN from which the user search will start. If no DN is specified, the search will start from the realm DN. You should not use `cn=directorymanager` as the base DN, due to proxy authentication conflicts.

Bind DN

This attribute value is used with Bind Password to reset the user password.

Bind Password

This attribute value is used with Bind DN to reset the user password.

Password Reset Option

This attribute determines the classname for resetting the password. The default classname is `com.sun.identity.password.RandomPasswordGenerator`. The password reset class can be customized through a plug-in. This class needs to be implemented by the `PasswordGenerator` interface.

Password Change Notification Option

This attribute determines the method for user notification of password resetting. The default classname is: `com.sun.identity.password.EmailPassword` The password notification class can be customized through a plug-in. This class needs to be implemented by the `NotifyPassword` interface. See the Access Manager Developer's Guide for more information.

Password Reset

Selecting this attribute will enable the password reset feature.

Personal Question

Selecting this attribute will allow a user to create a unique question for password resetting.

Maximum Number of Questions

This value specifies the maximum number of questions to be asked in the password reset page.

Force Change Password on Next Login

When enabled, this option forces the user to change his or her password on the next login. If you want an administrator, other than the top-level administrator, to set the force password reset option, you must modify the Default Permissions ACIs to allow access to that attribute.

Password Reset Failure Lockout

This attribute specifies whether to disallow users to reset their password if that user initially fails to reset the password using the Password Reset application. By default, this feature is not enabled.

Password Reset Failure Lockout Count

This attributes defines the number of attempts that a user may try to reset a password, within the time interval defined in Password Reset Failure Lockout Interval, before being locked out. For example, if Password Reset Failure Lockout Count is set to 5 and Login Failure Lockout Interval is set to 5 minutes, the user has five chances within five minutes to reset the password before being locked out.

Password Reset Failure Lockout Interval

This attribute defines (in minutes) the amount of time in which the number of password reset attempts (as defined in Password Reset Failure Lockout Count) can be completed, before being locked out.

Email Address to Send Lockout Notification

This attribute specifies an email address that will receive notification if a user is locked out from the Password Reset service. Specify multiple email address in a space-separated list.

Warn User After N Failure

This attribute specifies the number of password reset failures that can occur before Access Manager sends a warning message that user will be locked out.

Password Reset Failure Lockout Duration

This attribute defines (in minutes) the duration that user will not be able to attempt a password reset if a lockout has occurred.

Password Reset Lockout Attribute Name

This attribute contains the *inetuserstatus* value that is set in Password Reset Lockout Attribute Value. If a user is locked out from Password Reset, and the Password Reset Failure Lockout Duration (minutes) variable is set to 0, *inetuserstatus* will be set to inactive, prohibiting the user from attempting to reset his or her password.

Password Reset Lockout Attribute Value

This attribute specifies the *inetuserstatus* value (contained in Password Reset Lockout Attribute Name) of the user status, as either active or inactive. If a user is locked out from Password Reset, and the Password Reset Failure Lockout Duration (minutes) variable is set to 0, *inetuserstatus* will be set to inactive, prohibiting the user from attempting to reset his or her password.

Policy Configuration

The Policy Configuration attributes enable the administrator to set configuration global and realm properties used by the Policy service.

- "Global Properties" on page 98
- "Realm Attributes" on page 99

Global Properties

The Global Properties are:

Resource Comparator

Specifies the resource comparator information used to compare resources specified in a Policy rule definition. Resource comparison is used for both policy creation and evaluation.

Click the Add button and define the following attributes:

Service Type	Specifies the service to which the comparator should be used.
Class	Defines the Java class that implements the resource comparison algorithm.
Delimiter	Specifies the delimiter to be used in the resource name.
Wildcard	Specifies the wildcard that can be defined in resource names.

One Level Wildcard	Matches zero or more characters, at the same delimiter boundary.
Case Sensitive	Specifies if the comparison of the two resources should consider or ignore case. False ignores case, True considers case.

Continue Evaluation on Deny Decision

Specifies whether or not the policy framework should continue evaluating subsequent policies, even if a DENY policy decision exists. If it is not selected (default), policy evaluation would skip subsequent policies once the DENY decision is recognized.

Advices Handleable by Access Manager

Defines the names of policy advice keys for which the Policy Enforcement Point (Policy Agent) would redirect the user agent to Access Manager. If the agent receives a policy decision that does not allow access to a resource, but does posses advices, the agent checks to see whether it has a advice key listed in this attribute.

If such an advice is found, the user agent is redirected to Access Manager, potentially allowing the access to the resource.

Organization Alias Referrals

When set to Yes, this attribute allows you to create policies in sub-realms without having to create referral policies from the top-level or parent realm. You can only create policies to protect HTTP or HTTPS resources whose fully qualified hostname matches the DNSAlias of the realm. By default, this attribute is defined as No.

Realm Attributes

The LDAP Properties are:

Primary LDAP Server

Specifies the host name and port number of the primary LDAP server specified during Access Manager installation that will be used to search for Policy subjects, such as LDAP users, LDAP roles, LDAP groups, and so forth.

The format is *hostname:port*. For example: `machine1.example.com:389`

For failover configuration to multiple LDAP server hosts, this value can be a space-delimited list of hosts. The format is *hostname1:port1 hostname2:port2...*

For example: `machine1.example1.com:389` `machine2.example1.com:389`

Multiple entries must be prefixed by the local server name. This is to allow specific Access Managers to be configured to talk to specific Directory Servers.

The format is *servername*|*hostname:port* For example:

```
machine1.example1.com|machine1.example1.com:389
```

```
machine1.example2.com|machine1.example2.com:389
```

For failover configuration:

```
AM_Server1.example1.com|machine1.example1.com:389 machine2.example.com1:389
```

```
AM_Server2.example2.com|machine1.example2.com:389 machine2.example2.com:389
```

LDAP Base DN

Specifies the base DN in the LDAP server from which to begin the search. By default, it is the top-level realm of the Access Manager installation.

LDAP Users Base DN

This attribute specifies the base DN used by the LDAP Users subject in the LDAP server from which to begin the search. By default, it is the top-level realm of the Access Manager installation base.

Access Manager Roles Base DN

Defines the DN of the realm or organization which is used as a base while searching for the values of Access Manager Roles. This attribute is used by the *AccessManagerRoles* policy subject.

LDAP Bind DN

Specifies the bind DN in the LDAP server.

LDAP Bind Password

Defines the password to be used for binding to the LDAP server. By default, the `amldapuser` password that was entered during installation is used as the bind user.

LDAP Organization Search Filter

Specifies the search filter to be used to find organization entries. The default is `(objectclass=sunMangagedOrganization)`.

LDAP Organizations Search Scope

Defines the scope to be used to find organization entries. The scope must be one of the following:

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (default)

LDAP Groups Search Scope

Defines the scope to be used to find group entries. The scope must be one of the following:

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (default)

LDAP Groups Search Filter

Specifies the search filter to be used to find group entries. The default is `(objectclass=groupOfUniqueNames)`.

LDAP Users Search Filter

Specifies the search filter to be used to find user entries. The default is `(objectclass=inetorgperson)`.

LDAP Users Search Scope

Defines the scope to be used to find user entries. The scope must be one of the following:

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (default)

LDAP Roles Search Filter

Specifies the search filter to be used to find entries for roles. The default is `(&(objectclass=ldapsubentry)(objectclass=nsroledefinitions))`.

LDAP Roles Search Scope

This attribute defines the scope to be used to find entries for roles. The scope must be one of the following:

- SCOPE_BASE

- SCOPE_ONE
- SCOPE_SUB (default)

Access Manager Roles Search Scope

Defines the scope to be used to find entries for Access Manager Roles subject.

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (default)

LDAP Organization Search Attribute

Defines the attribute type for which to conduct a search on an organization. The default is `o`.

LDAP Groups Search Attribute

Defines the attribute type for which to conduct a search on a group. The default is `cn`.

LDAP Users Search Attribute

Defines the attribute type for which to conduct a search on a user. The default is `uid`.

LDAP Roles Search Attribute

This field defines the attribute type for which to conduct a search on a role. The default is `cn`.

Maximum Results Returned from Search

This field defines the maximum number of results returned from a search. The default value is 100. If the search limit exceeds the amount specified, the entries that have been found to that point will be returned.

Search Timeout

Specifies the amount of time before a timeout on a search occurs. If the search exceeds the specified time, the entries that have been found to that point will be returned

LDAP SSL

Specifies whether or not the LDAP server is running SSL. Selecting enables SSL, deselecting (default) disables SSL.

If the LDAP Server is running with SSL enabled (LDAPS), you must make sure that Access Manager is configured with proper SSL-trusted certificates so that Access Manager can connect to Directory server over LDAPS protocol.

LDAP Connection Pool Minimum Size

Specifies the minimal size of connection pools to be used for connecting to the Directory Server, as specified in the LDAP server attribute. The default is 1.

Connection Pool Maximum Size

This attribute specifies the maximum size of connection pools to be used for connecting to the Directory Server, as specified in the LDAP server attribute. The default is 10.

Selected Policy Subjects

Allows you to select a set of subject types available to be used for policy definition in the realm.

Selected Policy Conditions

Allows you to select a set of conditions types available to be used for policy definition in the realm.

Selected Policy Referrals

Allows you to select a set of referral types available to be used for policy definition in the realm.

Subject Results Time To Live

This attribute specifies the amount of time (in minutes) that a cached subject result can be used to evaluate the same policy request based on the single sign-on token.

When a policy is initially evaluated for an SSO token, the subject instances in the policy are evaluated to determine whether the policy is applicable to a given user. The subject result, which is keyed by the SSO token ID, is cached in the policy. If another evaluation occurs for the same policy for the same SSO token ID within the time specified in the Subject Result Time To Live attribute, the policy framework retrieves the cached subjects result, instead of evaluating the subject instances. This significantly reduces the time for policy evaluation.

User Alias

This attribute must be enabled if you create a policy to protect a resource whose subject's member in a remote Directory Server aliases a local user. This attribute must be enabled, for example, if you create `uid=rmuser` in the remote Directory Server and then add `rmuser` as an

alias to a local user (such as `uid=luser`) in Access Manager. When you login as `rmuser`, a session is created with the local user (`luser`) and policy enforcement is successful.

Selected Response Providers

Defines the policy response provider plug-ins that are enabled for the realm. Only the response provider plug-ins selected in this attribute can be added to policies defined in the realm.

Selected Dynamic Response Attributes

Defines the dynamic response attributes that are enabled for the realm. Only a subset of names selected in this attribute can be defined in the dynamic attributes list in *IDResponseProvider* to be added to policies defined in the realm.

Session

The Session service defines values for an authenticated user session such as maximum session time and maximum idle time. The Session attributes are global, dynamic, or user attributes. The attributes are:

- "Secondary Configuration Instance" on page 104
- "Maximum Number of Search Results" on page 105
- "Timeout for Search" on page 105
- "Property Change Notifications" on page 105
- "Quota Constraints" on page 105
- "Read Timeout for Quota Constraint" on page 105
- "Exempt Top-Level Admins From Constraint Checking" on page 105
- "Resulting Behavior If Session Quota Exhausted" on page 106
- "Notification Properties" on page 106
- "Maximum Session Time" on page 106
- "Maximum Idle Time" on page 106
- "Maximum Caching Time" on page 107
- "Active User Sessions" on page 107

Secondary Configuration Instance

Provides the connection information for the session repository used for the session failover functionality in Access Manager. The URL of the load balancer should be given as the identifier to this secondary configuration. If the secondary configuration is defined in this case, the session failover feature will be automatically enabled and become effective after the server restart. See "To Add a Sub Configuration" on page 107 for more information.

Maximum Number of Search Results

This attribute specifies the maximum number of results returned by a session search. The default value is 120.

Timeout for Search

This attributed defines the maximum amount of time before a session search terminates. The default value is 5 seconds.

Property Change Notifications

Enables or disables the feature session property change notification. In a single sign-on environment, one Access Manager session can be shared by multiple applications. If this feature is set to ON, if one application changes any of the session properties specified in the Notification Properties list (defined as a separate session service attribute), the notification will be sent to other applications participating in the same single sign-on environment.

Quota Constraints

Enables or disables session quota constraints. The enforcement of session quota constraints enables administrators to limit a user to have a specific number of active/concurrent sessions based on the constraint settings at the global level, or the configurations associated with the entities (realm/role/user) to which this particular user belongs.

The default setting for this attribute is OFF. You must restart the server if the settings are changed.

Read Timeout for Quota Constraint

Defines the amount of time (in number of milliseconds) that an inquiry to the session repository for the live user session counts will continue before timing out.

After the maximum read time is reached, an error is returned. This attribute will take effect only when the session quota constraint is enabled in the session failover deployment. The default value is 6000 milliseconds. You must restart the server if the settings are changed.

Exempt Top-Level Admins From Constraint Checking

Specifies whether the users with the Top-level Admin Role should be exempt from the session constraint checking. If YES, even though the session constraint is enabled, there will be no session quota checking for these administrators.

The default setting for this attribute is NO. You must restart the server if the settings are changed. This attribute will take effect only when the session quota constraint is enabled.

Note – the super user defined for the Access Manager in `AMConfig.properties` (`com.sun.identity.authentication.super.user`) is always exempt from the session quota constraint checking.

Resulting Behavior If Session Quota Exhausted

Specifies the resulting behavior when the user session quota is exhausted. There are two selectable options for this attribute:

DESTROY_OLD_SESSION	The next expiring session will be destroyed.
DENY_ACCESS	The new session creation request will be denied.

This attribute will take effect only when the session quota constraint is enabled and the default setting is DESTROY_OLD_SESSION .

Notification Properties

When a change occurs on a session property defined in the list, the notification will be sent to the registered listeners. The attribute will take effect when the feature of Session Property Change Notification is enabled.

Maximum Session Time

This attribute accepts a value in minutes to express the maximum time before the session expires and the user must reauthenticate to regain access. A value of 1 or higher will be accepted. The default value is 120. (To balance the requirements of security and convenience, consider setting the Max Session Time interval to a higher value and setting the Max Idle Time interval to a relatively low value.) Max Session Time limits the validity of the session. It does not get extended beyond the configured value.

Maximum Idle Time

This attribute accepts a value (in minutes) equal to the maximum amount of time without activity before a session expires and the user must reauthenticate to regain access. A value of 1 or higher will be accepted. The default value is 30. (To balance the requirements of security and convenience, consider setting the Max Session Time interval to a higher value and setting the Max Idle Time interval to a relatively low value.)

Maximum Caching Time

This attribute accepts a value (in minutes) equal to the maximum interval before the client contacts Access Manager to refresh cached session information. A value of 0 or higher will be accepted. The default value is 3. It is recommended that the maximum caching time should always be less than the maximum idle time.

Active User Sessions

Specifies the maximum number of concurrent sessions allowed for a user.

▼ To Add a Sub Configuration

1. **Click New in the Secondary Configuration Instance list.**
2. **Enter a name for the new Sub Configuration.**
3. **Enter data for the following fields:**

Session Store User	Defines the database user who is used to retrieve and store the session data.
Session Store Password	Defines the password for the database user defined in Session Store.
Session Store Password (Confirm)	Confirm the password.
Maximum Wait Time	Defines the total time a thread is willing to wait for acquiring a database connection object. The value is in milliseconds.
Database Url	Specifies the URL of the database.

4. **Click Add.**

User

The default user preferences are defined through the user service. These include time zone, locale and DN starting view. The User service attributes are dynamic attributes.

- "User Preferred Language" on page 108
- "User Preferred Timezone" on page 108
- "Inherited Locale" on page 108
- "Administrator Starting View" on page 108
- "Default User Status" on page 108

User Preferred Language

This field specifies the user's choice for the text language displayed in the Access Manager console. The default value is en. This value maps a set of localization keys to the user session so that the on-screen text appears in a language appropriate for the user.

User Preferred Timezone

This field specifies the time zone in which the user accesses the Access Manager console. There is no default value.

Inherited Locale

This field specifies the locale for the user. The default value is en_US. See "Supported Language Locales" on page 79 for a list of locales.

Administrator Starting View

If this user is a Access Manager administrator, this field specifies the node that would be the starting point displayed in the Access Manager console when this user logs in. There is no default value. A valid DN for which the user has, at the least, read access can be used.

Default User Status

This option indicates the default status for any newly created user. This status is superseded by the User Entry status. Only active users can authenticate through Access Manager. The default value is Active. Either of the following can be selected from the pull-down menu:

Active	The user can authenticate through Access Manager.
Inactive	The user cannot authenticate through Access Manager, but the user profile remains stored in the directory.

The individual user status is set by registering the User service, choosing the value, applying it to a role and adding the role to the user's profile.

System Properties

System Properties contain the following default services that you can configure:

- "Client Detection" on page 109
- "To Add a New Client" on page 111
- "Logging" on page 111
- "Naming" on page 115
- "Platform" on page 118

Client Detection

An initial step in the authentication process is to identify the type of client making the HTTP(S) request. This Access Manager feature is known as client detection. The URL information is used to retrieve the client's characteristics. Based on these characteristics, the appropriate authentication pages are returned. For example, when a Netscape browser is used to request a web page, Access Manager 7.1 displays an HTML login page. Once the user is validated, the client type (Netscape browser) is added to the session token. The attributes defined in the Client Detection service are global attributes.

- "Client Types" on page 109
- "Default Client Type" on page 110
- "Client Detection Class" on page 110
- "Client Detection" on page 111

Client Types

In order to detect client types, Access Manager needs to recognize their identifying characteristics. These characteristics identify the properties of all supported types in the form of client data. This attribute allows you to modify the client data through the Client Manager interface. To access the Client Manager, click the Edit link. Out of the box, Access Manager contains the following client types:

- HDML
- HTML
- JHTML
- VoiceX
- WML
- XHTML
- cHTML
- iHTML

For descriptions of these client types, see the Sun Java System Portal Server, Mobile Access Administration Guide at `http://docs.sun.com/app/docs/coll/PortalServer_05q4` .

Client Manager

The Client Manager is the interface that lists the base clients, styles and associated properties, and allows you to add and configure devices. The Base client types are listed at the top of Client Manager. These client types contain the default properties that can be inherited by all devices that belong to the client type.

Client Type

Style Profile The Client Manager groups all available clients, including the Base client type itself, in the Client Type list. For each client, you can modify the client properties by clicking on the device name. The properties are then displayed in the Client Editor window. To edit the properties, select the following classifications from the pull-down list:

Hardware Platform	Contains properties of the device's hardware, such as display size, supported character sets, and so forth.
Software Platform	Contains properties of the device's application environment, operating system, and installed software.
Network Characteristics	Contains properties describing the network environment, including the supported bearers.
BrowserUA	Contains attributes related to the browser user agent running on the device.
WapCharacteristics	Contains properties of the Wireless Application Protocol (WAP) environment supported by the device.
PushCharacteristicNames	Contains properties of the WAP environment supported by the device.
Additional Properties	Contains properties of the Wireless Application Protocol (WAP) environment supported by the device.

Note – For specific property definitions, see the *Open Mobile Alliance Ltd. (OMA) Wireless Application Protocol, Version 20-Oct-2001* at `http://www1.wapforum.org/tech/terms.asp?doc=WAP-248-UAProf-20011020-a.pdf`.

In order to access the document, you may first have to register with WAP Forum™. For information, please visit `http://www.wapforum.org/faqs/index.htm`.

Default Client Type

This attribute defines the default client type derived from the list of client types in the Client Types attribute. The default is genericHTML.

Client Detection Class

This attribute defines the client detection class for which all client detection requests are routed. The string returned by this attribute should match one of the client types listed in the Client Types attribute. The default client detection class is `com.sun.mobile.cdm.FEDIClientDetector`. Access Manager also contains `com.iplanet.services.cdm.ClientDetectionDefaultImpl`.

Client Detection

Enables client detection. If client detection is enabled (default), every request is routed thought the class specified in the Client Detection Class attribute. By default, the client detection capability is enabled. If this attribute is not selected, Access Manager assumes that the client is genericHTML and will be accessed from a HTML browser.

▼ To Add a New Client

1. **Click New in the Client Type list.**
2. **Select the device type with the following fields:**

Style	Displays the base style for the device. For example, HTML.
Device User Agent	Accepts the name for the device.

3. **Click Next.**
4. **Enter the following information for the new device:**

Client Type Name	Accepts the name for the device. The name must be unique across all devices
The HTTP User String	Defines the User-Agent in the HTTP request header. For example, Mozilla/4.0.

5. **Click Finish.**
6. **To duplicate a device and its properties, click the Duplicate link. Device names must unique. By default, Access Manager will rename the device to** `copy_of_`*devicename*.

Logging

The Logging service provides status and error messages related to Access Manager administration. An administrator can configures values such as log file size and log file location. Access Manager can record events in flat text files or in a relational database. The Logging service attributes are global attributes. The attributes are:

- "Maximum Log Size" on page 112
- "Number of History Files" on page 112
- "Log File Location" on page 112
- "Logging Type" on page 113
- "Database User Name" on page 113

- "Database User Password" on page 113
- "Database User Password (confirm)" on page 113
- "Database Driver Name" on page 113
- "Configurable Log Fields" on page 113
- "Log Verification Frequency" on page 114
- "Log Signature Time" on page 114
- "Secure Logging" on page 114
- "Maximum Number of Records" on page 114
- "Number of Files per Archive" on page 114
- "Buffer Size" on page 114
- "DB Failure Memory Buffer Size" on page 115
- "Buffer Time" on page 115
- "Time Buffering" on page 115

Maximum Log Size

This attribute accepts a value for the maximum size (in bytes) of a Access Manager log file. The default value is 1000000.

Number of History Files

This attribute has a value equal to the number of backup log files that will be retained for historical analysis. Any integer can be entered depending on the partition size and available disk space of the local system. The default value is 3.

The files only apply to the FILE logging type. When the logging type is set to DB, there are no history files and limit explicitly set by Access Manager to the size of the files.

Note – Entering a value of 0 is interpreted to be the same as a value of 1, meaning that if you specify 0, a history log file will be created.

Log File Location

The file-based logging function needs a location where log files can be stored. This field accepts a full directory path to that location. The default location is:

```
/var/opt/SUNWam/logs
```

If a non-default directory is specified, Access Manager will create the directory if it does not exist. You should then set the appropriate permissions for that directory (for example, 0700).

When configuring the log location for DB (database) logging (such as, Oracle or MySQL), part of the log location is case sensitive. For example, if you are logging to an Oracle database, the log location should be (note case sensitivity):

```
jdbc:oracle:thin:@machine.domain:port:DBName
```

To configure logging to DB, add the JDBC driver files to the web container's JVM classpath. You need to manually add JDBC driver files to the classpath of the `amadmin` script, otherwise `amadmin` logging can not load the JDBC driver.

Changes to logging attributes usually take effect after you save them. This does not require you to restart the server. If you are changing to secure logging, however, you should restart the server.

Logging Type

Enables you to specify either File, for flat file logging, or DB for database logging.

If the Database User Name or Database User Password is invalid, it will seriously affect Access Manager processing. If Access manager or the console becomes unstable, you set the following property in `AMConfig.properties`:

com.iplanet.am.logstatus=INACTIVE

After you have set the property, restart the server. You can then log in to the console and reset the logging attribute. Then, change the *logstatus* property to *ACTIVE* and restart the server.

Database User Name

This attribute accepts the name of the user that will connect to the database when the Logging Type attribute is set to DB.

Database User Password

This attribute accepts the database user password when the Logging Type attribute is set to DB.

Database User Password (confirm)

Confirm the database password.

Database Driver Name

This attribute enables you to specify the driver used for the logging implementation class.

Configurable Log Fields

Represents the list of fields that are to be logged. By default, all of the fields are logged. The fields are:

- CONTEXTID

- DOMAIN
- HOSTNAME
- IPADDRESS
- LOGGED BY
- LOGLEVEL
- LOGINID
- MESSAGEID
- MODULENAME

At minimum you should log CONTEXTID, DOMAIN, HOSTNAME, LOGINID and MESSAGEID.

Log Verification Frequency

This attribute sets the frequency (in seconds) that the server should verify the logs to detect tampering. The default time is 3600 seconds. This parameter applies to secure logging only.

Log Signature Time

This parameter sets the frequency (in seconds) that the log will be signed. The default time is 900 seconds. This parameter applies to secure logging only.

Secure Logging

This attribute enables or disables secure logging. By default, secure logging is off. Secure Logging enables detection of unauthorized changes or tampering of security logs.

Maximum Number of Records

This attribute sets the maximum number of records that the Java LogReader interfaces return, regardless of how many records match the read query. By default, it is set to 500. This attribute can be overridden by the caller of the Logging API through the *LogQuery* class.

Number of Files per Archive

This attribute is only applicable to secure logging. It specifies when the log files and keystore need to be archived, and the secure keystore regenerated, for subsequent secure logging. The default is five files per logger.

Buffer Size

This attribute specifies the maximum number of log records to be buffered in memory before the logging service attempts to write them to the logging repository. The default is one record.

DB Failure Memory Buffer Size

This attribute defines the maximum number of log records held in memory if database (DB) logging fails. This attribute is only applicable when DB logging is specified. When the Access Manager logging service loses connection to the DB, it will buffer up to the number of records specified. This attribute defaults to two times of the value defined in the Buffer Size attribute.

Buffer Time

This attribute defines the amount of time that the log records will buffered in memory before they are sent to the logging service to be logged. This attribute applies if Enable Time Buffering is ON. The default is 3600 seconds.

Time Buffering

When selected as ON, Access Manager will set a time limit for log records to be buffered in memory. The amount of time is set in the Buffer Time attribute.

Naming

The Naming service is used to get and set URLs, plug-ins and configurations as well as request notifications for various other Access Manager services such as session, authentication, logging, SAML and Federation.

This service enables clients to find the correct service URL if the platform is running more than one Access Manager. When a naming URL is found, the naming service will decode the session of the user and dynamically replace the protocol, host, and port with the parameters from the session. This ensures that the URL returned for the service is for the host that the user session was created on. The Naming attributes are:

- "Profile Service URL" on page 116
- "Session Service URL" on page 116
- "Logging Service URL" on page 116
- "Policy Service URL" on page 116
- "Authentication Service URL" on page 116
- "SAML Web Profile/Artifact Service URL" on page 117
- "SAML SOAP Service URL" on page 117
- "SAML Web Profile/POST Service URL" on page 117
- "SAML Assertion Manager Service URL" on page 117
- "Federation Assertion Manager Service URL" on page 117
- "Security Token Manager URL" on page 118
- "JAXRPC Endpoint URL" on page 118

Profile Service URL

This field takes a value equal to :

```
%protocol://%host:%port/Server_DEPLOY_URI/profileservice
```

This syntax allows for dynamic substitution of the profile URL based on the specific session parameters.

Session Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/sessionservice
```

This syntax allows for dynamic substitution of the session URL based on the specific session parameters.

Logging Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/loggingservice
```

This syntax allows for dynamic substitution of the logging URL based on the specific session parameters.

Policy Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/policyservice
```

This syntax allows for dynamic substitution of the policy URL based on the specific session parameters.

Authentication Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/authservice
```

This syntax allows for dynamic substitution of the authentication URL based on the specific session parameters.

SAML Web Profile/Artifact Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/SAMLAwareServlet
```

This syntax allows for dynamic substitution of the SAML web profile/artifact URL based on the specific session parameters.

SAML SOAP Service URL

This field takes a value equal to

```
%protocol://%host:%port/Server_DEPLOY_URI/SAMLSOAPReceiver
```

This syntax allows for dynamic substitution of the SAML SOAP URL based on the specific session parameters.

SAML Web Profile/POST Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/SAMLPOSTProfileServlet
```

This syntax allows for dynamic substitution of the SAML web profile/POST URL based on the specific session parameters.

SAML Assertion Manager Service URL

This field takes a value equal to:

```
%protocol://%host:%port/Server_DEPLOY_URI/AssertionManagerServlet/AssertionM
anagerIF
```

This syntax allows for dynamic substitution of the SAML Assertion Manager Service URL based on the specific session parameters.

Federation Assertion Manager Service URL

This field takes a value equal to:

```
%protocol://%host:%port/amserver/FSAssertionManagerServlet/FSAssertionMana
gerIF
```

This syntax allows for dynamic substitution of the Federation Assertion Manager Service URL based on the specific session parameters.

Security Token Manager URL

This field takes a value equal to:

```
%protocol://%host:%port/amserver/SecurityTokenManagerServlet/SecurityToken
ManagerIF/
```

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

JAXRPC Endpoint URL

This field takes a value equal to:

```
%protocol://%host:%port/amserver/jaxrpc/
```

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

Platform

The Platform service is where additional servers can be added to the Access Manager configuration as well as other options applied at the top level of the Access Manager application. The Platform service attributes are global attributes. The attributes are:

- "Site Name" on page 118
- "Instance Name" on page 119
- "Platform Locale" on page 119
- "Cookie Domains" on page 119
- "Login Service URL" on page 119
- "Logout Service URL" on page 119
- "Available Locales" on page 119
- "Client Character Sets" on page 120

Site Name

The naming service reads this attribute at initialization time. This list uniquely identifies the FQDN with the port number of the load balancer or SRA for load balancing on the back-end Access Manager servers. If the host specified in a request for a service URL is not in this list, the naming service will reject the request. Only the naming service protocol should be used in this attribute. See "To Create a New Site Name" on page 120.

Instance Name

The naming service reads this attribute at initialization time. This list contains the Access Manager session servers in a single Access Manager configuration. For example, if two Access Managers are installed and should work as one, they must both be included in this list. If the host specified in a request for a service URL is not in this list, the naming service will reject the request. Only the naming service protocol should be used in this attribute. See "To Create a New Instance Name" on page 120.

Platform Locale

The platform locale value is the default language subtype that Access Manager was installed with. The authentication, logging and administration services are administered in the language of this value. The default is en_US. See "Supported Language Locales" on page 79for a listing of supported language subtypes.

Cookie Domains

The list of domains that will be returned in the cookie header when setting a cookie to the user's browser during authentication. If empty, no cookie domain will be set. In other words, the Access Manager session cookie will only be forwarded to the Access Manager itself and to no other servers in the domain.

If SSO is required with other servers in the domain, this attribute must be set with the cookie domain. If you had two interfaces in different domains on one Access Manager then you would need to set both cookie domains in this attribute. If a load balancer is used, the cookie domain must be that of the load balancer's domain, not the servers behind the load balancer. The default value for this field is the domain of the installed Access Manager.

Login Service URL

This field specifies the URL of the login page. The default value for this attribute is `/Service_DEPLOY_URI/UI/Login`.

Logout Service URL

This field specifies the URL of the logout page. The default value for this attribute is `/Service_DEPLOY_URI/UI/Logout`.

Available Locales

This attribute stores all available locales configured for the platform. Consider an application that lets the user choose the user's locale. This application would get this attribute from the platform profile and present the list of locales to the user. The user would choose a locale and the application would set this in the user entry *preferredLocale*.

Client Character Sets

This attribute specifies the character set for different clients at the platform level. It contains a list of client types and the corresponding character sets. See"To Create a New Character Set" on page 121 for more information.

▼ To Create a New Site Name

1. **Click New in the Site Name list.**
2. **Enter the host name and port in the Server field.**
3. **Enter the Site Name.**

   This value uniquely identifies the server. Each server that is participating in load balancing or failover needs to have a unique identifier of a two-digit number. For example, `01`.
4. **Click Save.**

   To edit a site name, click an entry in the Site Name list and change the values accordingly.

▼ To Create a New Instance Name

The naming service reads this attribute at initialization time. This list contains the Access Manager session servers in a single Access Manager configuration.

1. **Click New in the Instance Name list.**
2. **Enter the hostname and port in the Server field.**
3. **Enter the Site Name.**

   This value uniquely identifies the server. Each server that is participating in load balancing or failover needs to have a unique identifier. This is also used to shorten the cookie length by mapping the server URL to the server ID. The syntax is:

   ```
   intance_ID(|site_ID)
   ```
4. **Click OK.**

   To edit an instance name, click an entry in the Instance Name list and change the values accordingly.
5. **Click Save in the Platform Service main page.**

▼ To Create a New Character Set

1. Click New from the Client Character Sets list.
2. Enter a value for the Client Type.
3. Enter a value for the Character Set. See "Supported Language Locales" on page 79 for the character sets available.
4. Click OK.
5. Click Save in the Platform Service main page.

PART III

File Reference

CHAPTER 6

amConfig.properties Reference

`AMConfig.properties` is the main configuration file for Access Manager. You can configure some, but not all, of the properties in this file. This chapter provides descriptions of properties contained in `AMConfig.properties`, default property values, and instructions for modifying values that can be changed without rendering Access Manager unusable.

This chapter contains the following sections:

- "About the `AMConfig.properties` File" on page 126
- "Access Manager Console" on page 126
- "Access Manager Server Installation" on page 126
- "am.util" on page 128
- "amSDK" on page 128
- "Application Server Installation" on page 128
- "Authentication" on page 129
- "Certificate Database" on page 130
- "Cookies" on page 130
- "Debugging" on page 131
- "Directory Server Installation" on page 132
- "Event Connection" on page 132
- "Global Services Management" on page 133
- "Helper Daemons" on page 133
- "Identity Federation" on page 134
- "JSS Proxy" on page 135
- "LDAP Connection" on page 136
- "Logging Service" on page 140
- "Naming Service" on page 141
- "Notification Service" on page 142
- "Policy Agents" on page 142
- "Policy Client API" on page 144
- "Profile Service" on page 144
- "Replication" on page 145
- "SAML Service" on page 145

- "Security" on page 146
- "Session Service" on page 147
- "SMTP" on page 148
- "Statistics Service" on page 148

About the AMConfig.properties File

At installation, AMConfig.properties is located in the following directory: etc/opt/SUNWam/config.

AMConfig.properties contains one property per line, and each property has a corresponding value. Properties and values are case-sensitive. Lines that begin with the characters slash and asterisk (/*) are comments, and comments are ignored by the application. Comments end with a last line that contains the closing characters asterisk and slash (*/).

After you modify properties in AMConfig.properties, you must restart Access Manager to activate the changes.

Access Manager Console

- com.iplanet.am.console.deploymentDescriptor

  Value is set during installation. Example: /amconsole
- com.iplanet.am.console.host

  Value is set during installation. Example: *hostName.domain.Name*.com
- com.iplanet.am.console.port

  Value is set during installation. Example: 80
- com.iplanet.am.console.protocol

  Value is set during installation. Example: http

Access Manager Server Installation

- com.iplanet.am.install.basedir

  This is a READ-ONLY property. Do not change the property value.

  Value is set during installation. Example: /opt/SUNWam/web-src/services/WEB-INF
- com.iplanet.am.install.vardir

  This is a READ-ONLY property. Do not change the property value.

  Value is set during installation. Example: /var/opt/SUNWam

- `com.iplanet.am.installdir`

  This is a READ-ONLY property. Do not change the property value.

  Value is set during installation. Example: `/opt/SUNWam`
- `com.iplanet.am.jdk.path`

  Value is set during installation. Example: `/usr/jdk/entsys-j2se`
- `com.iplanet.am.locale`

  Value is set during installation. Example: `en_US`
- `com.iplanet.am.server.host`

  Value is set during installation. Example: *hostName.domainName*`.com`
- `com.iplanet.am.server.port`

  Value is set during installation. Example: `80`
- `com.iplanet.am.server.protocol`

  Value is set during installation. Example: `http`
- `com.iplanet.am.version`

  Value is set during installation. Example: `7 2005Q4`
- `com.sun.identity.server.fqdnMap[ ]`

  Enables Access Manager Authentication service to take corrective action when a user types an incorrect URL . This is useful, for example, when a user specifies a partial hostname or uses an IP address to access protected resources.

  The syntax of this property represents invalid FQDN values mapped to their corresponding valid counterparts. The property uses the following form: `com.sun.identity.server.fqdnMap[`*invalid-name*`]=`*valid—name* . In this example, *invalid-name* is a possible invalid FQDN host name that may be used by the user, and the *valid—name* is the FQDN host name the filter will redirect the user to. If overlapping values for the same invalid FQDN exist, the application may become inaccessible. Using an invalid value for this property can also result in the application becoming inaccessible. You can use this property to map multiple host names. This is useful when the applications hosted on a server are accessible by multiple host names.

  You can use this property to configure Access Manager so that no corrective action is taken for certain hostname URLs. This is useful, for example, when it is required that no corrective action such as a redirect be used for users who access the application resources by using the raw IP address.

  You can specify a map entry such as: `com.sun.identity.server.fqdnMap[`*IP*`]=`*IP* .

  You can specify any number of such properties may as long as they are valid properties and conform to the requirements described above. Examples:
  `com.sun.identity.server.fqdnMap[`*isserver*`]=`*isserver.mydomain.com*
  `com.sun.identity.server.fqdnMap[`*isserver.mydomain*`]=`*isserver.mydomain.com*
  `com.sun.identity.server.fqdnMap[`*IP address*`]=`*isserver.mydomain.com*

am.util

- `com.iplanet.am.util.xml.validating`

  Default value is `no`. Determines if validation is required when parsing XML documents using the Access Manager `XMLUtils` class. This property is in effect only when value for the `com.iplanet.services.debug.level` property is set to `warning` or `message`. Allowable values are `yes` and `no`. The XML document validation is turned on only if the value for this property `yes`, and if value for `com.iplanet.services.debug.level` `property` is set to `warning` or `message`.

amSDK

Each SDK cache entry stores a set of `AMObject` attributes values for a user.

- `com.iplanet.am.sdk.cache.maxSize`

  Default value is `10000`. Specifies the size of the SDK cache when caching is enabled. Use an integer greater than 0, or the default size (10000 users) will be used.

- `com.iplanet.am.sdk.userEntryProcessingImpl`

  This property specifies a plug-in which implements the `com.iplanet.am.sdk.AMUserEntryProcessed` interface to perform some post-processing for user create, delete and modify operations. The property if used should specify the fully qualified class name which implements the above interface.

- `com.iplanet.am.sdk.caching.enabled`

  Setting this to true enables caching, and setting this to false disables caching. The default is true.

Note – Do not set this option to false unless you are running Access manager in a pure debugging mode. It should never be set to false in production.

Application Server Installation

- `com.iplanet.am.iASConfig`

  Value is set during installation. Example: `APPSERVERDEPLOYMENT`

  This property is used to determine if Access Manager is running on iPlanet Application Server.

Authentication

- `com.sun.identity.auth.cookieName`

  Default value is `AMAuthCookie`. Specifies the cookie name used by Authentication Service to set the session handler ID during the authentication process. Once this process is completed (success or failure), this cookie is cleared or removed.

- `com.sun.identity.authentication.ocsp.responder.nickname`

  Value is set during installation. The Certificate Authority (CA) certificate nick name for that responder. Example: `Certificate Manager - sun`. If set, the CA certificate must be presented in the Web Server's certificate database.

- `com.sun.identity.authentication.ocsp.responder.url`

  Value is set during installation. Example: `http://ocsp.sun.com/ocsp`

  Specifies the global OCSP responder URL for this instance. If the OCSP responder URL is set, the OCSP responder nick name must also be set. Otherwise both will be ignored. If both are not set, the OCSP responder URL presented in user's certificate will be used for OCSP validation. If the OCSP responder URL is not presented in user's certificate, then no OCSP validation will be performed.

- `com.sun.identity.authentication.ocspCheck`

  Default value is `true.` The global parameter to enable or disable OCSP checking. If this value is `false`, the OCSP feature in the Certificate Authentication module type cannot be used. .

- `com.sun.identity.authentication.special.users`

  Value is set during installation. Example: `cn=dsameuser,ou=DSAME Users,o=AMRoot|cn=amService-UrlAccessAgent,ou=DSAME Users,o=AMRoot`

  Identifies the special user or users for this Access Manager authentication component. This user is used by the Client APIs to authenticate remote applications to the Access Manager server using the full user DN. The user will always be authenticated against the local directory server. Multiple values of this special user DN are separated by the pipe character (|). Use of this property is restricted to Authentication component only.

- `com.sun.identity.authentication.super.user`

  Value is set during installation. Example: `uid=amAdmin,ou=People,o=AMRoot`

  Identifies the super user for this Access Manager instance. This user must use LDAP to log in, and must use the full DN. The user is always authenticated against the local Directory Server.

- `com.sun.identity.authentication.uniqueCookieDomain`

  Used to set the cookie domain for the above cookie name. This Cookie domain should be set such that it covers all the instances of the CDC (Cross Domain Controller) services installed in the network. For example, `.example.com` if all instances of Access Manager are within the domain `example.com`.

- `com.sun.identity.authentication.uniqueCookieName`

  Default value is `sunIdentityServerAuthNServer`. Specifies the cookie name set to the Access Manager server host URL when Access Manager is running against Session Cookie hijacking.

- `com.iplanet.am.auth.ldap.createUserAttrList`

  Specifies a list of user attributes that contain values that will be retrieved from an external Directory Server during LDAP Authentication when the Authentication Service is configured to dynamically create users. The new user created in the local Directory Server will have the values for attributes which have been retrieved from external Directory Server.

  Example: *attribute1*, *attribute2*, *attribute3*

Certificate Database

Set these properties to initialize the JSS Socket Factory when iPlanet Web Server is configured for SSL.

- `com.iplanet.am.admin.cli.certdb.dir`

  Value is set during installation. Example: `/opt/SUNWwbsvr/alias`

  Specifies certificate database path.

- `com.iplanet.am.admin.cli.certdb.passfile`

  Value is set during installation. Example: `/etc/opt/SUNWam/config/.wtpass`

  Specifies certificate database password file.

- `com.iplanet.am.admin.cli.certdb.prefix`

  Value is set during installation. Example: `https-`*hostName.domainName*`.com-`*hostName*`-`

  Specifies certificate database prefix.

Cookies

- `com.iplanet.am.cookie.encode`

  This property allows Access Manager to `URLencode` the cookie value which converts characters to ones that are understandable by HTTP.

  Value is set during installation. Example: `false`

- `com.iplanet.am.cookie.name`

  Default value is `iPlanetDirectoryPro`. Cookie name used by Authentication Service to set the valid session handler ID. The value of this cookie name is used to retrieve the valid session information.

- `com.iplanet.am.cookie.secure`

Allows the Access Manager cookie to be set in a secure mode in which the browser will only return the cookie when a secure protocol such as `HTTP(s)` is used.

Default value is `false`.

- `com.iplanet.am.console.remote`

  Value is set during installation. Example: `false`

  Determines whether the console is installed on a remote machine, or is installed on a local machine and will be used by authentication console.

- `com.iplanet.am.pcookie.name`

  Specifies the cookie name for a persistent cookie. A persistent cookie continues to exist after the browser window is closed. This enables a user to log in with a new browser session without having to reauthenticate. Default value is `DProPCookie`.

- `com.sun.identity.cookieRewritingInPath`

  Default value is `true`. This property is read by the Authentication Service when Access Manager is configured to run in cookieless mode. The property specifies that the cookie needs to be rewritten as extra path information in the URL using this form: `protocol://server:port/uri;`*cookiename*`=cookieValue?queryString`. If this property is not specified, then the cookie will be written as part of the query string.

- `com.sun.identity.enableUniqueSSOTokenCookie`

  Default value is `false`. Indicates that Access Manager is running against Session Cookie hijacking when the value is set to `true`.

Debugging

- `com.iplanet.services.debug.directory`

  Specifies the output directory where debug files will be created. Value is set during installation. Example: `/var/opt/SUNWam/debug`

- `com.iplanet.services.debug.level`

  Specifies debug level. Default value is `error`. Possible values are:

`off`	No debug file is created.
`error`	Only error messages are logged.
`warning`	Only warning messages are logged.
`message`	Error, warning, and informational messages are logged.

Directory Server Installation

- `com.iplanet.am.defaultOrg`

  Value is set at installation. Example: `o=AMRoot`

  Specifies the top-level realm or organization in the Access Manager information tree.
- `com.iplanet.am.directory.host`

  Value is set during installation. Example: *DirectoryServerHost.domainName*.`com`

  Specifies fully-qualified host name of the Directory Server.
- `com.iplanet.am.directory.port`

  Value is set during installation. Example: `389`

  Specifies the Directory Server port number .
- `com.iplanet.am.directory.ssl.enabled`

  Default value is `false`. Indicates if Security Socket Layer (SSL) is enabled.
- `com.iplanet.am.domaincomponent`

  Value is set during installation. Example: `o=AMRoot`

  Specifies the domain component (dc) attribute for the Access Manager information tree.
- `com.iplanet.am.rootsuffix`

  Value is set during installation. Example: `o=AMRoot`

Event Connection

- `com.iplanet.am.event.connection.delay.between.retries`

  Default value is 3000. Specifies the delay in milliseconds between retries to re-establish the Event Service connections.
- `com.iplanet.am.event.connection.ldap.error.codes.retries`

  Default values are `80,81,91`. Specifies the LDAP exception error codes for which retries to re-establish Event Service connections will trigger.
- `com.iplanet.am.event.connection.num.retries`

  Default value is `3`. Specifies the number of attempts made to successfully re-establish the Event Service connections.
- `com.sun.am.event.connection.idle.timeout`

  Default value is `0`. Specifies the number of minutes after which the persistent searches will be restarted.

This property is used when a load balancer or firewall is between the policy agents and the Directory Server, and the persistent search connections are dropped when TCP `idle timeout`occurs. The property value should be lower than the load balancer or firewall TCP timeout. This ensures that the persistent searches are restarted before the connections are dropped. A value of `0` indicates that searches will not be restarted. Only the connections that are timed out will be reset.

Global Services Management

- `com.iplanet.am.service.secret`

  Value is set during installation. Example: `AQICPX9e1cxSxB2RSy1WG1+O4msWpt/6djZl`
- `com.iplanet.am.services.deploymentDescriptor`

  Value is set during installation. Example: `/amserver`
- `com.iplanet.services.comm.server.pllrequest.maxContentLength`

  Default value is `16384` or 16k. Specifies the maximum content-length for an `HttpRequest` that Access Manager will accept.
- `com.iplanet.services.configpath`

  Value is set during installation. Example: `/etc/opt/SUNWam/config`

Helper Daemons

- `com.iplanet.am.daemons`

  Default value is `unix securid`. Description
- `securidHelper.ports`

  Default value is `58943`. This property takes a space-separated list and is used for the SecurID authentication module and helpers.
- `unixHelper.ipaddrs`

  Value is set during installation. Specifies a list of IP addresses to be read by the `amserver`script and passed to the UNIX helper when starting the helper. This property can contain a list of space-separated trusted IP Addresses in IPv4 format.
- `unixHelper.port`

  Default value is `58946`. Used in the UNIX Authentication module type.

Identity Federation

- `com.sun.identity.federation.alliance.cache.enabled`

  Default value is `true`. If `true`, federation metadata will be cached internally.

- `com.sun.identity.federation.fedCookieName`

  Default value is `fedCookie`. Specifies the name of the Federation Services cookie.

- `com.sun.identity.federation.proxyfinder`

  Default value is `com.sun.identity.federation.services.FSIDPProxyImpl`. Defines the implementation for finding a preferred identity provider to be proxied.

- `com.sun.identity.federation.services.signingOn`

  Default value is `false`. Specifies the level of signature verification for Liberty requests and responses.

`true`	Liberty requests and responses will be signed when sent, and Liberty requests and responses that are received will be verified for signature validity.
`false`	Liberty requests and responses that are sent and received will not be verified for signature.
`optional`	Liberty requests and responses will be signed or verified only if required by the Federation profiles.

- `com.sun.identity.password.deploymentDescriptor`

  Value is set during installation. Example: `/ampassword`

- `com.sun.identity.policy.Policy.policy_evaluation_weights`

  Default value is `10:10:10`. Indicates the proportional processing cost to evaluate a policy subject, rule, and condition. The values specified influence the order in which the subject, rule, and condition of a policy are evaluated. The value is expressed using three integers which represent a subject, a rule, and a condition. The values are delimited by a colon (:) to indicate the proportional processing cost to evaluate a policy subject, rule, and condition.

- `com.sun.identity.session.application.maxCacheTime`

  Default value is `3`. Specifies the maximum number of minutes for caching time for Application Sessions. By default, the cache does not expire unless this property is enabled.

- `com.sun.identity.sm.ldap.enableProxy`

  The default is false. The purpose of this flag is to report to Service Management that the Directory Proxy must be used for read, write, and/or modify operations to the Directory Server. This flag also determines if ACIs or delegation privileges are to be used.

  This flag must be set to "true" when the Access Manager SDK (from version 7 or 7.1) is communicating with Access Manger version 6.3. For example, in the co-existence/legacy mode this value should be "true". In the legacy DIT, the delegation policies were not

supported. Only ACIs were supported, so o to ensure proper delegation check, this flag must be set to 'true' in legacy mode installation to make use of the ACIs for access control. Otherwise the delegation check will fail.

In realm mode, this value should be set to false so only the delegation policies are used for access control. In version 7.0 and later, Access Manager supports data-agnostic feature in realm mode installation. So, in addition to Directory Server, other servers may be used to store service configuration data.

Additionally, this flag will report to the Service Management feature that the Directory Proxy does not need to be used for the read, write, and/or modify operations to the backend storage. This is because some data stores, like Active Directory, may not support proxy.

- `com.sun.identity.webcontainer`

  Value is set during installation. Example: `WEB_CONTAINER`

  Specifies the name of the of the web container. Although the servlet or JSPs are not web container dependent, Access Manager uses the servlet 2.3 API `request.setCharacterEncoding()` to correctly decode incoming non English characters. These APIs will not work if Access Manager is deployed on Sun Java System Web Server 6.1. Access Manager uses the `gx_charset` mechanism to correctly decode incoming data in Sun Java System Web Server versions 6.1 and S1AS7.0. Possible values `BEA6.1`, `BEA 8.1`, `IBM5.1` or `IAS7.0`. If the web container is Sun Java System Web Server, the tag is not replaced.

JSS Proxy

These properties identify the value for SSL `ApprovalCallback`. If the `checkSubjectAltName` or `resolveIPAddress` feature is enabled, you must create `cert7.db` and `key3.db` with the prefix value of`com.iplanet.am.admin.cli.certdb.prefix` in the `com.iplanet.am.admin.cli.certdb.dir`directory. Then restart Access Manager .

- `com.iplanet.am.jssproxy.checkSubjectAltName`

  Default value is `false`. When enabled, a server certificate includes the Subject Alternative Name (`SubjectAltName`) extension, and Access Manager checks all name entries in the extension. If one of the names in the `SubjectAltName` extension is the same as the server FQDN, Access Manager continues the SSL handshaking. To enable this property, set it to a comma separated list of trusted FQDNs. For example:
  `com.iplanet.am.jssproxy.checkSubjectAltName=`
  `amserv1.example.com,amserv2.example.com`

- `com.iplanet.am.jssproxy.resolveIPAddress`

  Default value is `false`.

- `com.iplanet.am.jssproxy.trustAllServerCerts`

Default value is `false`. If enabled (`true`), Access Manager ignores all certificate-related issues such as a name conflict and continues the SSL handshaking. To prevent a possible security risk, enable this property only for testing purposes, or when the enterprise network is tightly controlled. Avoid enabling this property if a security risk might occur (for example, if a server connects to a server in a different network).

- `com.iplanet.am.jssproxy.SSLTrustHostList`If set, Access Manager checks each server FQDN in the list against the server host in the certificate CN. If there is a FQDNs in the list that is matched with server certificate cn, Access Manager continues the SSL handshaking even if there is "Incorrect Domain name error". Use the following syntax to set the property:

  `com.iplanet.am.jssproxy.SSLTrustHostList =` *fqdn_am_server1* `,`*fqdn_am_server2*`,` *fqdn_am_server3*

- `com.sun.identity.jss.donotInstallAtHighestPriority`

  Default value is `false`. Determines if JSS will be added with highest priority to JCE. Set to `true` if other JCE providers should be used for digital signatures and encryptions.

LDAP Connection

- `com.iplanet.am.ldap.connection.delay.between.retries`

  Default is 1000. Specifies the number milliseconds between retries.

- `com.iplanet.am.ldap.connection.ldap.error.codes.retries`

  Default values are `80,81,91`. Specifies the `LDAPException` error codes for which retries to re-establish the LDAP connection will trigger.

- `com.iplanet.am.ldap.connection.num.retries`

  Default value is `3`. Specifies the number of attempts made to successfully re-establish the LDAP connection.

Liberty Alliance Interactions

- `com.sun.identity.liberty.interaction.htmlStyleSheetLocation`

  Value is set during installation. Example: `/opt/SUNWam/lib/is-html.xsl`

  Specifies path to style sheet that renders the interaction page in HTML.

- `com.sun.identity.liberty.interaction.wmlStyleSheetLocation`

  Value is set during installation. Example: `/opt/SUNWam/lib/is-wml.xsl`

  Specifies path to style sheet that renders the interaction page in WML.

- `com.sun.identity.liberty.interaction.wscSpecifiedInteractionChoice`

Default value is`interactIfNeeded`. Indicates whether a web service consumer participates in an interaction. Allowed values are:

`interactIfNeeded`	Interacts only if required. Also used if an invalid value is specified.
`doNotInteract`	No interaction.
`doNotInteractForData`	No interaction for data.

- `com.sun.identity.liberty.interaction.wscSpecifiedMaxInteractionTime`

  Default value is `80`. Web service consumer's preference on the acceptable duration for interaction. The value is expressed in seconds. The default value is used if the value is not specified or if a non-integer value is specified.

- `com.sun.identity.liberty.interaction.wscWillEnforceHttpsCheck`

  The default value is `yes`. Indicates whether a web service consumer enforces the requirement that a request redirected to a URL uses HTTPS. Valid values are `yes` and `no`. The case is ignored. The Liberty specification requires the value to be `yes`. If no value is specified, the default value is used.

- `com.sun.identity.liberty.interaction.wscWillInlcudeUserInteractionHeader`

  Default value is `yes`. If not value is specified, the default value is used. Indicates whether a web service consumer includes `userInteractionHeader`. Allowable values are `yes` and `no`. The case is ignored.

- `com.sun.identity.liberty.interaction.wscWillRedirect`

  Default value is `yes`. Indicates whether the web service consumer redirects user for interaction. Valid values are `yes` and `no`. If not value is specified, the default value is used.

- `com.sun.identity.liberty.interaction.wspRedirectHandler`

  Value is set during installation. Example:
  `http://`*hostName.domainName*`.com:`*portNumber*`/amserver/WSPRedirectHandler`

  Specifies the URL `WSPRedirectHandlerServlet` uses to handle Liberty WSF WSP-resource owner interactions based on user agent redirects. This should be running in the same JVM where the Liberty service provider is running.

- `com.sun.identity.liberty.interaction.wspRedirectTime`

  Default is `30`. Web service provider's expected duration for interaction. Expressed in seconds. If the value is not specified, or if the value is a non-integer, the default value is used.

- `com.sun.identity.liberty.interaction.wspWillEnforceHttpsCheck`

  Default value is `yes`. If no value is specified, the default value is used. Indicates whether the web service consumer enforces the requirement that `returnToURL`use HTTPS. Valid values are `yes` and `no`. (case ignored) the Liberty specification requires the value to be `yes`.

- `com.sun.identity.liberty.interaction.`

`wspWillEnforceReturnToHostEqualsRequestHost`

The Liberty specification requires the value to be `yes`. Indicates whether the web service consumer enforces that `returnToHost` and `requestHost` are the same. Valid values are`yes` and `no`.

- `com.sun.identity.liberty.interaction.wspWillRedirect`

  Default is `yes`. If no value is specified, the default value is used. Indicates whether a web service provider redirects the user for interaction. Valid values are `yes` and `no`. Case is ignored.

- `com.sun.identity.liberty.interaction.wspWillRedirectForData`

  Default value is `yes`. If no value is specified, the default value is used. Indicates whether the web service provider redirects the user for interaction for data. Valid values are `yes` and `no`. Case is ignored.

- `com.sun.identity.liberty.ws.interaction.enable`

  Default value is `false`.

- `com.sun.identity.liberty.ws.jaxb.namespacePrefixMappingList`

  Default value is

  ```
  =S=http://schemas.xmlsoap.org/soap/envelope/|sb=urn:liberty:sb:2003-08
  |pp=urn:liberty:id-sis-pp:2003-08|ispp=http://www.sun.com/identity/
  liberty/pp|is=urn:liberty:is:2003-08
  ```

  . Specifies the namespace prefix mapping used when marshalling a JAXB content tree to a DOM tree. The syntax is `prefix=namespace|prefix=namespace|...`

- `com.sun.identity.liberty.ws.jaxb.packageList`

  Specifies JAXB package list used when constructing `JAXBContext`. Each package must be separated by a colon (:).

- `com.sun.identity.liberty.ws.security.TokenProviderImpl`

  Default value is `com.sun.identity.liberty.ws.security.AMSecurityTokenProviderDescription`.

- `com.sun.identity.liberty.ws.soap.certalias`

  Value is set during installation. Client certificate alias that will be used in SSL connection for Liberty SOAP Binding.

- `com.sun.identity.liberty.ws.soap.messageIDCacheCleanupInterval`

  Default value is `60000`. Specifies the number of milliseconds to elapse before cache cleanup events begin. Each message is stored in a cache with its own`messageID` to avoid duplicate messages. When a message's current time less the received time exceeds the`staleTimeLimit` value, the message is removed from the cache.

- `com.sun.identity.liberty.ws.soap.staleTimeLimit`

Default value is `300000`. Determines if a message is stale and thus no longer trustworthy. If the message timestamp is earlier than the current timestamp by the specified number of milliseconds, the message the considered to be stale.

- `com.sun.identity.liberty.ws.soap.supportedActors`

  Default value is `http://schemas.xmlsoap.org/soap/actor/next`. Specifies supported SOAP actors. Each actor must be separated by a pipe character (|).

- `com.sun.identity.liberty.ws.ta.certalias`

  Value is set during installation. Specifies certificate alias for the trusted authority that will be used to sign SAML or SAML. BEARER token of response message.

- `com.sun.identity.liberty.ws.wsc.certalias`

  Value is set during installation. Specifies default certificate alias for issuing web service security token for this web service client.

- `com.sun.identity.liberty.ws.ta.certalias`

  Value is set during installation. Specifies certificate alias for trusted authority that will be used to sign SAML or SAML. BEARER token of response message.

- `com.sun.identity.liberty.ws.trustedca.certaliases`

  Value is set during installation.

  Specifies certificate aliases for trusted CA. SAML or SAML BEARER token of incoming request. Message must be signed by a trusted CA in this list. The syntax is
  cert alias 1`[:`*issuer 1*`]|`*cert alias 2*`[:`*issuer 2*`]|.....`
  Example: `myalias1:myissuer1|myalias2|myalias3:myissuer3`.
  The value `issuer` is used when the token doesn't have a `KeyInfo` inside the signature. The issuer of the token must be in this list, and the corresponding certificate alias will be used to verify the signature. If `KeyInfo` exists, the keystore must contain a certificate alias that matches the `KeyInfo` and the certificate alias must be in this list.

- `com.sun.identity.liberty.ws.security.TokenProviderImpl`

  Value is set during installation. Specifies implementation for security token provider.

- `com.sun.identity.saml.removeassertion`

  Default value is `true`. A flag to indicate if de-referenced assertions should be removed from the cache. Applies to assertions that were created associated with artifacts, and have been de-referenced.

Logging Service

- `com.iplanet.am.logstatus`

  Specifies whether logging is turned on (`ACTIVE`) or off (`INACTIVE`). Value is set to `ACTIVE` during installation.

Logging Properties You Can Add to AMConfig.properties

You can configure the degree of detail to be contained in a specific log file by adding attributes to the `AMConfig.properties` file. Use the following format:

`iplanet-am-logging.`*logfileName*`.level=`*java.util.logging.Level* where *logfileName* is the name of a log file for an Access Manager service (see table 1), and*java.util.logging.Level* is an allowable attribute value . Access Manager services log at the INFO level. SAML and Identity Federation services also log at more detailed levels (FINE, FINER, FINEST). Example:

```
iplanet-am-logging.amSSO.access.level=FINER
```

In addition there is a level OFF that can be used to turn off logging, and a level ALL that can be used to enable logging of all messages. Example:

```
iplanet-am-logging.amConsole.access.evel=OFF
```

TABLE 6–1 Access Manager Log Files

Log File Name	Records Logged
`amAdmin.access`	Successful amadmin command-line events
`amAdmin.error`	amadmin command-line error events
`amAuthLog.access`	Access Manager Policy Agent related events. See the Note following this table.
`amAuthentication.access`	Successful authentication events
`amAuthentication.error`	Authentication failures
`amConsole.access`	Console events
`amConsole.error`	Console error events.
`amFederation.access`	Successful Federation events.
`amFederation.error`	Federation error events.
`amPolicy.access`	Storage of policy allow events

TABLE 6–1 Access Manager Log Files *(Continued)*

Log File Name	Records Logged
amPolicy.error	Storage of policy deny events
amSAML.access	Successful SAML events
amSAML.error	SAME error events
amLiberty.access	Successful Liberty events
amLiberty.error	Liberty error events
amSSO.access	Single sign-on creation and destruction
amSSO.error	Single sign-on error events

Note – The amAuthLog filename is determined by the Policy Agent properties in AMAgent.properties. For Web Policy Agents, the property is com.sun.am.policy.agents.config.remote.log. For J2EE Policy Agents, the property is com.sun.identity.agents.config.remote.logfile. The default is amAuthLog.*host.domain.port*, where *host.domain* is the fully-qualified host name of the host running the Policy Agent web server, and where *port* is the port number of that web server. If you have multiple Policy Agents deployed, you can have multiple instances of this file. The property com.sun.identity.agents.config.audit.accesstype (for both Web and J2EE Agents) determines what data is logged remotely. The logged data can include policy allows, policy denies, both allows and denies, or neither allows nor denies.

Naming Service

- com.iplanet.am.naming.failover.url

  This property is no longer being used in Access Manager 7.0.

- com.iplanet.am.naming.url

  Value is set during installation. Example:
  http://*hostName.domainName*.com:*portNumber*/amserver/namingservice

  Specifies the naming service URL to use.

Notification Service

Use the following keys to configure the notification thread pool.

- `com.iplanet.am.notification.threadpool.size`

  Default value is `10`. Defines the size of the pool by specifying the total number of threads.

- `com.iplanet.am.notification.threadpool.threshold`

  Default value is `100`. Specifies the maximum task queue length.

  When a notification task comes in, it is sent to the task queue for processing. If the queue reaches the maximum length, further incoming requests will be rejected along with a `ThreadPoolException`, until the queue has a vacancy.

- `com.iplanet.am.notification.url`

  Value is set during installation. Example:
  `http://`*hostName.domainName*`.com:`*portNumber*`/amserver/notificationservice`

Policy Agents

- `com.iplanet.am.policy.agents.url.deploymentDescriptor`

  Value is set during installation. Example: `AGENT_DEPLOY_URI`

- `com.sun.identity.agents.app.username`

  Default value is `UrlAccessAgent`. Specifies the username to use for the Application authentication module.

- `com.sun.identity.agents.cache.size`

  Default value is 1000. Specifies the size of the resource result cache. The cache is created on the server where the policy agent is installed.

- `com.sun.identity.agents.header.attributes`

  Default values are `cn,ou,o,mail,employeenumber,c`. Specifies the policy attributes to be returned by the policy evaluator. Uses the form `a[,...]`. In this example, `a` is the attribute in the data store to be fetched.

- `com.sun.identity.agents.logging.level`

  Default value is `NONE`. Controls the granularity of the Policy Client API logging level. The default value is `NONE`. Possible values are:

`ALLOW`	Logs `access allowed` requests.
`DENY`	Logs `access denied` requests.
`BOTH`	Logs both `access allowed` and `access denied` requests.
`NONE`	Logs no requests.

- `com.sun.identity.agents.notification.enabled`

Default value is `false`. Enables or disables notifications for the Policy Client API.

- `com.sun.identity.agents.notification.url`

  Used by the policy client SDK to register policy change notifications. A mis-configuration of this property will result in policy notifications being disabled.

- `com.sun.identity.agents.polling.interval`

  Default value is `3`. Specifies the polling interval which is the number of minutes after which an entry is dropped from the Client APIs cache.

- `com.sun.identity.agents.resource.caseSensitive`

  Default value is `false`. Description

  Indicates whether case sensitive is turned on or off during policy evaluation.

- `com.sun.identity.agents.true.value`

  Indicates the true value of a policy action. This value can be ignored if the application does not need to access the `PolicyEvaluator.isAllowed` method. This value signifies how a policy decision from Access Manager should be interpreted. Default value is `allow`.

- `com.sun.identity.agents.resource.comparator.class`

  Default value is `com.sun.identity.policy.plugins.URLResourceName`

  Specifies the resource comparison class name. Available implementation classes are: `com.sun.identity.policy.plugins.PrefixResourceName` and `com.sun.identity.policy.plugins.URLResourceName`.

- `com.sun.identity.agents.resource.delimiter`

  Default value is a backslash (`/`). Specifies the delimiter for the resource name.

- `com.sun.identity.agents.resource.wildcard`

  Default value is `*`. Specifies the wildcard for the resource name.

- `com.sun.identity.agents.server.log.file.name`

  Default value is `amRemotePolicyLog`. Specifies the name of the log file to use for logging messages to Access Manager. Only the name of the file is needed. The directory of the file is determined other Access Manager configuration settings.

- `com.sun.identity.agents.use.wildcard`

  Default value is `true`. Indicates whether to use a wildcard for resource name comparison.

Policy Client API

- `com.sun.identity.policy.client.booleanActionValues`

  `iPlanetAMWebAgentService|POST|allow|deny`

  Default value is `iPlanetAMWebAgentService|GET|allow|deny:`.

  Specifies Boolean action values for policy action names. Uses the form `serviceName|actionName|trueValue|falseValue`. Values for action names are delimited by a colon (:).

- `com.sun.identity.policy.client.cacheMode`

  Default value is `self`. Specifies cache mode for the client policy evaluator. Valid values are `subtree` and `self`. If set to `subtree`, the policy evaluator obtains policy decisions from the server for all the resources from the root of resource actually requested. If set to `self`, the policy evaluator gets the policy decision from the server only for the resource actually requested.

- `com.sun.identity.policy.client.clockSkew`

  Adjusts for time difference between the policy client machine and the policy server. If this property does not exist, and if the policy agent time differs from the policy server time, you occasionally see and incorrect policy decision. You must run a time-syncing service to keep the time on the policy server and on the policy client as close as possible. Use this property to adjust for the small time difference regardless of running time syncing service. Clock skew in seconds = agentTime - serverTime . Comment the property out on the policy server. Uncomment the line and set the appropriate value on the policy client machine or the machine running the policy agent agent-server clock skew (in seconds).

- `com.sun.identity.policy.client.resourceComparators=`

  `serviceType=iPlanetAMWebAgentService|class=`

  Specifies `ResourceComparators` to be used for different service names. Copy the value from the Access Manager console. Go to `Service Configuration` > `PolicyConfiguration` > `Global:ResourceComparator`. Concatenate multiple values from Access Manager using a colon (:) as the delimiter.

- `com.sun.identity.policy.plugins.URLResourceName|wildcard`

  Default value is `*|delimiter=/|caseSensitive=trueDescription`

Profile Service

- `com.iplanet.am.profile.host`

  This property is no longer used in Access Manager 7. It is provided only for backward compatibility. Value is set during installation. Example: *hostName.domainName*`.com`

- `com.iplanet.am.profile.port`

  This property is no longer used in Access Manager 7. It is provided only for backward compatibility. Value is set during installation. Example: `80`

Replication

Use the following keys to configure replication setup.

- `com.iplanet.am.replica.delay.between.retries`

  Default value is `1000`. Specifies the number of milliseconds between retries.
- `com.iplanet.am.replica.num.retries`

  Default value is `0`. Specifies the number of times to retry.

SAML Service

- `com.sun.identity.saml.assertion.version`

  Default value is `1.1`. Specifies default SAML version used. Possible values are 1.0 or 1.1.
- `com.sun.identity.saml.checkcert`

  Default value is `on`. Flag for checking the certificate embedded in the `KeyInfo` against the certificates in the keystore. Certificates in the keystore are specified by the `com.sun.identity.saml.xmlsig.keystore` property. Possible values are: on|off. If the flag is "on", * the certification must be presented in the keystore for * XML signature validation. If the flag is "off", skip * the presence checking. */

  `on` Certification must be presented in the keystore for XML signature validation

  `off` Skips the presence checking.
- `com.sun.identity.saml.protocol.version`

  Default value is `1.1`. Specifies default SAML version used. Possible values are 1.0 or 1.1.
- `com.sun.identity.saml.removeassertion`
- `com.sun.identity.saml.request.maxContentLength`

  Default value is `16384`. Specifies the maximum content-length for an `HTTP Request` that will be used in SAML.
- `com.sun.identity.saml.xmlsig.certalias`

  Default value is `test`. Description
- `com.sun.identity.saml.xmlsig.keypass`

  Value is set during installation. Example: `/etc/opt/SUNWam/config/.keypass`

Specifies the path to the SAML XML key password file.

- `com.sun.identity.saml.xmlsig.keystore`

  Value is set during installation. Example: `/etc/opt/SUNWam/config/keystore.jks`

  Specifies the path to the SAML XML keystore password file.

- `com.sun.identity.saml.xmlsig.storepass`

  Value is set during installation. Example: `/etc/opt/SUNWam/config/.storepass`

  Specifies the path to the SAML XML key storepass file.

Security

- `com.iplanet.security.encryptor`

  Default value is `com.iplanet.services.util.JSSEncryption`. Specifies the encrypting class implementation. Available classes are: `com.iplanet.services.util.JCEEncryption` and `com.iplanet.services.util.JSSEncryption`.

- `com.iplanet.security.SecureRandomFactoryImpl`

  Default value is `com.iplanet.am.util.JSSSecureRandomFactoryImpl`. Specifies the factory class name for `SecureRandomFactory`. Available implementation classes are: `com.iplanet.am.util.JSSSecureRandomFactoryImpl` which uses JSS, and `com.iplanet.am.util.SecureRandomFactoryImpl` which uses pure Java.

- `com.iplanet.security.SSLSocketFactoryImpl`

  Default value is `com.iplanet.services.ldap.JSSSocketFactory`. Specifies the factory class name for `LDAPSocketFactory`. Available classes are: `com.iplanet.services.ldap.JSSSocketFactory` which uses JSS, and `netscape.ldap.factory.JSSESocketFactory` which uses pure Java.

- `com.sun.identity.security.checkcaller`

  Default value is `false`. Enables or disables Java security manager permissions check for Access Manager. Disabled by default. If enabled, then you should make appropriate changes to the Java policy file of the container in which Access Manager is deployed. This way, Access Manager JAR files can be trusted for performing sensitive operations. For more information, see the Java API Reference (Javadoc) entry for `com.sun.identity.security`.

- `am.encryption.pwd`

  Value is set during installation. Example: `dSB9LkwPCSoXfIKHVMhIt3bKgibtsggd`

  Specifies the key used to encrypt and decrypt passwords.

Session Service

- `com.iplanet.am.clientIPCheckEnabled`

  Default value is `false`. Specifies whether or not the IP address of the client is checked in all `SSOToken` creations or validations.

- `com.iplanet.am.session.client.polling.enable`

  This is a READ-ONLY property. Do not modify the property value.

  Default value is `false`. Enables client-side session polling. Please note that the session polling mode and the session notification mode are mutually exclusive. If the polling mode is enabled, the session notification is automatically turned off, and vice versa.

- `com.iplanet.am.session.client.polling.period`

  Default value is `180`. Specifies number of seconds in a polling period.

- `com.iplanet.am.session.httpSession.enabled`

  Default value is `true`. Enables or disables USING `httpSession`.

- `com.iplanet.am.session.invalidsessionmaxtime`

  Default value is `10`. Specifies the number of minutes after which the invalid session will be removed from the session table if it is created and the user does not login. This value should always be greater than the timeout value in the Authentication module properties file.

- `com.iplanet.am.session.maxSessions`

  Default value is `5000`. Specify the maximum number of allowable concurrent sessions.

  Login sends a Maximum Sessions error if the maximum concurrent sessions value exceeds this number.

- `com.iplanet.am.session.protectedPropertiesList`

  Allows you to protect certain core or internal session properties from remote updates via the `SetProperty` method of the Session Service. By setting this "hidden" key security parameter, you can customize session attributes in order to participate in authorization as well as other Access Manager features. To use this parameter:

  1. With a text editor, add the parameter to the `AMConfig.properties` file.
  2. Set the parameter to the session properties that you want to protect. For example:

     ```
     com.iplanet.am.session.protectedPropertiesList =
     PropertyName1,PropertyName2,PropertyName3
     ```

  3. Restart the Access Manager Web container for the values to take effect.

- `com.iplanet.am.session.purgedelay`

  Default value is `60`. Specifies the number of minutes to delay the purge session operation.

After a session times out, this is an extended time period during which the session continues to reside in the session server. This property is used by the client application to check if the session has timed out through SSO APIs. At the end of this extended time period, the session is destroyed. The session is not sustained during the extended time period if the user logs out or if the session is explicitly destroyed by an Access Manager component. The session is in the INVALID state during this extended period.

- `com.sun.am.session.caseInsensitiveDN`

  Default value is `true`. Compares the Agent DN. If the value is `false`, the comparison is case-sensitive.

- `com.sun.am.session.enableHostLookUp`

  Default value is `false`. Enables or disables host lookup during session logging.

SMTP

- `com.iplanet.am.smtphost`

  Default value is `localhost`. Specifies the mail server host.

- `com.iplanet.am.smtpport`

  Default value is `25`. Specifies the mail server port.

Statistics Service

- `com.iplanet.am.stats.interval`

  Default value is `60`. Specifies number of minutes to elapse between statistics logging. Minimum is 5 seconds to avoid CPU saturation. Access Manager assumes any value less than 5 seconds to be 5 seconds.

- `com.iplanet.services.stats.directory`

  Value is set during installation. Example: `/var/opt/SUNWam/stats` Specifies directory where debug files are created.

- `com.iplanet.services.stats.state`

  Default value is `file`. Specifies location of statistics log. Possible values are:

`off`	No statistics are logged.
`file`	Statistics are written to a file under the specified directory.
`console`	Statistics are written into Web Server log files.

CHAPTER 7

serverconfig.xml Reference

The file `serverconfig.xml` provides configuration information for Sun Java™ System Access Manager regarding the Directory Server that is used as its data store. This chapter explains the elements of the file and how to configure it for failover, how can you have multiple instances, how can you un-deploy the console and remove console files from a server. It contains the following sections:

- "Overview" on page 149
- "server-config Definition Type Document" on page 150
- "Failover Or Multimaster Configuration" on page 153

Overview

`serverconfig.xml` is located in `/` *AccessManager-base* `/SUNWam/config/ums`. It contains the parameters used by the Identity SDK to establish the LDAP connection pool to Directory Server. No other function of the product uses this file. Two users are defined in this file: `user1` is a Directory Server proxy user and `user2` is the Directory Server administrator.

Proxy User

The *Proxy User* can take on any user's privileges (for example, the organization administrator or an end user). The connection pool is created with connections bound to the proxy user. Access Manager creates a proxy user with the DN of `cn=puser,ou=DSAME Users,dc=example,dc=com`. This user is used for all queries made to Directory Server. It benefits from a proxy user ACI already configured in the Directory Server and, therefore, can perform actions on behalf of a user when necessary. It maintains an open connection through which all queries are passed (retrieval of service configurations, organization information, etc.). The proxy user password is always encrypted. "Proxy User" on page 149 illustrates where the encrypted password is located in `serverconfig.xml` .

EXAMPLE 7–1 Proxy User In serverconfig.xml

```
<User name="User1" type="proxy">
<DirDN>
cn=puser,ou=DSAME Users,dc=example,dc=com
</DirDN>
<DirPassword>
AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
</DirPassword>
</User>
```

Admin User

`dsameuser` is used for binding purposes when the Access Manager SDK performs operations on Directory Server that are not linked to a particular user (for example, retrieving service configuration information). "Proxy User" on page 149 performs these operations on behalf of `dsameuser`, but a bind must first validate the `dsameuser` credentials. During installation, Access Manager creates `cn=dsameuser,ou=DSAME Users,dc=example,dc=com` . "Proxy User" on page 149 illustrates where the encrypted `dsameuser` password is found in `serverconfig.xml` .

EXAMPLE 7–2 Admin User In serverconfig.xml

```
<User name="User2" type="admin">
<DirDN>
cn=dsameuser,ou=DSAME Users,dc=example,dc=com
</DirDN>
<DirPassword>
AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
</DirPassword>
</User>
```

server-config Definition Type Document

`server-config.dtd` defines the structure for `serverconfig.xml` . It is located in *AccessManager-base* `/SUNWam/dtd`. This section defines the main elements of the DTD. "MiscConfig Element" on page 152 is an example of the `serverconfig.xml` file.

iPlanetDataAccessLayer Element

iPlanetDataAccessLayer is the root element. It allows for the definition of multiple server groups per XML file. Its immediate sub-element is the "ServerGroup Element" on page 151. It contains no attributes.

ServerGroup Element

ServerGroup defines a pointer to one or more directory servers. They can be master servers or replica servers. The sub-elements that qualify the *ServerGroup* include "Server Element" on page 151, "User Element" on page 151, "BaseDN Element" on page 152 and "MiscConfig Element" on page 152. The XML attributes of *ServerGroup* are the name of the server group, and *minConnPool* and *maxConnPool* which define the minimum (1) and maximum (10) connections that can be opened for the LDAP connection pool. More than one defined ServerGroup element is not supported.

Note – Access Manager uses a connection pool to access Directory Server. All connections are opened when Access Manager starts and are not closed. They are reused.

Server Element

Server defines a specific Directory Server instance. It contains no sub-elements. The required XML attributes of *Server* are a user-friendly name for the server, the host name, the port number on which the Directory Server runs, and the type of LDAP connection that must be opened (either simple or SSL).

Note – For an example of automatic failover using the Server element, see "Failover Or Multimaster Configuration" on page 153.

User Element

User contains sub-elements that define the user configured for the Directory Server instance. The sub-elements that qualify *User* include *DirDN* and *DirPassword*. It's required XML attributes are the name of the user, and the type of user. The values for *type* identify the user's privileges and the type of connection that will be opened to the Directory Serverinstance. Options include:

- auth—defines a user authenticated to Directory Server.
- proxy—defines a Directory Server proxy user. See "Proxy User" on page 149 for more information.

- rebind—defines a user with credentials that can be used to rebind.
- admin—defines a user with Directory Server administrative privileges. See "Admin User" on page 150 for more information.

DirDN Element

DirDN contains the LDAP Distinguished Name of the defined user.

DirPassword Element

DirPassword contains the defined user's encrypted password.

Caution – It is important that passwords and encryption keys are kept consistent throughout the deployment. For example, the passwords defined in this element are also stored in Directory Server. If the password is to be changed in one place, it must be updated in both places. Additionally, this password is encrypted. If the encryption key defined in the `am.encryption.pwd` property is changed, all passwords in `serverconfig.xml` must be re-encrypted using `ampassword --encrypt` *password*. .

BaseDN Element

BaseDN defines the base Distinguished Name for the server group. It contains no sub-elements and no XML attributes.

MiscConfig Element

MiscConfig is a placeholder for defining any LDAP JDK features like cache size. It contains no sub-elements. It's required XML attributes are the name of the feature and its defined value.

EXAMPLE 7–3 serverconfig.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!--
 Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.

 Use is subject to license terms.

-->
<iPlanetDataAccessLayer>
        <ServerGroup name="default" minConnPool="1" maxConnPool="10">
                <Server name="Server1" host="
                ishost.domain_name" port="389"
```

EXAMPLE 7–3 serverconfig.xml *(Continued)*

```
type="SIMPLE" />
                <User name="User1" type="proxy">
                        <DirDN>
                                cn=puser,ou=DSAME Users,dc=example,dc=com
                        </DirDN>
                        <DirPassword>
                                AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
                        </DirPassword>
                </User>
                <User name="User2" type="admin">
                        <DirDN>
                                cn=dsameuser,ou=DSAME Users,dc=example,dc=com
                        </DirDN>
                        <DirPassword>
                                AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
                        </DirPassword>
                </User>
                <BaseDN>
                        dc=example,dc=com
                </BaseDN>
        </ServerGroup>
</iPlanetDataAccessLayer>
```

Failover Or Multimaster Configuration

Access Manager allows automatic failover to any Directory Server defined as a "ServerGroup Element" on page 151"Server Element" on page 151 in `serverconfig.xml`. More than one server can be configured for failover purposes or multimasters. If the first configured server goes down, the second configured server will takeover. "Failover Or Multimaster Configuration" on page 153 illustrates `serverconfig.xml` with automatic failover configuration.

EXAMPLE 7–4 Configured Failover in serverconfig.xml

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<!--
PROPRIETARY/CONFIDENTIAL. Use of this product is subject to license terms.
Copyright 2002 Sun Microsystems, Inc. All rights reserved.
-->
<iPlanetDataAccessLayer>
     <ServerGroup name="default" minConnPool="1" maxConnPool="10">
```

EXAMPLE 7–4 Configured Failover in serverconfig.xml *(Continued)*

```
          <Server name="Server1" host="
            amhost1.domain_name" port="389" type="SIMPLE" />
          <Server name="Server2" host="
            amhost2.domain_name" port="389" type="SIMPLE" />
          <Server name="Server3" host="
            amhost3.domain_name" port="390" type="SIMPLE" />
          <User name="User1" type="proxy">
               <DirDN>
                    cn=puser,ou=DSAME Users,dc=example,dc=com
               </DirDN>
               <DirPassword>
                    AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
               </DirPassword>
          </User>
          <User name="User2" type="admin">
               <DirDN>
                    cn=dsameuser,ou=DSAME Users,dc=example,dc=com
               </DirDN>
               <DirPassword>
                    AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
               </DirPassword>
          </User>
          <BaseDN>
               o=isp
          </BaseDN>
     </ServerGroup>
</iPlanetDataAccessLayer>
```

PART IV

Error Codes and Log File Reference

CHAPTER 8

Access Manager Component Error Codes

This appendix provides a list of the error messages generated by Access Manager. While this list is not exhaustive, the information presented in this chapter will serve as a good starting point for common problems. The tables listed in this appendix provide the error code itself, a description and/or probable cause of the error, and describes the actions that can be taken to fix the encountered problem.

This appendix lists error codes for the following functional areas:

- "Access Manager Console Errors" on page 157
- "Authentication Error Codes" on page 159
- "Policy Error Codes" on page 162
- "amadmin Error Codes" on page 163

If you require further assistance in diagnosing errors, please contact Sun Technical Support:

http://www.sun.com/service/sunone/software/index.html

Access Manager Console Errors

The following table describes the error codes generated and displayed by the Access Manager Console.

TABLE 8–1 Access Manager Console Errors

Error Message	Description/Probable Cause	Action
Unable to get attribute from data store.	The object may have been removed by another user prior to being removed by the current user.	Redisplay the objects that you are trying to delete and try the operation again.

TABLE 8–1 Access Manager Console Errors *(Continued)*

Error Message	Description/Probable Cause	Action
Invalid URL	This occurs if the URL for an Access Manager console window is entered incorrectly.	
There are no entities.	The parameters entered in the search window, or in the Filter fields, did not match any objects in the directory.	Run the search again with a different set of parameters
There are no attributes to display.	The selected object does not contain any editable attributes defined in its schema.	
There is no information to display for this service.	The services viewed from the Service Configuration module do not have global or organization based attributes	
Size limit Exceeded. Refine your search to locate more entries.	The parameters specified in the search have returned more entries than are allowed to be returned	Modify the Maximum Results Returned from a Search attribute in the Administration service to a larger value. You can also modify the search parameters to be more restrictive.
Time limit Exceeded. Refine your search to locate more entries.	The search for the specified parameters has taken longer than the allowed search time.	Modify the Timeout for Search attribute in the Administration service to a larger value. You can also modify the search parameters, so they are less restrictive, to return more values.
Invalid user's start location. Please contact your administrator.	The start location DN in the users entry is no longer valid	Edit the properties of the User service and change the value for Administrator DN to a valid DN value.
Could not create identity object. User does not have sufficient access.	An operation was executed by a user with insufficient permissions. The permissions a user has defined determines what operations they can perform.	

Authentication Error Codes

The following table describes the error codes generated by the Authentication service. These errors are displayed to the user/administrator in the Authentication module.

TABLE 8–2 Authentication Error Codes

Error Message	Description/Probable Cause	Action
You are already logged in	The user has already logged in and has a valid session, but there is no Success URL redirect defined.	Either logout, or set up some login success redirect URL(s) through the Access Manager Console. Use the ”goto’ query parameter with the value as Admin Console URL.
Logout Failure	A user is unable to logout of Access Manager.	Restart the server.
Authentication exception	An authentication Exception is thrown due to an incorrect handler	Check the Login URL for any invalid or special characters.
Can non redirect to default page.	Access Manager cannot redirect to Success or Failure redirect URL.	Check the web container’s error log to see if there are any errors.
gotoLoginAfterFail link	This link is generated when most errors occur. The link will send the user to the original Login URL page.	
Invalid password	The password entered is invalid.	Passwords must contain at least 8 characters. Check that the password contains the appropriate amount of characters and ensure that it has not expired.
Authentication failed	. This is the generic error message displayed in the default login failed template. The most common cause is invalid/incorrect credentials.	Enter valid and correct user name/password (the credentials required by the invoked authentication module.)
No user profile was found matching the entered user name in the given organization.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Enter your login information again. If this is your first login attempt, select New User in the login screen.
The password entered does not contain enough characters.	This error is displayed while logging in to the Membership/Self-registration authentication module.	The login password must contain at least 8 characters by default (this number is configurable through the Membership Authentication module).

TABLE 8–2 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
A user already exists with this name in the given organization.	This error is displayed while logging in to the Membership/Self-registration authentication module.	User IDs must be unique within the organization.
The User Name and Password fields cannot have the same value.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure that the username and password are different.
No user name was entered	.This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure to enter the user name.
No password was entered.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure to enter the password.
Missing the confirmation password field.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure to enter the password in the Confirm Password field.
The password and the confirm password do not match.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure that the password and confirmation password match.
An error occurred while storing the user profile.	This error is displayed while logging in to the Membership/Self-registration authentication module.	Make sure that the attributes and elements are valid and correct for Self Registration in the `Membership.xml` file.
This organization is not active	The organization is not active.	Activate the organization through the Access Manager console by changing the organization status from `inactive` to `active`.
Internal Authentication Error.	This is a generic Authentication error which may be caused by different and multiple environmental and/or configuration issues.	

TABLE 8–2 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
User is not active	The user no longer has an active status.	Activate the user through the Admin Console by changing the user status from `inactive` to `active`. if the user is locked out by Memory Locking, restart the server.
User does not belong to the specified role.	This error is displayed during role-based authentication.	Make sure that the login user belongs to the role specified for the role-based authentication.
User session has timed out.	The user session has timed out.	Login in again.
Specified authentication module is denied.	The specified authentication module is denied.	Make sure that the required authentication module is registered under the required organization, that the template is created and saved for the module, and that the module is selected in the Organization Authentication Modules list in the Core Authentication module.
No configuration found	The configuration for the authentication module was not found.	Check the Authentication Configuration service for the required authentication method.
Persistent Cookie Username does not exist	Persistent Cookie Username does not exist in the Persistent Cookie Domain.	
No organization found.	The organization was not found.	Make sure that the requested organization is valid and correct.
User has no profile in the specified organization.	User has no profile in the specified organization.	Make sure that the user exists and is valid in the specified organization in the local Directory Server.
One of the required fields was not completed.	One of the required fields was not completed.	Make sure that all required fields are entered.
Maximum Session Limit was reached	The maximum sessions limit was reached.	Logout and login again.

Policy Error Codes

The following table describes the error codes generated by the Policy framework and displayed in the Access Manager Console.

TABLE 8–3 Policy Error Codes

Error Message	Description/Probable Cause	Action
Illegal character "/" in the policy name	There was an illegal character "/" in the policy name.	Make sure that the policy name does not contain the "/' character.
A rule with the same name already exists	A rule with the same name already exists within the realm.	Use a different name for policy creation.
Another rule with the given name already exists	Another rule with the given name already exists	Use a different rule name for policy creation.
A rule with the same rule value already exists	A rule with the same rule value already exists within the policy.	Use a different rule value.
No referral exists to the realm.	No referral exists to the realm.	In order to create policies under a sub realm, you must create a referral policy at its parent realm to indicate what resources can be referred to this sub realm
LDAP search size limit exceeded.	An error occurred because the search found more than the maximum number of results.	Change the search pattern or policy configuration of the organization for the search control parameters.T he Search Size Limit is located in the Policy Configuration service.
LDAP search time limit exceeded.	An error occurred because the search found more than the maximum number of results.	Change the search pattern or policy configuration of the organization for the search control parameters. The Search Time Limit is located in the Policy Configuration service.
Invalid LDAP Bind password.	Invalid LDAP Bind password.	The password for LDAP Bind user defined in Policy Configuration is incorrect. This leads to the inability to get an authenticated LDAP connection to perform policy operations.

TABLE 8–3 Policy Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
Application SSO token is invalid	The server could not validate the Application SSO token. Most likely the SSO token is expired.	Enter the authentication credentials again.
User SSO token is invalid.	The server could not validate the User SSO token. Most likely the SSO token is expired.	User must reauthenticate..
Property value not an integer	The property value not an integer.	The value for this plugin's property should be an integer.
Property Value not defined	Property value should be defined.	Provide a value for the given property.
Start IP is larger than End IP	Start IP is larger than End IP for the policy's condition.	An attempt was made to set end IP Address to be larger than start IP Address in IP Address condition. The Start IP cannot be larger than the End IP.
Start Date is larger than End Date	Start date is larger than end date for the policy's condition.	An attempt was made to set end Date to be larger than start Date in the policy's Time Condition. The Start Date cannot be larger than the End Date.
Policy not found in realm.	An error occurred trying to locate a non-existing policy in a realm	Make sure that the policy exists under the specified realm.
User does not have sufficient access.	The user does not have sufficient right to perform policy operations.	Perform policy operations with the user who has appropriate access rights.
Invalid LDAP Server host.	The LDAP Server Host attribute value is invalid.	Change the invalid LDAP Server host that was entered in the Policy Configuration service.

amadmin Error Codes

The following table describes the error codes generated by the `amadmin` command line tool to Access Manager's debug file.

TABLE 8–4 amadmin error codes

Code	Description/Probable Cause	Action
1	Too few arguments.	Make sure that the mandatory arguments (`--runasdn`, `--password`, `--passwordfile`, `--schema`, `--data`, and `--addattributes`) and their values are supplied in the command line.
2	The input XML file was not found.	Check the syntax and make sure that the input XML is valid.
3	The user DN for the `--runasdn` value is missing.	Provide the user DN as the value for `--runasdn`.
4	The service name for the `--deletservice` value is missing.	Provide the service name as the value for `--deleteservice`.
5	The password for the `--password` value is missing.	Provide the password as the value for `--password`.
6	The locale name was not provided. The locale will default to en_US.	See the Online Help for a list of locales.
7	Missing XML input file.	Provide at least one input XML filename to process.
8	One or more arguments are incorrect.	Check that all arguments are valid. For a set of valid arguments, type `amadmin --help`.
9	Operation failed.	When `amadmin` fails, it produces more precise error codes to indicate the specific error. Refer to those error codes to evaluate the problem.
10	Cannot process requests.	When `amadmin` fails, it produces more precise error codes to indicate the specific error. Refer to those error codes to evaluate the problem.
12	Policy cannot be created.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
13	Policy cannot be deleted.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
14	Service cannot be deleted.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
15	Cannot authenticate user.	Make sure the user DN and password are correct.
16	Cannot parse the input XML file.	Make sure that the XML is formatted correctly and adheres to the `amAdmin.dtd`.

TABLE 8–4 amadmin error codes *(Continued)*

Code	Description/Probable Cause	Action
17	Cannot parse due to an application error or a parser initialization error.	Make sure that the XML is formatted correctly and adheres to the `amAdmin.dtd`.
18	Cannot parse because a parser with specified options cannot be built.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
19	Cannot read the input XML file.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
20	Cannot parse because the XML file is not a valid file.	Check the syntax and make sure that the input XML is valid.
21	Cannot parse because the XML file is not a valid file.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
22	XML file validation warnings for the file.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
23	Cannot process the XML file.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
24	Neither `--data` or `--schema` options are in the command.	Check that all arguments are valid. For a set of valid arguments, type `amadmin --help`.
25	The XML file does not follow the correct DTD.	Check the XML file for the `DOCTYPE` element.
26	LDAP Authentication failed due to invalid DN, password, hostname, or portnumber.	Make sure the user DN and password are correct.
28	Service Manager exception (SSO exception).	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
29	Service Manager exception.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
30	Schema file inputstream exception.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.

TABLE 8–4 amadmin error codes *(Continued)*

Code	Description/Probable Cause	Action
31	Policy Manager exception (SSO exception).	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
32	Policy Manager exception.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
33	More than one debug option is specified.	Only one debug option should be specified.
34	Login failed.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
36	Invalid attribute value.	Check the level set for the LDAP search. It should be either `SCOPE_SUB` or `SCOPE_ONE`.
37	Error in getting object type.	Make sure that the DN in the XML file is value and contains the correct object type.
38	Invalid organization DN.	Make sure that the DN in the XML file is valid and is an organization object.
39	Invalid role DN.	Make sure that the DN in the XML file is valid and is a role object.
40	Invalid static group DN.	Make sure that the DN in the XML file is valid and is a static group object.
41	Invalid people container DN.	Make sure the DN in the XML file is valid and is a people container object.
42	Invalid organizational unit DN.	Make sure that the DN in the XML file is valid and is a container object.
43	Invalid service host name.	Make sure that the hostname for retrieving valid sessions is correct.
44	Subschema error.	Subcschema is only supported for global and organization attributes.
45	Cannot locate service schema for service.	Make sure that the sub schema in the XML file is valid.
46	The role template can be true only if the schema type is dynamic.	Make sure that the role template in the XML file is valid.
47	Cannot add users to a filtered role.	Made sure that the role DN in the XML file is not a filtered role.
48	Template does not exist.	Make sure that the service template in the XML file is valid.

TABLE 8–4 amadmin error codes *(Continued)*

Code	Description/Probable Cause	Action
49	Cannot add users to a dynamic group.	Made sure that the group DN in the XML file is not a dynamic group.
50	Policies can not be created in an organization that is a child organization of a container.	Make sure that the organization in which the policy is to be created is not a child of a container.
51	The group container was not found.	Create a group container for the parent organization or container.
52	Cannot remove a user from a filtered role.	Make sure that the role DN in the XML file is not filtered role.
53	Cannot remove users from a dynamic group.	Make sure that the group DN in the XML file is not a dynamic group.
54	The subschema string does not exist.	Make sure that the subschema string exists in the XML file.
59	You are trying to add user to an organization or container. And default people container does not exists in an organization or container.	Make sure the default people container exists.
60	Default URL prefix is not found following --defaultURLPrefix argument	provide the default URL prefix accordingly.
61	Meta Alias is not found following --metaalias argument	provide the Meta Alias accordingly.
62	Entity Name is not specified.	provide the entity name.
63	File name for importing meta data is missing.	provide the file name that contains meta data.
64	File name for storing exported meta data is missing.	provide the file name for storing meta data.
65	Unable to get a handler to Meta attribute. Specified user name and password may be incorrect.	ensure that user name and password are correct.
66	Missing resource bundle name when adding, viewing or deleting resource bundle that is store in directory server.	provide the resource bundle name
67	Missing file name of file that contains the resource strings when adding resource bundle to directory server.	Please provide a valid file name.

TABLE 8–4 amadmin error codes *(Continued)*

Code	Description/Probable Cause	Action
68	Failed to load liberty meta to Directory Server.	Please check the meta data again before loading it again

CHAPTER 9

Access Manager Log File Reference

This appendix lists the possible log files for each area of Access Manager functionality. The tables in this appendix document the following log file items:

- Id — The log identification number.
- Log Level — The Log Level attribute for the message.
- Description — A description of the logging message.
- Data — The data type to which the message pertains.
- Triggers — Reason for the log file message.
- Actions — Actions for you to take to gain more information.

Definitions and locations and of the log files are described in the *Sun Java System Access Manager 7.1 Technical Overview*.

Log Reference for amadmin Command Line Utility

TABLE 9–1 Log Reference Document for Amadmin_CLI

Id	Log Level	Description	Data	Triggers	Actions
1	INFO	Unsuccessful login for user.	user id	Unsuccessful login for user.	
2	INFO	ADMINEXCEPTION Received	Element name error message	Received ADMINEXCEPTION while processing Admin request(s).	Look in OpenAdmin debug file for more information.
3	INFO	Session destroyed	name of user	Session destroyed.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
11	INFO	Service Schema Loaded	schema name	Successfully loaded service schema.	
12	INFO	Service deleted	service name	Successfully deleted service.	
13	INFO	Attributes Added	attribute name	Attributes successfully added.	
21	INFO	There are no policies for this service	service name	Delete Policy Rule Flag specified, but service has no policies.	
22	INFO	Policy Schema for Service not found	service name	Delete Policy Rule Flag specified, but could not find the policy schema for the service	
23	INFO	Deleting Policies For Service	service name	Deleting Service with Delete Policy Rule Flag specified.	
24	INFO	Done Deleting Policies For Service	service name	Deleting Service with Delete Policy Rule Flag specified.	
25	INFO	Created Policy in Organization	policy name organization DN	Created Policy in Organization DN.	
26	INFO	Deleted Policy from Organization	policy name organization DN	Deleted Policy from Organization DN.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
31	INFO	Add Resource Bundle of Locale to Directory Server	resource bundle name resource locale	Resource Bundle of Locale successfully stored in Directory Server.	
32	INFO	Add Default Resource Bundle to Directory Server	resource bundle name	Default Resource Bundle successfully stored in Directory Server.	
33	INFO	Deleted Resource Bundle of Locale from Directory Server	resource bundle name resource locale	Successfully deleted Resource Bundle of Locale from Directory Server.	
34	INFO	Deleted Default Resource Bundle of Locale from Directory Server	resource bundle name	Successfully deleted default Resource Bundle from Directory Server.	
41	INFO	Modified Service Schema of service	name of service	Successfully modified Service Schema of service.	
42	INFO	Deleted Service Sub Schema of service	name of sub schema name of service	Successfully deleted service sub schema of service.	
43	INFO	Added Service Sub Schema to service.	name of service	Successfully added service sub schema to service.	
44	INFO	Added Sub Configuration to service.	name of sub configuration name of service	Successfully added sub configuration to service.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
45	INFO	Modified Sub Configuration of service	name of sub configuration name of service	Successfully modified sub configuration of service.	
46	INFO	Deleted Sub Configuration of service	name of sub configuration name of service	Successfully deleted sub configuration of service.	
47	INFO	Deleted all Service Configurations of service.	name of service	Successfully deleted all service configurations of service.	
91	INFO	Modify Service SubConfiguration in Organization	subconfiguration name service name organization DN	Successfully Modified Service SubConfiguration in Organization.	
92	INFO	Added Service SubConfiguration in Organization	subconfiguration name service name organization DN	Successfully Added Service SubConfiguration in Organization.	
93	INFO	Deleted Service SubConfiguration in Organization	subconfiguration name service name organization DN	Successfully Deleted Service SubConfiguration in Organization.	
94	INFO	Created remote provider in organization	provider name organization DN	Successfully created remote provider in organization.	
95	INFO	Modified remote provider in organization	provider name organization DN	Successfully modified remote provider in organization.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
96	INFO	Modified hosted provider in organization	provider name organization DN	Successfully modified hosted provider in organization.	
97	INFO	Created hosted provider in organization	provider name organization DN	Successfully created hosted provider in organization.	Look under identity repository log for more information.
98	INFO	Deleted Remote Provider in organization	provider name organization DN	Successfully Deleted Remote Provider in organization.	
99	INFO	Created Authentication Domain in organization	name of circle of trust organization DN	Successfully Created Authentication Domain in 0rganization.	
100	INFO	Deleted Authentication Domain in organization.	name of circle of trust organization DN	Successfully Deleted Authentication Domain in 0rganization.	
101	INFO	Modified Authentication Domain in organization.	name of circle of trust organization DN	Successfully Modified Authentication Domain in 0rganization.	
102	INFO	Attempt to modify service template	DN of service template	Attempted to modify service template.	
103	INFO	Modified service template	DN of service template	Successfully modified service template.	
104	INFO	Attempt to remove service template	DN of service template	Attempted to remove service template.	
105	INFO	Removed service template	DN of service template	Successfully removed service template.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
106	INFO	Attempt to add service template	DN of service template	Attempted to add service template.	
107	INFO	Added service template	DN of service template	Successfully added service template.	
108	INFO	Attempt to add nested groups to group	name of group to add DN of containing group	Attempted to add nested groups to group.	
109	INFO	Added nested groups to group	name of group to add DN of containing group	Successfully added nested groups to group.	
110	INFO	Attempt to add user to group or role	name of user target group or role	Attempted to add user to group or role.	
111	INFO	Added user to group or role	name of user target group or role	Successfully added user to group or role.	
112	INFO	Attempt to create entity.	localized name of entity DN of entity container where entity is to be created	Attempted to Create entity.	
113	INFO	Created entity.	localized name of entity DN of entity	Created entity.	
114	INFO	Attempt to create role	role DN container where role is to be created	Attempted to create role.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
115	INFO	Created role	name of role	Created role.	
116	INFO	Attempt to create group container	name of group container container where group container is to be created.	Attempted to create group container.	
117	INFO	Create group container	name of group container	Created group container.	
118	INFO	Attempt to create group.	name of group type of group container where group is to be created.	Attempted to create group.	
119	INFO	Create group.	name of group	Created group.	
120	INFO	Attempt to create people container.	DN of people container container where people container is to be created.	Attempted to create people container.	
121	INFO	Create people container.	DN of people container	Created people container.	
122	INFO	Attempt to create service template in organization or role	name of service template name of organization or role	Attempted to create service template in organization or role.	
123	INFO	Create service template in organization or role	name of service template name of organization or role	Created service template in organization or role.	
124	INFO	Attempt to create container	name of container container where container is to be created.	Attempted to create container.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
125	INFO	Create container	name of container	Created container.	
126	INFO	Attempt to create user.	name of user organization, organizational unit or people container where user is to be created in.	Attempted to create user.	
127	INFO	Create user.	name of user	Created user.	
128	INFO	Attempt to delete entity.	DN of entity	Attempted to delete entity.	
129	INFO	Delete entity.	localized name of entity DN of entity	Deleted entity.	
130	INFO	Attempt to delete people container	DN of people container	Attempted to delete people container.	
131	INFO	Delete people container	DN of people container	Deleted people container.	
132	INFO	Attempt to delete role	name of role	Attempted to delete role.	
133	INFO	Delete role	name of role	Deleted role.	
134	INFO	Attempt to delete service template in organization	name of service template name of organization	Attempted to delete service template in organization.	
135	INFO	Delete service template in organization	name of service template name of organization	Deleted service template in organization.	
136	INFO	Attempt to delete container.	name of container	Attempted to delete container.	
137	INFO	Delete container.	name of container	Deleted container.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
138	INFO	Attempt to modify entity	localized name of entity DN of entity	Attempted to modify entity.	
139	INFO	Modify entity	localized name of entity DN of entity	Modified entity.	
140	INFO	Attempt to modify people container.	DN of people container	Attempted to modify people container.	
141	INFO	Modify people container.	DN of people container	Modified people container.	
142	INFO	Attempt to modify container.	name of container	Attempted to modify container.	
143	INFO	Modify container.	name of container	Modified container.	
144	INFO	Attempt to register service under organization.	name of service name of organization	Attempted to register service under organization	
145	INFO	Register service under organization.	name of service name of organization	Registered service under organization	
146	INFO	Attempt to unregister service under organization.	name of service name of organization	Attempted to unregister service under organization	
147	INFO	Unregister service under organization.	name of service name of organization	Unregistered service under organization	
148	INFO	Attempt to modify group.	name of group	Attempted to modify group	
149	INFO	Modify group.	name of group	Modified group	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
150	INFO	Attempt to remove nested group from group.	name of nested group name of group	Attempted to remove nested group from group.	
151	INFO	Remove nested group from group.	name of nested group name of group	Removed nested group from group.	
152	INFO	Attempt to delete group	name of group	Attempted to delete group.	
153	INFO	Delete group	name of group	Deleted group.	
154	INFO	Attempt to remove a user from a Role	name of user name of role	Attempted to remove a user from a Role.	
155	INFO	Remove a user from a Role	name of user name of role	Removed a user from a Role.	
156	INFO	Attempt to remove a user from a Group	name of user name of group	Attempted to remove a user from a Group.	
157	INFO	Remove a user from a Group	name of user name of group	Removed a user from a Group.	
201	INFO	Attempt to add an Identity to an Identity in a Realm	name of identity to add type of identity to add name of identity to add to type of identity to add to name of realm	Attempted to add an Identity to an Identity in a Realm.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
202	INFO	Add an Identity to an Identity in a Realm	name of identity to add type of identity to add name of identity to add to type of identity to add to name of realm	Added an Identity to an Identity in a Realm.	
203	INFO	Attempt to assign service to an identity in a realm.	name of service name of identity type of identity name of realm	Attempted to assign service to an identity in a realm.	
204	INFO	Assign service to an identity in a realm.	name of service name of identity type of identity name of realm	Assigned service to an identity in a realm.	
205	INFO	Attempt to create identities of a type in a realm.	type of identity name of realm	Attempted to create identities of a type in a realm.	
206	INFO	Create identities of a type in a realm.	type of identity name of realm	Created identities of a type in a realm.	
207	INFO	Attempt to create identity of a type in a realm.	name of identity type of identity name of realm	Attempted to create identity of a type in a realm.	
208	INFO	Create identity of a type in a realm.	name of identity type of identity name of realm	Created identity of a type in a realm.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
209	INFO	Attempt to delete identity of a type in a realm	name of identity type of identity name of realm	Attempted to delete identity of a type in a realm.	
210	INFO	Delete identity of a type in a realm	name of identity type of identity name of realm	Deleted identity of a type in a realm.	
211	INFO	Attempt to modify a service for an Identity in a Realm	name of service type of identity name of identity name of realm	Attempted to modify a service for an Identity in a Realm.	
212	INFO	Modify a service for an Identity in a Realm	name of service type of identity name of identity name of realm	Modified a service for an Identity in a Realm.	
213	INFO	Attempt to remove an Identity from an Identity in a Realm	name of identity to remove type of identity to remove name of identity to remove from type of identity to remove from name of realm	Attempted to remove an Identity from an Identity in a Realm.	
214	INFO	Remove an Identity from an Identity in a Realm	name of identity to remove type of identity to remove name of identity to remove from type of identity to remove from name of realm	Removed an Identity from an Identity in a Realm.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
215	INFO	Attempt to set Service Attributes for an Identity in a Realm	name of service type of identity name of identity name of realm	Attempted to set Service Attributes for an Identity in a Realm.	
216	INFO	Set Service Attributes for an Identity in a Realm	name of service type of identity name of identity name of realm	Set Service Attributes for an Identity in a Realm.	
217	INFO	Attempt to unassign a service from an Identity in a Realm	name of service type of identity name of identity name of realm	Attempted to unassign a service from an Identity in a Realm.	
218	INFO	Unassign a service from an Identity in a Realm	name of service type of identity name of identity name of realm	Unassigned a service from an Identity in a Realm.	
219	INFO	Attempt to create organization	name of organization container where sub organization is to be created	Attempted to create an organization.	
220	INFO	Create organization	name of organization	Created an organization.	
221	INFO	Attempt to delete suborganization.	name of suborganization	Attempted to delete suborganization.	
222	INFO	Delete suborganization.	name of suborganization	Deleted suborganization.	
223	INFO	Attempt to modify role	name of role	Attempted to modify role.	
224	INFO	Modify role	name of role	Modified role.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
225	INFO	Attempt to modify suborganization.	name of suborganization	Attempted to modify suborganization.	
226	INFO	Modify suborganization.	name of suborganization	Modified suborganization.	
227	INFO	Attempt to delete user.	name of user	Attempted to delete user.	
228	INFO	Delete user.	name of user	Deleted user.	
229	INFO	Attempt to modify user.	name of user	Attempted to modify user.	
230	INFO	Modify user.	name of user	Modified user.	
231	INFO	Attempt to add values to a Service Attribute in a Realm.	name of attribute name of service name of realm	Attempted to add values to a Service Attribute in a Realm.	
232	INFO	Add values to a Service Attribute in a Realm.	name of attribute name of service name of realm	Added values to a Service Attribute in a Realm.	
233	INFO	Attempt to assign a Service to a Realm	name of service name of realm	Attempted to assign a Service to a Realm.	
234	INFO	Assign a Service to a Realm	name of service name of realm	Assigned a Service to a Realm.	
235	INFO	Attempt to create a Realm	name of realm created name of parent realm	Attempted to create a Realm.	
236	INFO	Create a Realm	name of realm created name of parent realm	Created a Realm.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
237	INFO	Delete Realm.	recursive or not name of realm deleted	Deleted Realm.	
238	INFO	Delete Realm.	recursive or not name of realm deleted	Deleted Realm.	
239	INFO	Attempt to modify a service in a Realm.	name of service name of realm	Attempted to modify a service in a Realm.	
240	INFO	Modify a service in a Realm.	name of service name of realm	Modified a service in a Realm.	
241	INFO	Attempt to remove an attribute from a service in a Realm	name of attribute name of service name of realm	Attempted to remove an attribute from a service in a Realm.	
242	INFO	Remove an attribute from a service in a Realm	name of attribute name of service name of realm	Removed an attribute from a service in a Realm.	
243	INFO	Attempt to remove values from a service's attribute in a Realm	name of attribute name of service name of realm	Attempted to remove values from a service's attribute in a Realm.	
244	INFO	Remove values from a service's attribute in a Realm	name of attribute name of service name of realm	Removed values from a service's attribute in a Realm.	
245	INFO	Attempt to set attributes for a service in a Realm.	name of service name of realm	Attempted to set attributes for a service in a Realm.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
246	INFO	Set attributes for a service in a Realm.	name of service name of realm	Set attributes for a service in a Realm.	
247	INFO	Attempt to unassign a service from a Realm.	name of service name of realm	Attempted to unassign a service from a Realm.	
248	INFO	Unassign a service from a Realm.	name of service name of realm	Unassigned a service from a Realm.	
249	INFO	Attempt to assign a Service to an Organization Configuration	name of service name of realm	Attempted to assign a Service to an Organization Configuration.	
250	INFO	Assign a Service to an Organization Configuration	name of service name of realm	Assigned a Service to an Organization Configuration.	
251	INFO	Assign a Service to an Organization Configuration Not Done	name of service name of realm	Assigned a Service to an Organization Configuration, but the service is not one of the org config's assignable services.	
252	INFO	Assign a Service to a Realm Not Done	name of service name of realm	Assigned a Service to a Realm, but the service is not one of the realm's assignable services.	
253	INFO	Attempt to unassign a service from an Organization Configuration.	name of service name of realm	Attempted to unassign a service from an Organization Configuration.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
254	INFO	Unassign a service from an Organization Configuration.	name of service name of realm	Unassigned a service from an Organization Configuration.	
255	INFO	Unassign a service not in the Organization Configuration or Realm.	name of service name of realm	Requested to unassign a service not in the Organization Configuration or Realm.	
256	INFO	Attempt to modify a service in an Organization Configuration.	name of service name of realm	Attempted to modify a service in an Organization Configuration.	
257	INFO	Modify a service in an Organization Configuration.	name of service name of realm	Modified a service in an Organization Configuration.	
258	INFO	Modify a service not in the Organization Configuration or Realm.	name of service name of realm	Attempted to modify a service not in the Organization Configuration or Realm.	
259	INFO	Attempt to get privileges of an Identity.	name of realm name of identity type of identity	Attempted to get privileges of an Identity.	
260	INFO	Get privileges of an Identity.	name of realm name of identity type of identity	Gotten privileges of an Identity.	
261	INFO	Attempt to add privileges to an Identity.	name of realm name of identity type of identity	Attempted to add privileges to an Identity.	

TABLE 9–1 Log Reference Document for Amadmin_CLI *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
262	INFO	Added privileges to an Identity.	name of realm name of identity type of identity	Added privileges to an Identity.	
263	INFO	Attempt to remove privileges from an Identity.	name of realm name of identity type of identity	Attempted to remove privileges from an Identity.	
264	INFO	Removed privileges to an Identity.	name of realm name of identity type of identity	Removed privileges from an Identity.	

Log Reference for Authentication

TABLE 9–2 Log Reference Document for Authentication

Id	Log Level	Description	Data	Triggers	Actions
100	INFO	Authentication is Successful	message	User authenticated with valid credentials	
101	INFO	User based authentication is successful	message authentication type user name	User authenticated with valid credentials	
102	INFO	Role based authentication is successful	message authentication type role name	User belonging to role authenticated with valid credentials	
103	INFO	Service based authentication is successful	message authentication type service name	User authenticated with valid credentials to a configured service under realm	

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
104	INFO	Authentication level based authentication is successful	message authentication type authentication level value	User authenticated with valid credentials to one or more authentication modules having authentication level value greater than or equal to specified authentication level	
105	INFO	Module based authentication is successful	message authentication type module name	User authenticated with valid credentials to authentication module under realm	
200	INFO	Authentication Failed	error message	Incorrect/invalid credentials presented User locked out/not active	Enter correct/valid credentials to required authentication module
201	INFO	Authentication Failed	error message	Invalid credentials entered.	Enter the correct password.
202	INFO	Authentication Failed	error message	Named Configuration (Auth Chain) does not exist.	Create and configure a named config for this org.
203	INFO	Authentication Failed	error message	No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
204	INFO	Authentication Failed	error message	This user is not active.	Activate the user.
205	INFO	Authentication Failed	error message	Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
206	INFO	Authentication Failed	error message	User account has expired.	Contact system administrator.
207	INFO	Authentication Failed	error message	Login timed out.	Try to login again.
208	INFO	Authentication Failed	error message	Authentication module is denied.	Configure this module or use some other module.
209	INFO	Authentication Failed	error message	Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
210	INFO	Authentication Failed	error message	Org/Realm does not exists.	Use a valid Org/Realm.
211	INFO	Authentication Failed	error message	Org/Realm is not active.	Activate the Org/Realm.
212	INFO	Authentication Failed	error message	Cannot create a session.	Ensure that session service is configured and maxsession is not reached.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
213	INFO	User based authentication failed	error message authentication type user name	No authentication configuration (chain of one or more authentication modules) configured for user Incorrect/invalid credentials presented User locked out/not active	Configure authentication configuration (chain of one or more authentication modules) for user Enter correct/valid credentials to required authentication module
214	INFO	Authentication Failed	error message authentication type user name	User based Auth. Invalid credentials entered.	Enter the correct password.
215	INFO	Authentication Failed	error message authentication type user name	Named Configuration (Auth Chain) does not exist for this user	Create and configure a named config for this user
216	INFO	Authentication Failed	error message authentication type user name	User based Auth. No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.
217	INFO	Authentication Failed	error message authentication type user name	User based Auth. This user is not active.	Activate the user.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
218	INFO	Authentication Failed	error message authentication type user name	User based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
219	INFO	Authentication Failed	error message authentication type user name	User based Auth. User account has expired.	Contact system administrator.
220	INFO	Authentication Failed	error message authentication type user name	User based Auth. Login timed out.	Try to login again.
221	INFO	Authentication Failed	error message authentication type user name	User based Auth. Authentication module is denied.	Configure this module or use some other module.
222	INFO	Authentication Failed	error message authentication type user name	User based auth. Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
223	INFO	Authentication Failed	error message authentication type user name	User based auth. Org/Realm does not exists.	Use a valid Org/Realm.
224	INFO	Authentication Failed	error message authentication type user name	User based auth. Org/Realm is not active.	Activate the Org/Realm.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
225	INFO	Authentication Failed	error message authentication type user name	User based auth. Cannot create a session.	Ensure that session service is configured and maxsession is not reached.
226	INFO	Role based authentication failed	error message authentication type role name	No authentication configuration (chain of one or more authentication modules) configured for role Incorrect/invalid credentials presented User does not belong to this role User locked out/not active	Configure authentication configuration (chain of one or more authentication modules) for role Enter correct/valid credentials to required authentication module Assign this role to the authenticating user
227	INFO	Authentication Failed	error message authentication type role name	Role based Auth. Invalid credentials entered.	Enter the correct password.
228	INFO	Authentication Failed	error message authentication type role name	Named Configuration (Auth Chain) does not exist for this role.	Create and configure a named config for this role.
229	INFO	Authentication Failed	error message authentication type role name	Role based Auth. No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
230	INFO	Authentication Failed	error message authentication type role name	Role based Auth. This user is not active.	Activate the user.
231	INFO	Authentication Failed	error message authentication type role name	Role based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
232	INFO	Authentication Failed	error message authentication type role name	Role based Auth. User account has expired.	Contact system administrator.
233	INFO	Authentication Failed	error message authentication type role name	Role based Auth. Login timed out.	Try to login again.
234	INFO	Authentication Failed	error message authentication type role name	Role based Auth. Authentication module is denied.	Configure this module or use some other module.
235	INFO	Authentication Failed	error message authentication type role name	Role based auth. Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
236	INFO	Authentication Failed	error message authentication type role name	Role based auth. Org/Realm does not exists.	Use a valid Org/Realm.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
237	INFO	Authentication Failed	error message authentication type role name	Role based auth. Org/Realm is not active.	Activate the Org/Realm.
238	INFO	Authentication Failed	error message authentication type role name	Role based auth. Cannot create a session.	Ensure that session service is configured and maxsession is not reached.
239	INFO	Authentication Failed	error message authentication type role name	Role based auth. User does not belong to this role.	Add the user to this role.
240	INFO	Service based authentication failed	error message authentication type service name	No authentication configuration (chain of one or more authentication modules) configured for service Incorrect/invalid credentials presented User locked out/not active	Configure authentication configuration (chain of one or more authentication modules) for service Enter correct/valid credentials to required authentication module
241	INFO	Authentication Failed	error message authentication type service name	Service based Auth. Invalid credentials entered.	Enter the correct password.
242	INFO	Authentication Failed	error message authentication type service name	Named Configuration (Auth Chain) does not exist with this service name.	Create and configure a named config.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
243	INFO	Authentication Failed	error message authentication type service name	Service based Auth. No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.
244	INFO	Authentication Failed	error message authentication type service name	Service based Auth. This user is not active.	Activate the user.
245	INFO	Authentication Failed	error message authentication type service name	Service based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
246	INFO	Authentication Failed	error message authentication type service name	Service based Auth. User account has expired.	Contact system administrator.
247	INFO	Authentication Failed	error message authentication type service name	Service based Auth. Login timed out.	Try to login again.
248	INFO	Authentication Failed	error message authentication type service name	Service based Auth. Authentication module is denied.	Configure this module or use some other module.
249	INFO	Authentication Failed	error message authentication type service name	Service based Auth. Service does not exist.	Please use only valid Service.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
250	INFO	Authentication Failed	error message authentication type service name	Service based auth. Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
251	INFO	Authentication Failed	error message authentication type service name	Service based auth. Org/Realm does not exists.	Use a valid Org/Realm.
252	INFO	Authentication Failed	error message authentication type service name	Service based auth. Org/Realm is not active.	Activate the Org/Realm.
253	INFO	Authentication Failed	error message authentication type service name	Service based auth. Cannot create a session.	Ensure that session service is configured and maxsession is not reached.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
254	INFO	Authentication level based authentication failed	error message authentication type authentication level value	There are no authentication module(s) having authentication level value greater than or equal to specified authentication level	Configure one or more authentication modules having authentication level value greater than or equal to required authentication level
				Incorrect/invalid credentials presented to one or more authentication modules having authentication level greater than or equal to specified authentication level	Enter correct/valid credentials to one or more authentication modules having authentication level greater than or equal to specified authentication level
				User locked out/not active	
255	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. Invalid credentials entered.	Enter the correct password.
256	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. No Auth Configuration available.	Create an auth configuration.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
257	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.
258	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. This user is not active.	Activate the user.
259	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
260	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. User account has expired.	Contact system administrator.
261	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. Login timed out.	Try to login again.
262	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. Authentication module is denied.	Configure this module or use some other module.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
263	INFO	Authentication Failed	error message authentication type authentication level value	Level based Auth. Invalid Authg Level.	Please specify valid auth level.
264	INFO	Authentication Failed	error message authentication type authentication level value	Level based auth. Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
265	INFO	Authentication Failed	error message authentication type authentication level value	Level based auth. Org/Realm does not exists.	Use a valid Org/Realm.
266	INFO	Authentication Failed	error message authentication type authentication level value	Level based auth. Org/Realm is not active.	Activate the Org/Realm.
267	INFO	Authentication Failed	error message authentication type authentication level value	Level based auth. Cannot create a session.	Ensure that session service is configured and maxsession is not reached.
268	INFO	Module based authentication failed	error message authentication type module name	Module is not registered/configured under realm Incorrect/invalid credentials presented User locked out/not active	Register/configure authentication module under realm Enter correct/valid credentials to authentication module

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
269	INFO	Authentication Failed	error message authentication type module name	Module based Auth. Invalid credentials entered.	Enter the correct password.
270	INFO	Authentication Failed	error message authentication type module name	Module based Auth. No user profile found for this user.	User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.
271	INFO	Authentication Failed	error message authentication type module name	Module based Auth. This user is not active.	Activate the user.
272	INFO	Authentication Failed	error message authentication type module name	Module based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
273	INFO	Authentication Failed	error message authentication type module name	Module based Auth. User account has expired.	Contact system administrator.
274	INFO	Authentication Failed	error message authentication type module name	Module based Auth. Login timed out.	Try to login again.
275	INFO	Authentication Failed	error message authentication type module name	Module based Auth. Authentication module is denied.	Configure this module or use some other module.

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
276	INFO	Authentication Failed	error message authentication type module name	Module based auth. Limit for maximum number of allowed session has been reached.	Logout of a session or increase the limit.
277	INFO	Authentication Failed	error message authentication type module name	Module based auth. Org/Realm does not exists.	Use a valid Org/Realm.
278	INFO	Authentication Failed	error message authentication type module name	Module based auth. Org/Realm is not active.	Activate the Org/Realm.
279	INFO	Authentication Failed	error message authentication type module name	Module based auth. Cannot create a session.	Ensure that session service is configured and maxsession is not reached.
300	INFO	User logout is Successful	message	User logged out	
301	INFO	User logout is successful from user based authentication	message authentication type user name	User logged out	
302	INFO	User logout is successful from role based authentication	message authentication type role name	User belonging to this role logged out	
303	INFO	User logout is successful from service based authentication	message authentication type service name	User logged out of a configured service under realm	

TABLE 9–2 Log Reference Document for Authentication *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
304	INFO	User logout is successful from authentication level based authentication	message authentication type authentication level value	User logged out of one or more authentication modules having authentication level value greater than or equal to specified authentication level	
305	INFO	User logout is successful from module based authentication	message authentication type module name	User logged out of authentication module under realm	

Access Manager Console

TABLE 9–3 Log Reference Document for Console

Id	Log Level	Description	Data	Triggers	Actions
1	INFO	Attempt to create Identity	identity name identity type realm name	Click on create button in Realm Creation Page.	
2	INFO	Creation of Identity succeeded.	identity name identity type realm name	Click on create button in Realm Creation Page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
3	SEVERE	Creation of Identity failed	identity name identity type realm name error message	Unable to create an identity under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
4	SEVERE	Creation of Identity failed	identity name identity type realm name error message	Unable to create an identity under a realm due to data store error.	Look under data store log for more information.
11	INFO	Attempt to search for Identities	base realm identity type search pattern search size limit search time limit	Click on Search button in identity search view.	
12	INFO	Searching for Identities succeeded	base realm identity type search pattern search size limit search time limit	Click on Search button in identity search view.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
13	SEVERE	Searching for identities failed	identity name identity type realm name error message	Unable to perform search operation on identities under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
14	SEVERE	Searching for identities failed	identity name identity type realm name error message	Unable to perform search operation on identities under a realm due to data store error.	Look under data store log for more information.
21	INFO	Attempt to read attribute values of an identity	identity name name of attributes	View identity profile view.	
22	INFO	Reading of attribute values of an identity succeeded	identity name name of attributes	View identity profile view.	
23	SEVERE	Reading of attribute values of an identity failed	identity name name of attributes error message	Unable to read attribute values of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
24	SEVERE	Reading of attribute values of an identity failed	identity name name of attributes error message	Unable to read attribute values of an identity due to data store error.	Look under data store log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
25	SEVERE	Reading of attribute values of an identity failed	identity name name of attributes error message	Unable to read attribute values of an identity due to exception service manager API.	Look under service manage log for more information.
31	INFO	Attempt to modify attribute values of an identity	identity name name of attributes	Click on Save button in identity profile view.	
32	INFO	Modification of attribute values of an identity succeeded	identity name name of attributes	Click on Save button in identity profile view.	
33	SEVERE	Modification of attribute values of an identity failed	identity name name of attributes error message	Unable to modify attribute values of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
34	SEVERE	Modification of attribute values of an identity failed	identity name name of attributes error message	Unable to modify attribute values of an identity due to data store error.	Look under data store log for more information.
41	INFO	Attempt to delete identities	realm name name of identities to be deleted	Click on Delete button in identity search view.	
42	INFO	Deletion of identities succeeded	realm name name of identities to be deleted	Click on Delete button in identity search view.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
43	SEVERE	Deletion of identities failed	realm name name of identities to be deleted error message	Unable to delete identities. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
44	SEVERE	Deletion of identities failed	realm name name of identities to be deleted error message	Unable to delete identities due to data store error.	Look under data store log for more information.
51	INFO	Attempt to read identity's memberships information	name of identity membership identity type	View membership page of an identity.	
52	INFO	Reading of identity's memberships information succeeded	name of identity membership identity type	View membership page of an identity.	
53	SEVERE	Reading of identity's memberships information failed.	name of identity membership identity type error message	Unable to read identity's memberships information. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
54	SEVERE	Reading of identity's memberships information failed.	name of identity membership identity type error message	Unable to read identity's memberships information due to data store error.	Look under data store log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
61	INFO	Attempt to read identity's members information	name of identity members identity type	View members page of an identity.	
62	INFO	Reading of identity's members information succeeded	name of identity members identity type	View members page of an identity.	
63	SEVERE	Reading of identity's members information failed.	name of identity member identity type error message	Unable to read identity's members information. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
64	SEVERE	Reading of identity's members information failed.	name of identity member identity type error message	Unable to read identity's members information due to data store error.	Look under data store log for more information.
71	INFO	Attempt to add member to an identity	name of identity name of identity to be added.	Select members to be added to an identity.	
72	INFO	Addition of member to an identity succeeded	name of identity name of identity added.	Select members to be added to an identity.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
73	SEVERE	Addition of member to an identity failed.	name of identity name of identity to be added. error message	Unable to add member to an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
74	SEVERE	Addition of member to an identity failed.	name of identity name of identity to be added. error message	Unable to add member to an identity due to data store error.	Look under data store log for more information.
81	INFO	Attempt to remove member from an identity	name of identity name of identity to be removed.	Select members to be removed from an identity.	
82	INFO	Removal of member from an identity succeeded	name of identity name of identity removed.	Select members to be removed from an identity.	
83	SEVERE	Removal of member to an identity failed.	name of identity name of identity to be removed. error message	Unable to remove member from an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
84	SEVERE	Removal of member from an identity failed.	name of identity name of identity to be removed. error message	Unable to remove member to an identity due to data store error.	Look under data store log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
91	INFO	Attempt to read assigned service names of an identity	name of identity	Click on Add button in service assignment view of an identity.	
92	INFO	Reading assigned service names of an identity succeeded	name of identity	Click on Add button in service assignment view of an identity.	
93	SEVERE	Reading assigned service names of an identity failed.	name of identity error message	Unable to read assigned service names of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
94	SEVERE	Reading assigned service names of an identity failed.	name of identity error message	Unable to read assigned service names of an identity due to data store error.	Look under data store log for more information.
101	INFO	Attempt to read assignable service names of an identity	name of identity	View the services page of an identity.	
102	INFO	Reading assignable service names of an identity succeeded	name of identity	View the services page of an identity.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
103	SEVERE	Reading assignable service names of an identity failed.	name of identity error message	Unable to read assignable service names of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
104	SEVERE	Reading assignable service names of an identity failed.	name of identity error message	Unable to read assignable service names of an identity due to data store error.	Look under data store log for more information.
111	INFO	Attempt to assign a service to an identity	name of identity name of service	Click Add button of service view of an identity.	
112	INFO	Assignment of service to an identity succeeded	name of identity name of service	Click Add button of service view of an identity.	
113	SEVERE	Assignment of service to an identity failed.	name of identity name of service error message	Unable to assign service to an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
114	SEVERE	Assignment of service to an identity failed.	name of identity name of service error message	Unable to assign service to an identity due to data store error.	Look under data store log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
121	INFO	Attempt to unassign a service from an identity	name of identity name of service	Click Remove button in service view of an identity.	
122	INFO	Unassignment of service to an identity succeeded	name of identity name of service	Click Remove button in service view of an identity.	
123	SEVERE	Unassignment of service from an identity failed.	name of identity name of service error message	Unable to unassign service from an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
124	SEVERE	Unassignment of service from an identity failed.	name of identity name of service error message	Unable to unassign service from an identity due to data store error.	Look under data store log for more information.
131	INFO	Attempt to read service attribute values of an identity	name of identity name of service	View service profile view of an identity.	
132	INFO	Reading of service attribute values of an identity succeeded	name of identity name of service	View service profile view of an identity.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
133	SEVERE	Reading of service attribute values of an identity failed.	name of identity name of service error message	Unable to read service attribute values of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation	Look under data store log for more information.
134	SEVERE	Reading of service attribute values of an identity failed.	name of identity name of service error message	Unable to read service attribute values of an identity due to data store error.	Look under data store log for more information.
141	INFO	Attempt to write service attribute values to an identity	name of identity name of service	Click on Save button in service profile view of an identity.	
142	INFO	Writing of service attribute values to an identity succeeded	name of identity name of service	Click on Save button in service profile view of an identity.	
143	SEVERE	Writing of service attribute values to an identity failed.	name of identity name of service error message	Unable to write service attribute values to an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store log for more information.
144	SEVERE	Writing of service attribute values to an identity failed.	name of identity name of service error message	Unable to write service attribute values to an identity due to data store error.	Look under data store log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
201	INFO	Attempt to read all global service default attribute values	name of service	View global configuration view of a service.	
202	INFO	Reading of all global service default attribute values succeeded	name of service	View global configuration view of a service.	
203	INFO	Attempt to read global service default attribute values	name of service name of attribute	View global configuration view of a service.	
204	INFO	Reading of global service default attribute values succeeded	name of service name of attribute	View global configuration view of a service.	
205	INFO	Reading of global service default attribute values failed	name of service name of attribute	View global configuration view of a service.	Look under service management log for more information.
211	INFO	Attempt to write global service default attribute values	name of service name of attribute	Click on Save button in global configuration view of a service.	
212	INFO	Writing of global service default attribute values succeeded	name of service name of attribute	Click on Save button in global configuration view of a service.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
213	SEVERE	Writing of global service default attribute values failed.	name of service name of attribute error message	Unable to write global service default attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
214	SEVERE	Writing of global service default attribute values failed.	name of service name of attribute error message	Unable to write service default attribute values due to service management error.	Look under service management log for more information.
221	INFO	Attempt to get sub configuration names	name of service name of base global sub configuration	View a global service view of which its service has sub schema.	
222	INFO	Reading of global sub configuration names succeeded	name of service name of base global sub configuration	View a global service view of which its service has sub schema.	
223	SEVERE	Reading of global sub configuration names failed.	name of service name of base global sub configuration error message	Unable to get global sub configuration names. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
224	SEVERE	Reading of global sub configuration names failed.	name of service name of base global sub configuration error message	Unable to get global sub configuration names due to service management error.	Look under service management log for more information.
231	INFO	Attempt to delete sub configuration	name of service name of base global sub configuration name of sub configuration to be deleted	Click on delete selected button in global service profile view.	
232	INFO	Deletion of sub configuration succeeded	name of service name of base global sub configuration name of sub configuration to be deleted	Click on delete selected button in global service profile view.	
233	SEVERE	Deletion of sub configuration failed.	name of service name of base global sub configuration name of sub configuration to be deleted error message	Unable to delete sub configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
234	SEVERE	Deletion of sub configuration failed.	name of service name of base global sub configuration name of sub configuration to be deleted error message	Unable to delete sub configuration due to service management error.	Look under service management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
241	INFO	Attempt to create sub configuration	name of service name of base global sub configuration name of sub configuration to be created name of sub schema to be created	Click on add button in create sub configuration view.	
242	INFO	Creation of sub configuration succeeded	name of service name of base global sub configuration name of sub configuration to be created name of sub schema to be created	Click on add button in create sub configuration view.	
243	SEVERE	Creation of sub configuration failed.	name of service name of base global sub configuration name of sub configuration to be created name of sub schema to be created error message	Unable to create sub configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
244	SEVERE	Creation of sub configuration failed.	name of service name of base global sub configuration name of sub configuration to be created name of sub schema to be created error message	Unable to create sub configuration due to service management error.	Look under service management log for more information.
251	INFO	Reading of sub configuration's attribute values succeeded	name of service name of sub configuration	View sub configuration profile view.	
261	INFO	Attempt to write sub configuration's attribute values	name of service name of sub configuration	Click on save button in sub configuration profile view.	
262	INFO	Writing of sub configuration's attribute values succeeded	name of service name of sub configuration	Click on save button in sub configuration profile view.	
263	SEVERE	Writing of sub configuration's attribute value failed.	name of service name of sub configuration error message	Unable to write sub configuration's attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
264	SEVERE	Writing of sub configuration's attribute value failed.	name of service name of sub configuration error message	Unable to write sub configuration's attribute value due to service management error.	Look under service management log for more information.
301	INFO	Attempt to get policy names under a realm.	name of realm	View policy main page.	
302	INFO	Getting policy names under a realm succeeded	name of realm	View policy main page.	
303	SEVERE	Getting policy names under a realm failed.	name of realm error message	Unable to get policy names under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under policy log for more information.
304	SEVERE	Getting policy names under a realm failed.	name of realm error message	Unable to get policy names under a realm due to policy SDK related errors.	Look under policy log for more information.
311	INFO	Attempt to create policy under a realm.	name of realm name of policy	Click on New button in policy creation page.	
312	INFO	Creation of policy succeeded	name of realm name of policy	Click on New button in policy creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
313	SEVERE	Creation of policy failed.	name of realm name of policy error message	Unable to create policy under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under policy log for more information.
314	SEVERE	Creation of policy failed.	name of realm name of policy error message	Unable to create policy under a realm due to policy SDK related errors.	Look under policy log for more information.
321	INFO	Attempt to modify policy.	name of realm name of policy	Click on Save button in policy profile page.	
322	INFO	Modification of policy succeeded	name of realm name of policy	Click on Save button in policy profile page.	
323	SEVERE	Modification of policy failed.	name of realm name of policy error message	Unable to modify policy under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under policy log for more information.
324	SEVERE	Modification of policy failed.	name of realm name of policy error message	Unable to modify policy due to policy SDK related errors.	Look under policy log for more information.
331	INFO	Attempt to delete policy.	name of realm names of policies	Click on Delete button in policy main page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
332	INFO	Deletion of policy succeeded	name of realm name of policies	Click on Delete button in policy main page.	
333	SEVERE	Deletion of policy failed.	name of realm name of policies error message	Unable to delete policy. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under policy log for more information.
334	SEVERE	Deletion of policy failed.	name of realm name of policies error message	Unable to delete policy due to policy SDK related errors.	Look under policy log for more information.
401	INFO	Attempt to get realm names	name of parent realm	View realm main page.	
402	INFO	Getting realm names succeeded.	name of parent realm	View realm main page.	
403	SEVERE	Getting realm names failed.	name of parent realm error message	Unable to get realm names due to service management SDK exception.	Look under service management log for more information.
411	INFO	Attempt to create realm	name of parent realm name of new realm	Click on New button in create realm page.	
412	INFO	Creation of realm succeeded.	name of parent realm name of new realm	Click on New button in create realm page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
413	SEVERE	Creation of realm failed.	name of parent realm name of new realm error message	Unable to create new realm due to service management SDK exception.	Look under service management log for more information.
421	INFO	Attempt to delete realm	name of parent realm name of realm to delete	Click on Delete button in realm main page.	
422	INFO	Deletion of realm succeeded.	name of parent realm name of realm to delete	Click on Delete button in realm main page.	
423	SEVERE	Deletion of realm failed.	name of parent realm name of realm to delete error message	Unable to delete realm due to service management SDK exception.	Look under service management log for more information.
431	INFO	Attempt to get attribute values of realm	name of realm	View realm profile page.	
432	INFO	Getting attribute values of realm succeeded.	name of realm	View realm profile page.	
433	SEVERE	Getting attribute values of realm failed.	name of realm error message	Unable to get attribute values of realm due to service management SDK exception.	Look under service management log for more information.
441	INFO	Attempt to modify realm's profile	name of realm	Click on Save button in realm profile page.	
442	INFO	Modification of realm's profile succeeded.	name of realm	Click on Save button in realm profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
443	SEVERE	Modification of realm's profile failed.	name of realm error message	Unable to modify realm's profile due to service management SDK exception.	Look under service management log for more information.
501	INFO	Attempt to get delegation subjects under a realm	name of realm search pattern	View delegation main page.	
502	INFO	Getting delegation subjects under a realm succeeded.	name of realm search pattern	View delegation main page.	
503	SEVERE	Getting delegation subjects under a realm failed.	name of realm search pattern error message	Unable to get delegation subjects. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under delegation management log for more information.
504	SEVERE	Getting delegation subjects under a realm failed.	name of realm search pattern error message	Unable to get delegation subjects due to delegation management SDK related errors.	Look under delegation management log for more information.
511	INFO	Attempt to get privileges of delegation subject	name of realm ID of delegation subject	View delegation subject profile page.	
512	INFO	Getting privileges of delegation subject succeeded.	name of realm ID of delegation subject	View delegation subject profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
513	SEVERE	Getting privileges of delegation subject failed.	name of realm ID of delegation subject error message	Unable to get privileges of delegation subject. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under delegation management log for more information.
514	SEVERE	Getting privileges of delegation subject failed.	name of realm ID of delegation subject error message	Unable to get privileges of delegation subject due to delegation management SDK related errors.	Look under delegation management log for more information.
521	INFO	Attempt to modify delegation privilege	name of realm ID of delegation privilege ID of subject	Click on Save button in delegation subject profile page.	
522	INFO	Modification of delegation privilege succeeded.	name of realm ID of delegation privilege ID of subject	Click on Save button in delegation subject profile page.	
523	SEVERE	Modification of delegation privilege failed.	name of realm ID of delegation privilege ID of subject error message	Unable to modify delegation privilege. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under delegation management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
524	SEVERE	Modification of delegation privilege failed.	name of realm ID of delegation privilege ID of subject error message	Unable to modify delegation privilege due to delegation management SDK related errors.	Look under delegation management log for more information.
601	INFO	Attempt to get data store names	name of realm	View data store main page.	
602	INFO	Getting data store names succeeded.	name of realm	View data store main page.	
603	SEVERE	Getting data store names failed.	name of realm error message	Unable to get data store names. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
604	SEVERE	Getting data store names failed.	name of realm error message	Unable to get data store names due to service management SDK exception.	Look under service management log for more information.
611	INFO	Attempt to get attribute values of identity repository	name of realm name of identity repository	View data store profile page.	
612	INFO	Getting attribute values of data store succeeded.	name of realm name of identity repository	View data store profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
613	SEVERE	Getting attribute values of data store failed.	name of realm name of identity repository error message	Unable to get attribute values of identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
614	SEVERE	Getting attribute values of data store failed.	name of realm name of identity repository error message	Unable to get attribute values of data store due to service management SDK exception.	Look under service management log for more information.
621	INFO	Attempt to create identity repository	name of realm name of identity repository type of identity repository	Click on New button in data store creation page.	
622	INFO	Creation of data store succeeded.	name of realm name of identity repository type of identity repository	Click on New button in data store creation page.	
623	SEVERE	Creation of data store failed.	name of realm name of identity repository type of identity repository error message	Unable to create identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
624	SEVERE	Creation data store failed.	name of realm name of identity repository type of identity repository error message	Unable to create data store due to service management SDK exception.	Look under service management log for more information.
631	INFO	Attempt to delete identity repository	name of realm name of identity repository	Click on Delete button in data store main page.	
632	INFO	Deletion of data store succeeded.	name of realm name of identity repository	Click on Delete button in data store main page.	
633	SEVERE	Deletion of data store failed.	name of realm name of identity repository error message	Unable to delete identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
634	SEVERE	Deletion data store failed.	name of realm name of identity repository error message	Unable to delete data store due to service management SDK exception.	Look under service management log for more information.
641	INFO	Attempt to modify identity repository	name of realm name of identity repository	Click on Save button in data store profile page.	
642	INFO	Modification of data store succeeded.	name of realm name of identity repository	Click on Save button in data store profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
643	SEVERE	Modification of data store failed.	name of realm name of identity repository error message	Unable to modify identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
644	SEVERE	Modification data store failed.	name of realm name of identity repository error message	Unable to modify data store due to service management SDK exception.	Look under service management log for more information.
701	INFO	Attempt to get assigned services of realm	name of realm	View realm's service main page.	
702	INFO	Getting assigned services of realm succeeded.	name of realm	View realm's service main page.	
703	SEVERE	Getting assigned services of realm failed.	name of realm error message	Unable to get assigned services of realm due authentication configuration exception.	Look under authentication log for more information.
704	SEVERE	Getting assigned services of realm failed.	name of realm error message	Unable to get assigned services of realm due to service management SDK exception.	Look under service management log for more information.
705	SEVERE	Getting assigned services of realm failed.	name of realm error message	Unable to get assigned services of realm due to data store SDK exception.	Look under service management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
706	SEVERE	Getting assigned services of realm failed.	name of realm error message	Unable to get assigned services of realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
711	INFO	Attempt to get assignable services of realm	name of realm	View realm's service main page.	
712	INFO	Getting assignable services of realm succeeded.	name of realm	View realm's service main page.	
713	SEVERE	Getting assignable services of realm failed.	name of realm error message	Unable to get assignable services of realm due authentication configuration exception.	Look under authentication log for more information.
714	SEVERE	Getting assignable services of realm failed.	name of realm error message	Unable to get assignable services of realm due to service management SDK exception.	Look under service management log for more information.
715	SEVERE	Getting assignable services of realm failed.	name of realm error message	Unable to get assignable services of realm due to ID Repository management SDK exception.	Look under ID Repository management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
716	SEVERE	Getting assignable services of realm failed.	name of realm error message	Unable to get assignable services of realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
721	INFO	Attempt to unassign service from realm	name of realm name of service	Click on Unassign button in realm's service page.	
722	INFO	Unassign service from realm succeeded.	name of realm name of service	Click on Unassign button in realm's service page.	
723	SEVERE	Unassign service from realm failed.	name of realm name of service error message	Unable to unassign service from realm due to service management SDK exception.	Look under service management log for more information.
725	SEVERE	Unassign service from realm failed.	name of realm name of service error message	Unable to unassign service from realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under data store management log for more information.
724	SEVERE	Unassign service from realm failed.	name of realm name of service error message	Unable to unassign service from realm due to data store management SDK exception.	Look under data store management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
731	INFO	Attempt to assign service to realm	name of realm name of service	Click on assign button in realm's service page.	
732	INFO	Assignment of service to realm succeeded.	name of realm name of service	Click on assign button in realm's service page.	
733	SEVERE	Assignment of service to realm failed.	name of realm name of service error message	Unable to assign service to realm due to service management SDK exception.	Look under service management log for more information.
734	SEVERE	Assignment of service to realm failed.	name of realm name of service error message	Unable to assign service to realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
735	SEVERE	Assignment of service to realm failed.	name of realm name of service error message	Unable to assign service to realm due to data store SDK exception.	Look under service management log for more information.
741	INFO	Attempt to get attribute values of service in realm	name of realm name of service name of attribute schema	View realm's service profile page.	
742	INFO	Getting of attribute values of service under realm succeeded.	name of realm name of service name of attribute schema	View realm's service profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
743	SEVERE	Getting of attribute values of service under realm failed.	name of realm name of service name of attribute schema error message	Unable to get attribute values of service due to service management SDK exception.	Look under service management log for more information.
744	INFO	Getting of attribute values of service under realm failed.	name of realm name of service name of attribute schema error message	Unable to get attribute values of service due to data store SDK exception.	Look under service management log for more information.
745	SEVERE	Getting of attribute values of service under realm failed.	name of realm name of service name of attribute schema error message	Unable to get attribute values of service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
751	INFO	Attempt to modify attribute values of service in realm	name of realm name of service	Click on Save button in realm's service profile page.	
752	INFO	Modification of attribute values of service under realm succeeded.	name of realm name of service	Click on Save button in realm's service profile page.	
753	SEVERE	Modification of attribute values of service under realm failed.	name of realm name of service error message	Unable to modify attribute values of service due to service management SDK exception.	Look under service management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
754	SEVERE	Modification of attribute values of service under realm failed.	name of realm name of service error message	Unable to modify attribute values of service due to data store error.	Look under data store log for more information.
755	SEVERE	Modification of attribute values of service under realm failed.	name of realm name of service error message	Unable to modify attribute values of service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation	Look under data store log for more information.
801	INFO	Attempt to get authentication type		View authentication profile page.	
802	INFO	Getting of authentication type succeeded.		View authentication profile page.	
803	SEVERE	Getting of authentication type failed.	error message	Unable to get authentication type due to authentication configuration SDK exception.	Look under authentication management log for more information.
811	INFO	Attempt to get authentication instances under a realm	name of realm	View authentication profile page.	
812	INFO	Getting of authentication instances under a realm succeeded.	name of realm	View authentication profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
813	SEVERE	Getting of authentication instances under a realm failed.	name of realm error message	Unable to get authentication instance due to authentication configuration SDK exception.	Look under authentication management log for more information.
821	INFO	Attempt to remove authentication instances under a realm	name of realm name of authentication instance	View authentication profile page.	
822	INFO	Removal of authentication instances under a realm succeeded.	name of realm name of authentication instance	View authentication profile page.	
823	SEVERE	Removal of authentication instances under a realm failed.	name of realm name of authentication instance error message	Unable to remove authentication instance due to authentication configuration SDK exception.	Look under authentication management log for more information.
831	INFO	Attempt to create authentication instance under a realm	name of realm name of authentication instance type of authentication instance	Click on New button in authentication creation page.	
832	INFO	Creation of authentication instance under a realm succeeded.	name of realm name of authentication instance type of authentication instance	Click on New button in authentication creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
833	SEVERE	Creation of authentication instance under a realm failed.	name of realm name of authentication instance type of authentication instance error message	Unable to create authentication instance due to authentication configuration exception.	Look under authentication configuration log for more information.
841	INFO	Attempt to modify authentication instance	name of realm name of authentication service	Click on Save button in authentication profile page.	
842	INFO	Modification of authentication instance succeeded.	name of realm name of authentication service	Click on Save button in authentication profile page.	
843	SEVERE	Modification of authentication instance failed.	name of realm name of authentication service error message	Unable to modify authentication instance due to service management SDK exception.	Look under service anagement log for more information.
844	SEVERE	Modification of authentication instance failed.	name of realm name of authentication service error message	Unable to modify authentication instance. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
851	INFO	Attempt to get authentication instance profile	name of realm name of authentication instance	View authentication instance profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
852	INFO	Getting of authentication instance profile succeeded.	name of realm name of authentication instance	View authentication instance profile page.	
853	SEVERE	Getting of authentication instance profile failed.	name of realm name of authentication instance error message	Unable to get authentication instance profile due to authentication configuration SDK exception.	Look under authentication management log for more information.
861	INFO	Attempt to modify authentication instance profile	name of realm name of authentication instance	Click on Save button in authentication instance profile page.	
862	INFO	Modification of authentication instance profile succeeded.	name of realm name of authentication instance	Click on Save button in authentication instance profile page.	
863	SEVERE	Modification of authentication instance profile failed.	name of realm name of authentication instance error message	Unable to modify authentication instance profile due to authentication configuration SDK exception.	Look under authentication management log for more information.
864	SEVERE	Modification of authentication instance profile failed.	name of realm name of authentication instance error message	Unable to modify authentication instance profile due to service management SDK exception.	Look under service management log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
864	SEVERE	Modification of authentication instance profile failed.	name of realm name of authentication instance error message	Unable to modify authentication instance profile. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
871	INFO	Attempt to get authentication profile under a realm	name of realm	View authentication profile under a realm page.	
872	INFO	Getting authentication profile under a realm succeeded.	name of realm	View authentication profile under a realm page.	
873	SEVERE	Getting authentication profile under a realm failed.	name of realm error message	Unable to get authentication profile under a realm due to service management SDK exception.	Look under service management log for more information.
881	INFO	Attempt to get authentication configuration profile	name of realm name of authentication configuration	View authentication configuration profile page.	
882	INFO	Getting authentication configuration profile succeeded.	name of realm name of authentication configuration	View authentication configuration profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
883	SEVERE	Getting authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to get authentication configuration profile. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
884	SEVERE	Getting authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to get authentication configuration profile due to service management SDK exception.	Look under service management log for more information.
885	SEVERE	Getting authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to get authentication configuration profile due to authentication configuration SDK exception.	Look under authentication configuration log for more information.
891	INFO	Attempt to modify authentication configuration profile	name of realm name of authentication configuration	Click on Save button in authentication configuration profile page.	
892	INFO	Modification of authentication configuration profile succeeded.	name of realm name of authentication configuration	Click on Save button in authentication configuration profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
893	SEVERE	Modification of authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to modify authentication configuration profile. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
894	SEVERE	Modification of authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to modify authentication configuration profile due to service management SDK exception.	Look under service management log for more information.
895	SEVERE	Modification of authentication configuration profile failed.	name of realm name of authentication configuration error message	Unable to modify authentication configuration profile due to authentication configuration SDK exception.	Look under authentication configuration log for more information.
901	INFO	Attempt to create authentication configuration	name of realm name of authentication configuration	Click on New button in authentication configuration creation page.	
902	INFO	Creation of authentication configuration succeeded.	name of realm name of authentication configuration	Click on New button in authentication configuration creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
903	SEVERE	Creation of authentication configuration failed.	name of realm name of authentication configuration error message	Unable to create authentication configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
904	SEVERE	Creation of authentication configuration failed.	name of realm name of authentication configuration error message	Unable to create authentication configuration due to service management SDK exception.	Look under service management log for more information.
905	SEVERE	Creation of authentication configuration failed.	name of realm name of authentication configuration error message	Unable to create authentication configuration due to authentication configuration SDK exception.	Look under authentication configuration log for more information.
1001	INFO	Attempt to get entity descriptor names.	search pattern	View entity descriptor main page.	
1002	INFO	Getting entity descriptor names succeeded	search pattern	View entity descriptor main page.	
1003	SEVERE	Getting entity descriptor names failed.	search pattern error message	Unable to get entity descriptor names due to federation SDK related errors.	Look under federation log for more information.
1011	INFO	Attempt to create entity descriptor.	descriptor name descriptor type	Click on New button in entity descriptor creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
1012	INFO	Creation entity descriptor succeeded	descriptor name descriptor type	Click on New button in entity descriptor creation page.	
1013	SEVERE	Creation entity descriptor failed.	descriptor name descriptor type error message	Unable to create entity descriptor due to federation SDK related errors.	Look under federation log for more information.
1021	INFO	Attempt to delete entity descriptors.	descriptor names	Click on Delete button in entity descriptor main page.	
1022	INFO	Deletion entity descriptors succeeded	descriptor names	Click on Delete button in entity descriptor main page.	
1023	SEVERE	Deletion entity descriptors failed.	descriptor names error message	Unable to delete entity descriptors due to federation SDK related errors.	Look under federation log for more information.
1031	INFO	Attempt to get attribute values of an affiliate entity descriptor.	descriptor name	View affiliate entity descriptor profile page.	
1032	INFO	Getting of attribute values of an affiliate entity descriptor succeeded.	descriptor name	View affiliate entity descriptor profile page.	
1033	SEVERE	Getting of attribute values of an affiliate entity descriptor failed.	descriptor name error message	Unable to get attribute value of an affiliate entity descriptor due to federation SDK related errors.	Look under federation log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
1041	INFO	Attempt to modify an affiliate entity descriptor.	descriptor name	Click on Save button of affiliate entity descriptor profile page.	
1042	INFO	Modification of an affiliate entity descriptor succeeded.	descriptor name	Click on Save button of affiliate entity descriptor profile page.	
1043	SEVERE	Modification of an affiliate entity descriptor failed.	descriptor name error message	Unable to modify an affiliate entity descriptor due to federation SDK related errors.	Look under federation log for more information.
1044	SEVERE	Modification of an affiliate entity descriptor failed.	descriptor name error message	Unable to modify an affiliate entity descriptor due to incorrect number format of one or more attribute values.	Look under federation log for more information.
1051	INFO	Attempt to get attribute values of an entity descriptor.	descriptor name	View entity descriptor profile page.	
1052	INFO	Getting attribute values of entity descriptor succeeded.	descriptor name	View entity descriptor profile page.	
1053	SEVERE	Getting attribute values of entity descriptor failed.	descriptor name error message	Unable to get attribute values of entity descriptor due to federation SDK related errors.	Look under federation log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
1061	INFO	Attempt to modify entity descriptor.	descriptor name	Click on Save button in entity descriptor profile page.	
1062	INFO	Modification of entity descriptor succeeded.	descriptor name	Click on Save button in entity descriptor profile page.	
1063	SEVERE	Modification of entity descriptor failed.	descriptor name error message	Unable to modify entity descriptor due to federation SDK related errors.	Look under federation log for more information.
1101	INFO	Attempt to get authentication domain names.	search pattern	View authentication domain main page.	
1102	INFO	Getting authentication domain names succeeded.	search pattern	View authentication domain main page.	
1103	SEVERE	Getting authentication domain names failed.	search pattern error message	Unable to get authentication domain names due to federation SDK related errors.	Look under federation log for more information.
1111	INFO	Attempt to create authentication domain	name of authentication domain	Click on New button in authentication domain creation page.	
1112	INFO	Creation authentication domain succeeded.	name of authentication domain	Click on New button in authentication domain creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
1113	SEVERE	Creation authentication domain failed.	name of authentication domain error message	Unable to create authentication domain due to federation SDK related errors.	Look under federation log for more information.
1121	INFO	Attempt to delete authentication domains	name of authentication domains	Click on Delete button in authentication domain main page.	
1122	INFO	Deletion authentication domain succeeded.	name of authentication domains	Click on Delete button in authentication domain main page.	
1123	SEVERE	Deletion authentication domain failed.	name of authentication domains error message	Unable to delete authentication domain due to federation SDK related errors.	Look under federation log for more information.
1131	INFO	Attempt to get authentication domain's attribute values	name of authentication domain	View authentication domain profile page.	
1132	INFO	Getting attribute values of authentication domain succeeded.	name of authentication domain	View authentication domain profile page.	
1133	SEVERE	Getting attribute values of authentication domain failed.	name of authentication domains error message	Unable to get attribute values of authentication domain due to federation SDK related errors.	Look under federation log for more information.
1141	INFO	Attempt to modify authentication domain	name of authentication domain	Click on Save button in authentication domain profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
1142	INFO	Modification authentication domain succeeded.	name of authentication domain	Click on Save button in authentication domain profile page.	
1143	SEVERE	Modification authentication domain failed.	name of authentication domain error message	Unable to modify authentication domain due to federation SDK related errors.	Look under federation log for more information.
1151	INFO	Attempt to get all provider names		View authentication domain profile page.	
1152	INFO	Getting all provider names succeeded.		View authentication domain profile page.	
1153	SEVERE	Getting all provider names failed.	error message	Unable to get all provider names due to federation SDK related errors.	Look under federation log for more information.
1161	INFO	Attempt to get provider names under a authentication domain	name of authentication domain	View authentication domain profile page.	
1162	INFO	Getting provider names under authentication domain succeeded.	name of authentication domain	View authentication domain profile page.	
1163	SEVERE	Getting provider names under authentication domain failed.	name of authentication domain error message	Unable to get provider names under authentication domain due to federation SDK related errors.	Look under federation log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
1171	INFO	Attempt to add providers to an authentication domain	name of authentication domain name of providers	Click on Save button in provider assignment page.	
1172	INFO	Addition of provider to an authentication domain succeeded.	name of authentication domain name of providers	Click on Save button in provider assignment page.	
1173	SEVERE	Addition of provider to an authentication domain failed.	name of authentication domain name of providers error message	Unable to add provider to authentication domain due to federation SDK related errors.	Look under federation log for more information.
1181	INFO	Attempt to remove providers from authentication domain	name of authentication domain name of providers	Click on Save button in provider assignment page.	
1182	INFO	Deletion of providers from authentication domain succeeded.	name of authentication domain name of providers	Click on Save button in provider assignment page.	
1183	SEVERE	Deletion of provider from authentication domain failed.	name of authentication domain name of providers error message	Unable to remove provider from authentication domain due to federation SDK related errors.	Look under federation log for more information.
1301	INFO	Attempt to create provider	name of provider role of provider type of provider	Click on Save button in provider assignment page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
1302	INFO	Creation of providers succeeded.	name of provider role of provider type of provider	Click on Save button in provider assignment page.	
1303	SEVERE	Creation of provider failed.	name of provider role of provider type of provider error message	Unable to create provider due to federation SDK related errors.	Look under federation log for more information.
1303	SEVERE	Creation of provider failed.	name of provider role of provider type of provider error message	Unable to create provider due to federation SDK related errors.	Look under federation log for more information.
1304	SEVERE	Creation of provider failed.	name of provider role of provider type of provider error message	Unable to create provider because Administration Console cannot find the appropriate methods to set values for this provider.	This is a web application error. Please contact Sun Support for assistant.
1311	INFO	Attempt to get attribute values for provider	name of provider role of provider type of provider	View provider profile page.	
1312	INFO	Getting attribute values of providers succeeded.	name of provider role of provider type of provider	View provider profile page.	
1321	INFO	Attempt to get handler to provider	name of provider role of provider	View provider profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
1322	INFO	Getting handler to provider succeeded.	name of provider role of provider	View provider profile page.	
1323	SEVERE	Getting handler to provider failed.	name of provider role of provider error message	Unable to get handler to provider due to federation SDK related errors.	Look under federation log for more information.
1331	INFO	Attempt to modify provider	name of provider role of provider	Click on Save button in provider profile page.	
1332	INFO	Modification of provider succeeded.	name of provider role of provider	Click on Save button in provider profile page.	
1333	SEVERE	Modification of provider failed.	name of provider role of provider error message	Unable to modify provider due to federation SDK related errors.	Look under federation log for more information.
1334	SEVERE	Modification of provider failed.	name of provider role of provider error message	Unable to modify provider because Administration Console cannot find the appropriate methods to set values for this provider.	This is a web application error. Please contact Sun Support for assistant.
1341	INFO	Attempt to delete provider	name of provider role of provider	Click on delete provider button in provider profile page.	
1342	INFO	Deletion of provider succeeded.	name of provider role of provider	Click on delete provider button in provider profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
1343	SEVERE	Deletion of provider failed.	name of provider role of provider error message	Unable to delete provider due to federation SDK related errors.	Look under federation log for more information.
1351	INFO	Attempt to get prospective trusted provider	name of provider role of provider	View add trusted provider page.	
1352	INFO	Getting of prospective trusted provider succeeded.	name of provider role of provider	View add trusted provider page.	
1353	SEVERE	Getting of prospective trusted provider failed.	name of provider role of provider error message	Unable to get prospective trusted provider due to federation SDK related errors.	Look under federation log for more information.
2001	INFO	Attempt to get attribute values of schema type of a service schema	name of service name of schema type name of attribute schemas	View service profile page.	
2002	INFO	Getting attribute values of schema type of a service schema succeeded.	name of service name of schema type name of attribute schemas	View service profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
2003	SEVERE	Getting attribute values of schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to get attribute values of schema type of a service schema. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
2004	SEVERE	Getting attribute values of schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to get attribute values of schema type of a service schema due to service management SDK related errors.	Look under service management log for more information.
2005	INFO	Getting attribute values of schema type of a service schema failed.	name of service name of schema type name of attribute schemas	View service profile page.	Need no action on this event. Console attempts to get a schema from a service but schema does not exist.
2011	INFO	Attempt to get attribute values of attribute schema of a schema type of a service schema	name of service name of schema type name of attribute schemas	View service profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
2012	INFO	Getting attribute values of attribute schema of a schema type of a service schema succeeded.	name of service name of schema type name of attribute schemas	View service profile page.	
2013	SEVERE	Getting attribute values of attribute schema of a schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to get attribute values of schema type of a service schema. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
2014	SEVERE	Getting attribute values of attribute schema of a schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to get attribute values of schema type of a service schema due to service management SDK related errors.	Look under service management log for more information.
2021	INFO	Attempt to modify attribute values of attribute schema of a schema type of a service schema	name of service name of schema type name of attribute schemas	Click on Save button in service profile page.	
2022	INFO	Modification attribute values of attribute schema of a schema type of a service schema succeeded.	name of service name of schema type name of attribute schemas	Click on Save button in service profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
2023	SEVERE	Modification attribute values of attribute schema of a schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to modify attribute values of schema type of a service schema. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under service management log for more information.
2024	SEVERE	Modification attribute values of attribute schema of a schema type of a service schema failed.	name of service name of schema type name of attribute schemas error message	Unable to modify attribute values of schema type of a service schema due to service management SDK related errors.	Look under service management log for more information.
2501	INFO	Attempt to get device names of client detection service	name of profile name of style search pattern	View client profile page.	
2502	INFO	Getting device names of client detection service succeeded.	name of profile name of style search pattern	View client profile page.	
2511	INFO	Attempt to delete client in client detection service	type of client	Click on client type delete hyperlink page.	
2512	INFO	Deletion of client in client detection service succeeded.	type of client	Click on client type delete hyperlink page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
2513	SEVERE	Deletion of client in client detection service failed.	type of client error message	Unable to delete client due to client detection SDK related errors.	Look under client detection management log for more information.
2521	INFO	Attempt to create client in client detection service	type of client	Click on New button in Client Creation Page.	
2522	INFO	Creation of client in client detection service succeeded.	type of client	Click on New button in Client Creation Page.	
2523	SEVERE	Creation of client in client detection service failed.	type of client error message	Unable to create client due to client detection SDK related errors.	Look under client detection management log for more information.
2524	INFO	Creation of client in client detection service failed.	type of client error message	Unable to create client because client type is invalid.	Check the client type again before creation.
2531	INFO	Attempt to get client profile in client detection service	type of client classification	View client profile page.	
2532	INFO	Getting of client profile in client detection service succeeded.	type of client classification	View client profile page.	
2541	INFO	Attempt to modify client profile in client detection service	type of client	Click on Save button client profile page.	
2542	INFO	Modification of client profile in client detection service succeeded.	type of client	Click on Save button client profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
2543	SEVERE	Modification of client profile in client detection service failed.	type of client error message	Unable to modify client profile due to client detection SDK related errors.	Look under client detection management log for more information.
3001	INFO	Attempt to get current sessions	name of server search pattern	View session main page.	
3002	INFO	Getting of current sessions succeeded.	name of server search pattern	View session main page.	
3003	SEVERE	Getting of current sessions failed.	name of server name of realm error message	Unable to get current sessions due to session SDK exception.	Look under session management log for more information.
3011	INFO	Attempt to invalidate session	name of server ID of session	Click on Invalidate button in session main page.	
3012	INFO	Invalidation of session succeeded.	name of server ID of session	Click on Invalidate button in session main page.	
3013	SEVERE	Invalidation of session failed.	name of server ID of session error message	Unable to invalidate session due to session SDK exception.	Look under session management log for more information.
10001	INFO	Attempt to search for containers from an organization	DN of organization search pattern	Click on Search button in Organization's containers page.	
10002	INFO	Searching for containers from an organization succeeded.	DN of organization search pattern	Click on Search button in Organization's containers page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10003	SEVERE	Searching for containers from an organization failed.	DN of organization search pattern error message	Unable to search for containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10004	SEVERE	Searching for containers from an organization failed.	DN of organization search pattern error message	Unable to search for containers due to access management SDK exception.	Look under access management SDK log for more information.
10011	INFO	Attempt to search for containers from a container	DN of container search pattern	Click on Search button in Container's sub containers page.	
10012	INFO	Searching for containers from a container succeeded.	DN of container search pattern	Click on Search button in Container's sub containers page.	
10013	SEVERE	Searching for containers from a container failed.	DN of container search pattern error message	Unable to search for containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10014	SEVERE	Searching for containers from a container failed.	DN of container search pattern error message	Unable to search for containers due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10021	INFO	Attempt to create containers under an organization	DN of organization Name of container	Click on New button in Container Creation page.	
10022	INFO	Creation of container under an organization succeeded.	DN of organization Name of container	Click on New button in Container Creation page.	
10023	SEVERE	Creation of container under an organization failed.	DN of organization Name of container error message	Unable to create container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10024	SEVERE	Creation of container under an organization failed.	DN of organization Name of container error message	Unable to create container due to access management SDK exception.	Look under access management SDK log for more information.
10031	INFO	Attempt to create containers under an container	DN of container Name of container	Click on New button in Container Creation page.	
10032	INFO	Creation of container under an container succeeded.	DN of container Name of container	Click on New button in Container Creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10033	SEVERE	Creation of container under an container failed.	DN of container Name of container error message	Unable to create container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10034	SEVERE	Creation of container under an container failed.	DN of container Name of container error message	Unable to create container due to access management SDK exception.	Look under access management SDK log for more information.
10041	INFO	Attempt to get assigned services to container	DN of container	View Container's service profile page.	
10042	INFO	Getting assigned services to container succeeded.	DN of container	View Container's service profile page.	
10043	SEVERE	Getting assigned services to container failed.	DN of container error message	Unable to get services assigned to container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10044	SEVERE	Getting assigned services to container failed.	DN of container error message	Unable to get services assigned to container due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10101	INFO	Attempt to get service template under an organization	DN of organization Name of service Type of template	View Organization's service profile page.	
10102	INFO	Getting service template under an organization succeeded.	DN of organization Name of service Type of template	View Organization's service profile page.	
10103	SEVERE	Getting service template under an organization failed.	DN of organization Name of service Type of template error message	Unable to get service template. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10104	SEVERE	Getting service template under an organization failed.	DN of organization Name of service Type of template error message	Unable to get service template due to access management SDK exception.	Look under access management SDK log for more information.
10111	INFO	Attempt to get service template under a container	DN of container Name of service Type of template	View container's service profile page.	
10112	INFO	Getting service template under a container succeeded.	DN of container Name of service Type of template	View container's service profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10113	SEVERE	Getting service template under a container failed.	DN of container Name of service Type of template error message	Unable to get service template. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10114	SEVERE	Getting service template under a container failed.	DN of container Name of service Type of template error message	Unable to get service template due to access management SDK exception.	Look under access management SDK log for more information.
10121	INFO	Attempt to delete directory object	Name of object	Click on Delete button in object main page.	
10122	INFO	Deletion of directory object succeeded.	Name of object	Click on Delete button in object main page.	
10123	SEVERE	Deletion of directory object failed.	Name of object error message	Unable to delete directory object. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10124	SEVERE	Deletion of directory object failed.	Name of object error message	Unable to delete directory object due to access management SDK exception.	Look under access management SDK log for more information.
10131	INFO	Attempt to modify directory object	DN of object	Click on object profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10132	INFO	Modification of directory object succeeded.	DN of object	Click on object profile page.	
10133	SEVERE	Modification of directory object failed.	DN of object error message	Unable to modify directory object due to access management SDK exception.	Look under access management SDK log for more information.
10141	INFO	Attempt to delete service from organization	DN of organization Name of service	Click on unassign button in organization's service page.	
10142	INFO	Deletion of service from organization succeeded.	DN of organization Name of service	Click on unassign button in organization's service page.	
10143	SEVERE	Deletion of service from organization failed.	DN of organization Name of service error message	Unable to delete service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10144	SEVERE	Deletion of service from organization failed.	DN of organization Name of service error message	Unable to delete service due to access management SDK exception.	Look under access management SDK log for more information.
10151	INFO	Attempt to delete service from container	DN of container Name of service	Click on unassign button in container's service page.	
10152	INFO	Deletion of service from container succeeded.	DN of container Name of service	Click on unassign button in container's service page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10153	SEVERE	Deletion of service from container failed.	DN of container Name of service error message	Unable to delete service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10154	SEVERE	Deletion of service from container failed.	DN of container Name of service error message	Unable to delete service due to access management SDK exception.	Look under access management SDK log for more information.
10201	INFO	Attempt to serch for group containers under organization	DN of organization Search pattern	Click on Search button in organization's group containers page.	
10202	INFO	Searching for group containers under organization succeeded.	DN of organization Search pattern	Click on Search button in organization's group containers page.	
10203	SEVERE	Searching for group containers under organization failed.	DN of organization Search pattern error message	Unable to search group containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10204	SEVERE	Searching for group containers under organization failed.	DN of organization Search pattern error message	Unable to search group containers due to access management SDK exception.	Look under access management SDK log for more information.
10211	INFO	Attempt to serch for group containers under container	DN of container Search pattern	Click on Search button in container's group containers page.	
10212	INFO	Searching for group containers under container succeeded.	DN of container Search pattern	Click on Search button in container's group containers page.	
10213	SEVERE	Searching for group containers under container failed.	DN of container Search pattern error message	Unable to search group containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10214	SEVERE	Searching for group containers under container failed.	DN of container Search pattern error message	Unable to search group containers due to access management SDK exception.	Look under access management SDK log for more information.
10221	INFO	Attempt to search for group containers under group container	DN of group container Search pattern	Click on Search button in group container's group containers page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10222	INFO	Searching for group containers under group container succeeded.	DN of group container Search pattern	Click on Search button in group container's group containers page.	
10223	SEVERE	Searching for group containers under group container failed.	DN of group container Search pattern error message	Unable to search group containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10224	SEVERE	Searching for group containers under group container failed.	DN of group container Search pattern error message	Unable to search group containers due to access management SDK exception.	Look under access management SDK log for more information.
10231	INFO	Attempt to create group container in organization	DN of organization Name of group container	Click on New button in group container creation page.	
10232	INFO	Creation of group container under organization succeeded.	DN of organization Name of group container	Click on New button in group container creation page.	
10233	SEVERE	Creation of group container under organization failed.	DN of organization Name of group container error message	Unable to create group container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10234	SEVERE	Creation of group container under organization failed.	DN of organization Name of group container error message	Unable to create group container due to access management SDK exception.	Look under access management SDK log for more information.
10241	INFO	Attempt to create group container in container	DN of container Name of group container	Click on New button in group container creation page.	
10242	INFO	Creation of group container under container succeeded.	DN of container Name of group container	Click on New button in group container creation page.	
10243	SEVERE	Creation of group container under container failed.	DN of container Name of group container error message	Unable to create group container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10244	SEVERE	Creation of group container under container failed.	DN of container Name of group container error message	Unable to create group container due to access management SDK exception.	Look under access management SDK log for more information.
10251	INFO	Attempt to create group container in group container	DN of group container Name of group container	Click on New button in group container creation page.	
10252	INFO	Creation of group container under group container succeeded.	DN of group container Name of group container	Click on New button in group container creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10253	SEVERE	Creation of group container under group container failed.	DN of group container Name of group container error message	Unable to create group container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10254	SEVERE	Creation of group container under group container failed.	DN of group container Name of group container error message	Unable to create group container due to access management SDK exception.	Look under access management SDK log for more information.
10301	INFO	Attempt to search groups under organization	DN of organization search pattern	Click on Search button in organization's group page.	
10302	INFO	Searching for groups under organization succeeded.	DN of organization search pattern	Click on Search button in organization's group page.	
10303	SEVERE	Searching for groups under organization failed.	DN of organization search pattern error message	Unable to search for groups. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10304	SEVERE	Searching for groups under organization failed.	DN of organization search pattern error message	Unable to search groups due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10311	INFO	Attempt to search groups under container	DN of container search pattern	Click on Search button in container's group page.	
10312	INFO	Searching for groups under container succeeded.	DN of container search pattern	Click on Search button in container's group page.	
10313	SEVERE	Searching for groups under container failed.	DN of container search pattern error message	Unable to search for groups. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10314	SEVERE	Searching for groups under container failed.	DN of container search pattern error message	Unable to search groups due to access management SDK exception.	Look under access management SDK log for more information.
10321	INFO	Attempt to search groups under static group	DN of static group search pattern	Click on Search button in static group's group page.	
10322	INFO	Searching for groups under static group succeeded.	DN of static group search pattern	Click on Search button in static group's group page.	
10323	SEVERE	Searching for groups under static group failed.	DN of static group search pattern error message	Unable to search for groups. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10324	SEVERE	Searching for groups under static group failed.	DN of static group search pattern error message	Unable to search groups due to access management SDK exception.	Look under access management SDK log for more information.
10331	INFO	Attempt to search groups under dynamic group	DN of dynamic group search pattern	Click on Search button in dynamic group's group page.	
10332	INFO	Searching for groups under dynamic group succeeded.	DN of dynamic group search pattern	Click on Search button in dynamic group's group page.	
10333	SEVERE	Searching for groups under dynamic group failed.	DN of dynamic group search pattern error message	Unable to search for groups. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10334	SEVERE	Searching for groups under dynamic group failed.	DN of dynamic group search pattern error message	Unable to search groups due to access management SDK exception.	Look under access management SDK log for more information.
10341	INFO	Attempt to search groups under assignable dynamic group	DN of assignable dynamic group search pattern	Click on Search button in assignable dynamic group's group page.	
10342	INFO	Searching for groups under assignable dynamic group succeeded.	DN of assignable dynamic group search pattern	Click on Search button in assignable dynamic group's group page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10343	SEVERE	Searching for groups under assignable dynamic group failed.	DN of assignable dynamic group search pattern error message	Unable to search for groups. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10344	SEVERE	Searching for groups under assignable dynamic group failed.	DN of assignable dynamic group search pattern error message	Unable to search groups due to access management SDK exception.	Look under access management SDK log for more information.
10351	INFO	Attempt to create group under organization	DN of organization Name of group	Click on New button in group creation page.	
10352	INFO	Creation of groups under organization succeeded.	DN of organization Name of group	Click on New button in group creation page.	
10353	SEVERE	Creation of group under organization failed.	DN of organization Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10354	SEVERE	Creation of group under organization failed.	DN of organization Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10361	INFO	Attempt to create group under container	DN of container Name of group	Click on New button in group creation page.	
10362	INFO	Creation of groups under container succeeded.	DN of container Name of group	Click on New button in group creation page.	
10363	SEVERE	Creation of group under container failed.	DN of container Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10364	SEVERE	Creation of group under container failed.	DN of container Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.
10371	INFO	Attempt to create group under group container	DN of group container Name of group	Click on New button in group creation page.	
10372	INFO	Creation of groups under group container succeeded.	DN of group container Name of group	Click on New button in group creation page.	
10373	SEVERE	Creation of group under group container failed.	DN of group container Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10374	SEVERE	Creation of group under group container failed.	DN of group container Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.
10381	INFO	Attempt to create group under dynamic group	DN of dynamic group Name of group	Click on New button in group creation page.	
10382	INFO	Creation of groups under dynamic group succeeded.	DN of dynamic group Name of group	Click on New button in group creation page.	
10383	SEVERE	Creation of group under dynamic group failed.	DN of dynamic group Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10384	SEVERE	Creation of group under dynamic group failed.	DN of dynamic group Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.
10391	INFO	Attempt to create group under static group	DN of static group Name of group	Click on New button in group creation page.	
10392	INFO	Creation of groups under static group succeeded.	DN of static group Name of group	Click on New button in group creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10393	SEVERE	Creation of group under static group failed.	DN of static group Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10394	SEVERE	Creation of group under static group failed.	DN of static group Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.
10401	INFO	Attempt to create group under assignable dynamic group	DN of assignable dynamic group Name of group	Click on New button in group creation page.	
10402	INFO	Creation of groups under assignable dynamic group succeeded.	DN of assignable dynamic group Name of group	Click on New button in group creation page.	
10403	SEVERE	Creation of group under assignable dynamic group failed.	DN of assignable dynamic group Name of group error message	Unable to create group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10404	SEVERE	Creation of group under assignable dynamic group failed.	DN of assignable dynamic group Name of group error message	Unable to create group due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10411	INFO	Attempt to modify group	DN of group	Click on Save button in group profile page.	
10412	INFO	Modification of groups succeeded.	DN of group	Click on Save button in group profile page.	
10414	SEVERE	Modification of group failed.	DN of assignable dynamic group Name of group error message	Unable to modify group due to access management SDK exception.	Look under access management SDK log for more information.
10421	INFO	Attempt to search for users in group	DN of group Search pattern	View group's user page.	
10422	INFO	Searching for users in group succeeded.	DN of group Search pattern	View group's user page.	
10423	SEVERE	Searching for users in group failed.	DN of group Search pattern error message	Unable to search for users. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10424	SEVERE	Searching for users in group failed.	DN of group Search pattern error message	Unable to search for users due to access management SDK exception.	Look under access management SDK log for more information.
10431	INFO	Attempt to get nested groups	DN of group	View group's members page.	
10432	INFO	Getting nested groups succeeded.	DN of group	View group's members page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10433	SEVERE	Getting nested groups failed.	DN of group error message	Unable to get nested group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10434	SEVERE	Getting nested groups failed.	DN of group error message	Unable to get nested group due to access management SDK exception.	Look under access management SDK log for more information.
10441	INFO	Attempt to remove nested groups	DN of group DN of nested groups	Click on remove button in group's members page.	
10442	INFO	Removal of nested groups succeeded.	DN of group DN of nested groups	Click on remove button in group's members page.	
10443	SEVERE	Removal of nested groups failed.	DN of group DN of nested groups error message	Unable to remove nested group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10444	SEVERE	Removal of nested groups failed.	DN of group DN of nested groups error message	Unable to remove nested group due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10451	INFO	Attempt to remove users from group	DN of group DN of users	Click on remove button in group's members page.	
10452	INFO	Removal of users from group succeeded.	DN of group DN of users	Click on remove button in group's members page.	
10453	SEVERE	Removal of users from group failed.	DN of group DN of users error message	Unable to remove users. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10454	SEVERE	Removal of users from group failed.	DN of group DN of users error message	Unable to remove users due to access management SDK exception.	Look under access management SDK log for more information.
10501	INFO	Attempt to search people containers in organization	DN of organization Search pattern	View organization's people containers page.	
10502	INFO	Searching of people containers in organization succeeded.	DN of organization Search pattern	View organization's people containers page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10503	SEVERE	Searching of people containers in organization failed.	DN of organization Search pattern error message	Unable to search for people containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10504	SEVERE	Searching of people containers in organization failed.	DN of organization Search pattern error message	Unable to search for people containers due to access management SDK exception.	Look under access management SDK log for more information.
10511	INFO	Attempt to search people containers in container	DN of container Search pattern	View container's people containers page.	
10512	INFO	Searching of people containers in container succeeded.	DN of container Search pattern	View container's people containers page.	
10513	SEVERE	Searching of people containers in container failed.	DN of container Search pattern error message	Unable to search for people containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10514	SEVERE	Searching of people containers in container failed.	DN of container Search pattern error message	Unable to search for people containers due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10521	INFO	Attempt to search people containers in people container	DN of people container Search pattern	View people container's people containers page.	
10522	INFO	Searching of people containers in people container succeeded.	DN of people container Search pattern	View people container's people containers page.	
10523	SEVERE	Searching of people containers in people container failed.	DN of people container Search pattern error message	Unable to search for people containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10524	SEVERE	Searching of people containers in people container failed.	DN of people container Search pattern error message	Unable to search for people containers due to access management SDK exception.	Look under access management SDK log for more information.
10531	INFO	Attempt to create people container in organization	DN of organization Name of people container	Click on New button in people container creation page.	
10532	INFO	Creation of people containers in organization succeeded.	DN of organization Name of people container	Click on New button in people container creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10533	SEVERE	Creation of people container in organization failed.	DN of organization Name of people container error message	Unable to create for people containers. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10534	SEVERE	Creation of people container in organization failed.	DN of organization Name of people container error message	Unable to create for people container due to access management SDK exception.	Look under access management SDK log for more information.
10541	INFO	Attempt to create people container in container	DN of container Name of people container	Click on New button in people container creation page.	
10542	INFO	Creation of people container in container succeeded.	DN of container Name of people container	Click on New button in people container creation page.	
10543	SEVERE	Creation of people container in container failed.	DN of container Name of people container error message	Unable to create for people container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10544	SEVERE	Creation of people container in container failed.	DN of container Name of people container error message	Unable to create for people container due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10551	INFO	Attempt to create people container in people container	DN of people container Name of people container	Click on New button in people container creation page.	
10552	INFO	Creation of people container in people container succeeded.	DN of people container Name of people container	Click on New button in people container creation page.	
10553	SEVERE	Creation of people container in people container failed.	DN of people container Name of people container error message	Unable to create for people container. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10554	SEVERE	Creation of people container in people container failed.	DN of people container Name of people container error message	Unable to create for people container due to access management SDK exception.	Look under access management SDK log for more information.
10601	INFO	Attempt to get assigned services to an organization	DN of organization	View organization's service profile page.	
10602	INFO	Getting of assigned services to organization succeeded.	DN of organization	View organization's service profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10603	SEVERE	Getting of assigned services to organization failed.	DN of organization error message	Unable to get assigned services. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10604	SEVERE	Getting of assigned services to organization failed.	DN of organization error message	Unable to get assigned services due to access management SDK exception.	Look under access management SDK log for more information.
10611	INFO	Attempt to remove services from an organization	DN of organization Name of service	Click on unassign button in organization's service profile page.	
10612	INFO	Removal of services from organization succeeded.	DN of organization Name of service	Click on unassign button in organization's service profile page.	
10613	SEVERE	Removal of services from organization failed.	DN of organization Name of service error message	Unable to remove services. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10614	SEVERE	Removal of services from organization failed.	DN of organization Name of service error message	Unable to remove services due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10621	INFO	Attempt to search organization in an organization	DN of organization Search pattern	View organization's sub organization page.	
10622	INFO	Searching for organization in an organization succeeded.	DN of organization Search pattern	View organization's sub organization page.	
10623	SEVERE	Searching for organization in an organization failed.	DN of organization Search pattern error message	Unable to search for organizations. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10624	SEVERE	Searching for organization in an organization failed.	DN of organization Search pattern error message	Unable to search for organizations due to access management SDK exception.	Look under access management SDK log for more information.
10631	INFO	Attempt to modify organization	DN of organization	Click on Save button in organization profile page.	
10632	INFO	Modificaition of organization succeeded.	DN of organization	Click on Save button in organization profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10633	SEVERE	Modificaition of organization failed.	DN of organization error message	Unable to modify organization. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10634	SEVERE	Modificaition of organization failed.	DN of organization error message	Unable to modify organization due to access management SDK exception.	Look under access management SDK log for more information.
10641	INFO	Attempt to create organization in an organization	DN of organization Name of new organization	Click on New button in organization creation page.	
10642	INFO	Creation of organization in an organization succeeded.	DN of organization Name of new organization	Click on New button in organization creation page.	
10643	SEVERE	Creation of organization in an organization failed.	DN of organization Name of new organization error message	Unable to create organization. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10644	SEVERE	Creation of organization in an organization failed.	DN of organization Name of new organization error message	Unable to create organization due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10651	INFO	Attempt to get attribute values of an organization	DN of organization	View organization profile page.	
10652	INFO	Getting of attribute values of an organization succeeded.	DN of organization	View organization profile page.	
10653	SEVERE	Getting of attribute values of an organization failed.	DN of organization error message	Unable to get attribute values of organization. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10654	SEVERE	Getting of attribute values of an organization failed.	DN of organization error message	Unable to get attribute values of organization due to access management SDK exception.	Look under access management SDK log for more information.
10661	INFO	Attempt to add service to an organization	DN of organization Name of service	Click on assign button in organization's service page.	
10662	INFO	Addition of service to an organization succeeded.	DN of organization Name of service	Click on assign button in organization's service page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10663	SEVERE	Addition of service to an organization failed.	DN of organization Name of service error message	Unable to add service to organization. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10664	SEVERE	Addition of service to an organization failed.	DN of organization Name of service error message	Unable to add service to organization due to access management SDK exception.	Look under access management SDK log for more information.
10701	INFO	Attempt to remove users from role	DN of role Name of users	Click on remove button in role's user page.	
10702	INFO	Removal of users from role succeeded.	DN of role Name of users	Click on remove button in role's user page.	
10703	SEVERE	Removal of users from role failed.	DN of role Name of users error message	Unable to remove users. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10704	SEVERE	Removal of users from role failed.	DN of role Name of users error message	Unable to remove users due to access management SDK exception.	Look under access management SDK log for more information.
10711	INFO	Attempt to get attribute values of role	DN of role	View role profile page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10712	INFO	Getting attribute values of rolesucceeded.	DN of role	View role profile page.	
10713	SEVERE	Getting attribute values of role failed.	DN of role error message	Unable to get attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10714	SEVERE	Getting attribute values of role failed.	DN of role error message	Unable to get attribute values due to access management SDK exception.	Look under access management SDK log for more information.
10721	INFO	Attempt to modify role	DN of role	Click on Save button in role profile page.	
10722	INFO	Modification of role succeeded.	DN of role	Click on Save button in role profile page.	
10723	SEVERE	Modification of role failed.	DN of role error message	Unable to modify role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10724	SEVERE	Modification of role failed.	DN of role error message	Unable to modify role due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10731	INFO	Attempt to getting members in role	DN of role Search pattern	View role's members page.	
10732	INFO	Getting members in role succeeded.	DN of role Search pattern	View role's members page.	
10733	SEVERE	Getting members in role failed.	DN of role Search pattern error message	Unable to getting members. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10734	SEVERE	Getting members in role failed.	DN of role Search pattern error message	Unable to getting members due to access management SDK exception.	Look under access management SDK log for more information.
10741	INFO	Attempt to getting roles in organization	DN of role Search pattern	View organization's roles page.	
10742	INFO	Getting roles in organization succeeded.	DN of role Search pattern View role's members page.	View organization's roles page.	
10743	SEVERE	Getting roles in organization failed.	DN of role Search pattern error message	Unable to getting roles. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10744	SEVERE	Getting roles in organization failed.	DN of role Search pattern error message	Unable to getting roles due to access management SDK exception.	Look under access management SDK log for more information.
10751	INFO	Attempt to getting roles in container	DN of role Search pattern	View container's roles page.	
10752	INFO	Getting roles in container succeeded.	DN of role Search pattern View role's members page.	View container's roles page.	
10753	SEVERE	Getting roles in container failed.	DN of role Search pattern error message	Unable to getting roles. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10754	SEVERE	Getting roles in container failed.	DN of role Search pattern error message	Unable to getting roles due to access management SDK exception.	Look under access management SDK log for more information.
10761	INFO	Attempt to creating roles in container	DN of container Name of role	Click on New button in roles creation page.	
10762	INFO	Creation of roles in container succeeded.	DN of container Name of role	Click on New button in roles creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10763	SEVERE	Creation of roles in container failed.	DN of container Name of role	Unable to create role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10764	SEVERE	Creation of role in container failed.	DN of container Name of role error message	Unable to create role due to access management SDK exception.	Look under access management SDK log for more information.
10771	INFO	Attempt to creating roles in organization	DN of organization Name of role	Click on New button in roles creation page.	
10772	INFO	Creation of roles in organization succeeded.	DN of organization Name of role	Click on New button in roles creation page.	
10773	SEVERE	Creation of roles in organization failed.	DN of organization Name of role	Unable to create role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10774	SEVERE	Creation of role in organization failed.	DN of organization Name of role error message	Unable to create role due to access management SDK exception.	Look under access management SDK log for more information.
10781	INFO	Attempt to get assigned services in role	DN of role	View role's service page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10782	INFO	Getting of assigned services in role succeeded.	DN of role	View role's service page.	
10783	SEVERE	Getting of assigned services in role failed.	DN of role error message	Unable to get services in role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10784	SEVERE	Getting of assigned services in role failed.	DN of role error message	Unable to get services in role due to access management SDK exception.	Look under access management SDK log for more information.
10791	INFO	Attempt to remove service from role	DN of role Name of service	Click on unassign button in role's service page.	
10792	INFO	Removal of service from role succeeded.	DN of role Name of service	Click on unassign button in role's service page.	
10793	SEVERE	Removal of service from role failed.	DN of role Name of service error message	Unable to remove service from role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10794	SEVERE	Removal of service from role failed.	DN of role Name of service error message	Unable to remove service from role due to access management SDK exception.	Look under access management SDK log for more information.
10801	INFO	Attempt to add service to role	DN of role Name of service	Click on assign button in role's service page.	
10802	INFO	Addition of service to role succeeded.	DN of role Name of service	Click on assign button in role's service page.	
10803	SEVERE	Addition of service to role failed.	DN of role Name of service error message	Unable to add service to role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10804	SEVERE	Addition of service to role failed.	DN of role Name of service error message	Unable to add service to role due to access management SDK exception.	Look under access management SDK log for more information.
10901	INFO	Attempt to get assigned role of user	DN of user	View user's role page.	
10902	INFO	Getting of assigned role of user succeeded.	DN of user	View user's role page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10903	SEVERE	Getting of assigned role of user failed.	DN of user error message	Unable to get assigned roles. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10904	SEVERE	Getting of assigned role of user failed.	DN of user Name of service error message	Unable to get assigned roles due to access management SDK exception.	Look under access management SDK log for more information.
10911	INFO	Attempt to remove role from user	DN of user DN of role	Click on delete button in user's role page.	
10912	INFO	Removal of role from user succeeded.	DN of user DN of role	Click on delete button in user's role page.	
10913	SEVERE	Removal of role from user failed.	DN of user DN of role error message	Unable to remove role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10914	SEVERE	Removal of role from user failed.	DN of user DN of role Name of service error message	Unable to remove role due to access management SDK exception.	Look under access management SDK log for more information.
10921	INFO	Attempt to add role to user	DN of user DN of role	Click on add button in user's role page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10922	INFO	Addition of role to user succeeded.	DN of user DN of role	Click on add button in user's role page.	
10923	SEVERE	Addition of role to user failed.	DN of user DN of role error message	Unable to add role. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10924	SEVERE	Addition of role to user failed.	DN of user DN of role Name of service error message	Unable to add role due to access management SDK exception.	Look under access management SDK log for more information.
10931	INFO	Attempt to get assigned services of user	DN of user	View user's services page.	
10932	INFO	Getting assigned services of user succeeded.	DN of user	View user's services page.	
10933	SEVERE	Getting assigned services of user failed.	DN of user error message	Unable to get services. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10934	SEVERE	Getting assigned services of user failed.	DN of user error message	Unable to get services due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10941	INFO	Attempt to remove service from user	DN of user Name of service	Click on remove button in user's services page.	
10942	INFO	Removal of service from user succeeded.	DN of user Name of service	Click on remove button in user's services page.	
10943	SEVERE	Removal of service from user failed.	DN of user Name of service error message	Unable to remove services. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10944	SEVERE	Removal of service from user failed.	DN of user Name of service error message	Unable to remove services due to access management SDK exception.	Look under access management SDK log for more information.
10951	INFO	Attempt to search for user in an organization	DN of organization Search pattern	View organization's user page.	
10952	INFO	Searching for user in organization succeeded.	DN of organization Search pattern	View organization's user page.	
10953	SEVERE	Searching for user in organization failed.	DN of organization Search pattern error message	Unable to search for user. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10954	SEVERE	Searching for user in organization failed.	DN of organization Search pattern error message	Unable to search for user due to access management SDK exception.	Look under access management SDK log for more information.
10961	INFO	Attempt to modify user	DN of user	Click on Save button in user profile page.	
10962	INFO	Modification of user profile succeeded.	DN of user	Click on Save button in user profile page.	
10963	SEVERE	Modification of user profile failed.	DN of user error message	Unable to modify user. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10964	SEVERE	Modification of user profile failed.	DN of user error message	Unable to modify user due to access management SDK exception.	Look under access management SDK log for more information.
10971	INFO	Attempt to create user	DN of people container Name of user	Click on Add button in user creation page.	
10972	INFO	Creation of user succeeded.	DN of people container Name of user	Click on Add button in user creation page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10973	SEVERE	Creation of user failed.	DN of people container Name of user error message	Unable to create user. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10974	SEVERE	Creation of user failed.	DN of people container Name of user error message	Unable to create user due to access management SDK exception.	Look under access management SDK log for more information.
10981	INFO	Attempt to get attribute values of user	DN of user	View user profile page.	
10982	INFO	Getting attribute values of user succeeded.	DN of user	View user profile page.	
10983	SEVERE	Getting attribute values of user failed.	DN of user error message	Unable to get attribute values . It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10984	SEVERE	Getting attribute values of user failed.	DN of user error message	Unable to get attribute values due to access management SDK exception.	Look under access management SDK log for more information.
10991	INFO	Attempt to add service to user	DN of user Name of service	Click on add button in user's service page.	

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10992	INFO	Addition of service to user succeeded.	DN of user Name of service	Click on add button in user's service page.	
10993	SEVERE	Addition of service to user failed.	DN of user Name of service error message	Unable to add service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
10994	SEVERE	Addition of service to user failed.	DN of user Name of service error message	Unable to add service due to access management SDK exception.	Look under access management SDK log for more information.
11001	INFO	Attempt to get assigned groups of user	DN of user	View user's group page.	
11002	INFO	Getting of assigned group of user succeeded.	DN of user	View user's group page.	
11003	SEVERE	Getting of assigned group of user failed.	DN of user error message	Unable to get assigned group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
11004	SEVERE	Getting of assigned group of user failed.	DN of user error message	Unable to get assigned group due to access management SDK exception.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
11011	INFO	Attempt to remove group from user	DN of user DN of group	Click on remove button in user's group page.	
11012	INFO	Removal of group from user succeeded.	DN of user DN of group	Click on remove button in user's group page.	
11013	SEVERE	Removal of group from user failed.	DN of user DN of group error message	Unable to remove group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.
11014	SEVERE	Removal of group from user failed.	DN of user DN of group error message	Unable to remove group due to access management SDK exception.	Look under access management SDK log for more information.
11021	INFO	Attempt to add group to user	DN of user DN of group	Click on add button in user's group page.	
11022	INFO	Addition of group to user succeeded.	DN of user DN of group	Click on add button in user's group page.	
11023	SEVERE	Addition of group to user failed.	DN of user DN of group error message	Unable to add group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.	Look under access management SDK log for more information.

TABLE 9–3 Log Reference Document for Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
11024	SEVERE	Addition of group to user failed.	DN of user DN of group error message	Unable to add group due to access management SDK exception.	Look under access management SDK log for more information.

Federation

TABLE 9–4 Log Reference Document for Federation

Id	Log Level	Description	Data	Triggers	Actions
1	INFO	Authetication Domain Creation	authentication domain name	Created Authentication Domain	
2	INFO	Authentication Domain Deletion	authentication domain name	Deleted Authentication Domain	
3	INFO	Modify Authentication Domain	authentication domain name	Modified Authentication Domain	
4	INFO	Remote Provider Creation	provider id	Created Remote Provider	
5	INFO	Hosted Provider Creation	provider id	Created Hosted Provider	
6	INFO	Deleted Affliation	affliation id	Deleted Affliation	
7	INFO	Delete Entity	entity id	Deleted Entity	
8	INFO	Deleted Provider	provider id	Deleted Provider	
9	INFO	Modify Entity	entity id	Modified Entity	
10	INFO	Modify Affliation	affliation id	Modified Affliation	
11	INFO	Modify Provider	provider id	Modified Provider	

TABLE 9–4 Log Reference Document for Federation *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
12	INFO	Create Entity	entity id	Created Entity	
13	INFO	Create Affiliation	affliation id	Created Affiliation	
14	INFO	Write Account Federation Info	user DN federation info key federation info value	Acccount Federation Info with key was added to user	
15	INFO	Remove Account Federation Info	user DN provider id existing federation info key	Account federation info with key and provider ID was removed from user	
16	FINER	Create Assertion	assertion id or string	Assertion Created	
17	INFO	Liberty is not enabled.	message	Liberty is not enabled. Cannot process request.	Login to Adminstration Console to enable Federation Management in the Admin Coonsole Service.
18	INFO	Logout Request processing failed.	message	Logout Request processing failed	
19	INFO	Termination request processing failed	message	Termination request processing failed	
20	INFO	Failed in creating SOAP URL End point.	soap end point url	Failed in creating SOAP URL End point	
21	INFO	Mismatched AuthType and the protocol (based on SOAPUrl).	protocol authentication type	AuthType and the protocol (based on SOAPUrl) do not match.	

TABLE 9–4 Log Reference Document for Federation *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
22	INFO	Wrong Authentication type	authentication type	Wrong Authentication type	
23	FINER	SAML SOAP Receiver URL	soap url	SAML SOAP Receiver URL	
24	INFO	SOAP Response is Invalid	message	SOAP Response is Invalid.	
25	INFO	Assertion is invalid	message	This Assertion is invalid	
26	INFO	Single SignOn Failed	message	Single SignOn Failed	
27	INFO	Redirect to URL after granting access.	redirect url	Redirecting to URL after granting access.	
28	INFO	Authentication Response is missing	message	Authentication Response not found	
29	INFO	Account Federation Failed	message	Account Federation Failed	
30	INFO	SSOToken Generation Failed	message	Failed to generate SSOToken	
31	INFO	Authentication Response is invalid	invalid authentication response	Authentication Response is invalid	
32	INFO	Authentication Request processing failed	message	Authentication Request processing failed.	
33	INFO	Signature Verification Failed.	message	Signature Verification Failed.	
34	FINER	Created SAML Response	saml response	Created SAML Response	
35	FINER	Redirect URL	redirect url	Redirect to :	

TABLE 9–4 Log Reference Document for Federation *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
36	INFO	Common Domain Service Information not found	message	Common Domain Service Information not found.	
37	INFO	Provider is not trusted	provider id	Provider is not trusted.	
38	INFO	Authentication Request is invalid	message	Authentication Request is invalid	
39	INFO	Account Federation Information not found for user	user name	Account Federation Information not found for user :	
40	INFO	User not found.	user name	User not found.	
41	INFO	Logout profile not supported.	logout profile	Logout profile not supported.	Verify metadata is correct.
42	INFO	Logout is successful.	user name	Logout is successful.	
43	INFO	Logout failed to redirect due to incorrect URL.	message	Logout failed to redirect due to incorrect URL.	
44	INFO	Logout request not formed properly.	user name	Logout request not formed properly.	
45	INFO	Failed to get Pre/Logout handler.	logout url	Failed to get Pre/Logout handler.	
46	INFO	Single logout failed.	user name	Single logout failed.	
47	INFO	Failed to create SPProvidedNameIdentifier.	message	Failed to create SPProvidedNameIdentifier.	
48	INFO	Invalid Signature.	message	Invalid Signature.	
49	INFO	Federation Termination failed.	user name	Federation Termination failed. Cannot update account.	

TABLE 9–4 Log Reference Document for Federation *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
50	FINER	Federation Termination succeeded.	userDN	Federation Termination succeeded. User account updated.	
51	INFO	Response is Invalid	saml response	SAML Response is Invalid.	
52	INFO	Invalid Provider Registration.	provider id	Invalid Provider.	

Liberty

TABLE 9–5 Log Reference Document for Liberty

Id	Log Level	Description	Data	Triggers	Actions
1	INFO	Unable to process SASL Request	message id authentication mechanism authorization id advisory authentication id	Unable to process SASL Request.	
2	INFO	SASL Response Ok	message id authentication mechanism authorization id advisory authentication id	SASL Response Ok.	

TABLE 9–5 Log Reference Document for Liberty *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
3	INFO	Return SASL Authenticaton Response	message id authentication mechanism authorization id advisory authentication id	Returned SASL Response , continue Authentication.	
4	INFO	User not found in Data store	user name	User not found in Data store	
5	INFO	User found in Data Store	user name	User found in Data Store	
6	INFO	Cannot locate user from resourceID	resourceID	Cannot locate user from resourceID	
7	INFO	Successfully updated user profile	user name	Successfully updated user profile	
8	INFO	UnAuthorized. Failed to Query Personal Profile Service	resource id	Failed to Query Personal Profile Service	
9	INFO	Interaction Failed	resource id	Interaction with Personal Profile Service Failed	
10	INFO	Successfully queried PP Service	resource id	Personal Profile Service Query Succeeded	
11	INFO	Modify Failure	resource id	Failed to modify Personal Profile Service	
12	INFO	Modify Success	resource id	Personal Profile Service Successfully modified.	
13	INFO	Interaction Successful	successful interaction message	Successful interaction with Personal Profile Service	

TABLE 9–5 Log Reference Document for Liberty *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
14	INFO	Sending Message	request message id	Sending SOAP Request Message to WSP.	
15	INFO	Returning Response Message	response message id request message id	Returning Response Message for SOAP Request.	
16	INFO	Resending Message	message id	Resending SOAP Request Message to WSP	
17	INFO	Interaction manager redirecting user agent to interaction service	request message id	Interaction manager redirecting user agent to interaction service	
18	INFO	Interaction manager returning response element	message id reference message id cache entry status	Interaction manager returning response element	
19	INFO	Interaction query presented to user agent	message id	Interaction query presented to user agent	
20	INFO	User agent responded to interaction query	message id	User agent responded to interaction query	
21	INFO	User agent redirected back to SP	message id	User agent redirected back to SP	
22	INFO	Webservices Success	message id handler key	Webservices success.	
23	INFO	Webservices Failure	error message	Webservices Failure.	

Policy

TABLE 9–6 Log Reference Document for Policy

Id	Log Level	Description	Data	Triggers	Actions
1	INFO	Evaluating policy succeeded	policy name realm name service type name resource name action names policy decision	Evaluating policy.	
2	INFO	Getting protected policy resources succeeded	principal name resource name protecting policies	Getting protected policy resources.	
3	INFO	Creating policy in a realm succeeded	policy name realm name	Creating policy in a realm.	
4	INFO	Modifying policy in a realm succeeded	policy name realm name	Modifying policy in a realm.	
5	INFO	Removing policy from a realm succeeded	policy name realm name	Removing policy from a realm.	
6	INFO	Policy already exists in the realm	policy name realm name	Creating policy in the realm.	
7	INFO	Creating policy in a realm failed	policy name realm name	Creating policy in a realm.	Check if the user has privilege to create a policy in the realm.
8	INFO	Replacing policy in a realm failed	policy name realm name	Replacing policy in a realm.	Check if the user has privilege to replace a policy in the realm.

TABLE 9–6 Log Reference Document for Policy *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
81	INFO	Did not replace policy - A diifferent policy with the new name already exists in the realm	new policy name realm name	Replacing policy in a realm	
9	INFO	Removing policy from a realm failed	policy name realm name	Removing policy from a realm.	Check if the user has privilege to remove a policy from the realm.
10	INFO	Computing policy decision by an administrator succeeded	admin name principal name resource name policy decision	Computing policy decision by an administrator.	
11	INFO	Computing policy decision by an administrator ignoring subjects succeeded	admin name resource name policy decision	Computing policy decision by an administrator ignoring subjects.	

SAML

TABLE 9–7 Log Reference Document for SAML

Id	Log Level	Description	Data	Triggers	Actions
1	INFO	New assertion created	message id Assertion ID or Assertion if log level is LL_FINER	Browser Artifact Profile Browser POST Profile Create Assertion Artifact Authentication Query Attribute Query Authorization Decision Query	
2	INFO	New assertion artifact created	message id Assertion Artifact ID of the Assertion corresponding to the Artifact	Browser Artifact Profile Creating Assertion Artifact	
3	FINE	Assertion artifact removed from map	message id Assertion Artifact	SAML Artifact Query Assertion artifact expires	
4	FINE	Assertion removed from map	message id Assertion ID	SAML Artifact Query Assertion expires	
5	INFO	Access right by assertion artifact verified	message id Assertion Artifact	SAML Artifact Query	

TABLE 9–7 Log Reference Document for SAML *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
6	INFO	Authentication type configured and the actual SOAP protocol do not match.	message id	SAML SOAP Query	Login to console, go to Federation, then SAML, edit the Trusted Partners Configuration, check the selected Authentication Type field, make sure it matches the protocol specified in SOAP URL field.
7	INFO	Invalid authentication type	message id	SAML SOAP Query	Login to console, go to Federation, then SAML, edit the Trusted Partners Configuration, select one of the values for Authentication Type field, then save.
8	FINE	Remote SOAP receiver URL	message id SOAP Receiver URL	SAML SOAP Query	
9	INFO	No assertion present in saml response	message id SAML Response	SAML Artifact Query	Contact remote partner on what's wrong
10	INFO	Number of assertions in SAML response does not equal to number of artifacts in SAML request.	message id SAML Response	SAML Artifact Query	Contact remote partner on what's wrong
11	INFO	Artifact to be sent to remote partner	message id SAML Artifact	SAML Artifact Query	

TABLE 9–7 Log Reference Document for SAML *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
12	INFO	Wrong SOAP URL in trusted partner configuration	message id	SAML Artifact Query	Login to console, go to Federation, then SAML, edit the Trusted Partners Configuration, enter value for SOAP URL field, then save.
13	FINE	SAML Artifact Query SOAP request	message id SAML Artifact Query message	SAML Artifact Query	
14	INFO	No reply from remote SAML SOAP Receiver	message id	SAML Artifact Query	Check remote partner on what's wrong
15	FINE	SAML Artifact Query response	message id SAML Artifact Query response message	SAML Artifact Query	
16	INFO	No SAML response inside SOAP response	message id	SAML Artifact Query	Check remote partner on what's wrong
17	INFO	XML signature for SAML response is not valid	message id	SAML Artifact Query	Check remote partner on what's wrong on XML digital signature
18	INFO	Error in getting SAML response status code	message id	SAML Artifact Query	Check remote partner on what's wrong on response status code
19	INFO	TARGET parameter is missing from the request	message id	SAML Artifact Profile SAML POST Profile	Add "TARGET=target_url" as query parameter in the request

TABLE 9–7 Log Reference Document for SAML *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
20	INFO	Redirection URL in SAML artifact source site	message id target redirection URL SAML response message in case of POST profile and log level is LL_FINER	SAML Artifact Profile source SAML POST Profile source	
21	INFO	The specified target site is forbidden	message id target URL	SAML Artifact Profile source SAML POST Profile source	TARGET URL specified in the request is not handled by any trusted partner, check your TARGET url, make sure it matches one of the Target URL configured in trusted partner sites
22	INFO	Failed to create single-sign-on token	message id	SAML Artifact Profile destination SAML POST Profile destination	Authentication component failed to create SSO token, please check authentication log and debug for more details
23	INFO	Single sign on successful, access to target is granted	message id Response message in case of POST profile and log levele is LL_FINER or higher	SAML Artifact Profile destination SAML POST Profile destination	
24	INFO	Null servlet request or response	message id	SAML Artifact Profile SAML POST Profile	Check web container error log for details

TABLE 9–7 Log Reference Document for SAML *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
25	INFO	Missing SAML response in POST body	message id	SAML POST Profile destination	Check with remote SAML partner to see why SAML response object is missing from HTTP POST body
26	INFO	Error in response message	message id	SAML POST Profile destination	Unable to convert encoded POST body attribute to SAML Response object, check with remote SAML partner to see if there is any error in the SAML response create, for example, encoding error, invalid response sub-element etc.
27	INFO	Response is not valid	message id	SAML POST Profile destination	recipient attribute in SAML response does not match this site's POST profile URL Response status code is not success
28	INFO	Failed to get an instance of the message factory	message id	SAML SOAP Receiver init	Check your SOAP factory property (javax.xml.soap.MessageFactory) to make sure it is using a valid SOAP factory implementation

TABLE 9–7 Log Reference Document for SAML *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
29	INFO	Received Request from an untrusted site	message id Remote site Hostname or IP Address	SAML SOAP Queries	Login to console, go to Federation, then SAML service, edit the Trusted Partners Configuration, check the Host List field, make sure remote host/IP is one the values. In case of SSL with client auth, make sure Host List contains the client certificate alias of the remote site.
30	INFO	Invalid request from remote partner site	message id and request hostname/IP address return response	SAML SOAP Queries	Check with administrator of remote partner site
31	FINE	Request message from partner site	message id and request hostname/IP address request xml	SAML SOAP Queries	
32	INFO	Failed to build response due to internal server error	message id	SAML SOAP Queries	Check debug message to see why it is failing, for example, cannot create response status, major/minor version error, etc.
33	INFO	Sending SAML response to partner site	message id SAML response or response id	SAML SOAP Queries	

TABLE 9–7 Log Reference Document for SAML *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
34	INFO	Failed to build SOAP fault response body	message id	SAML SOAP Queries	Check debug message to see why it is failing, for example, unable to create SOAP fault, etc.

Session

TABLE 9–8 Log Reference Document for Session

Id	Log Level	Description	Data	Triggers	Actions
1	INFO	Session is Created	User ID	User is authenticated.	
2	INFO	Session has idle timeout	User ID	User session idle for long time.	
3	INFO	Session has Expired	User ID	User session has reached its maximun time limit.	
4	INFO	User has Logged out	User ID	User has logged out of the system.	
5	INFO	Session is Reactivated	User ID	User session state is active.	
6	INFO	Session is Destroyed	User ID	User session is destroyed and cannot be referenced.	
7	INFO	Session's property is changed.	User ID	User changed session's unprotected property.	
8	INFO	Session received Unknown Event	User ID	Unknown session event	

TABLE 9–8 Log Reference Document for Session *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
9	INFO	Attempt to set protected property	User ID	Attempt to set protected property	
10	INFO	User's session quota has been exhausted.	User ID	Session quota exhausted	
11	INFO	Session database used for session failover and session constraint is not available.	User ID	Unable to reach the session database.	
12	INFO	Session database is back online.	User ID	Session database is back online.	
13	INFO	The total number of valid sessions hosted on the AM server has reached the max limit.	User ID	Session max limit reached.	