Sun Java System Access Manager 7 2005Q4 Administration Guide

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

Part No: 819–2137–11
2005

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.

CETTE PUBLICATION EST FOURNIE “EN L'ETAT” ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REPONDRE A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.

Contents

Preface 13

Part I **Access Manager Configuration** 19

1 **Access Manager 7 2005Q4 Configuration Scripts** 21

Access Manager 7 2005Q4 Installation Overview 21

Access Manager `amconfig` Script Operations 23

Access Manager Sample Configuration Script Input File 23

Deployment Mode Variable 24

Access Manager Configuration Variables 25

Web Container Configuration Variables 28

Directory Server Configuration Variables 33

Access Manager `amconfig` Script 34

Access Manager Deployment Scenarios 35

Deploying Additional Instances of Access Manager 35

Configuring and Reconfiguring an Instance of Access Manager 37

Uninstalling Access Manager 38

Uninstalling All Access Manager Instances 38

Example Configuration Script Input File 39

2 **Installing and Configuring Third-Party Web Containers** 41

Installing and Configuring BEA WebLogic 8.1 41

▼ To Install and Configure WebLogic 8.1 41

Installing and Configuring IBM WebSphere 5.1 42

▼ To Install and Configure WebSphere 5.1 42

Using Java ES to Install Directory Server and Access Manager 44

▼ To Install Directory Server 44

Configuring Access Manager 44

▼ To Configure Access Manager 44

Creating the Configuration Script Input File 45

Running the Configuration Script 46

Restarting the Web Container 46

3 Configuring Access Manager in SSL Mode 47

Configuring Access Manager With a Secure Sun Java Enterprise System Web Server 47

▼ To Configure a Secure Web Server 47

Configuring Access Manager with a Secure Sun Java System Application Server 50

Setting Up Application Server 6.2 With SSL 50

Configuring Application Server 8.1 With SSL 53

Configuring Access Manager in SSL Mode 53

Configuring AMSDK with a Secure BEA WebLogic Server 54

▼ To Configure a Secure WebLogic Instance 54

Configuring AMSDK with a Secure IBM WebSphere Application Server 55

▼ To Configure a Secure WebSphere Instance 56

Configuring Access Manager to Directory Server in SSL Mode 56

Configuring Directory Server in SSL Mode 57

Connecting Access Manager to the SSL-enabled Directory Server 57

Part II Access Control 59

4 The Access Manager Console 61

Administration View 61

Realms Mode Console 61

Legacy Mode Console 62

User Profile View 64

5 Managing Realms 67

Creating and Managing Realms 67

▼ To Create a New Realm 67

General Properties 68

Authentication 68

Services 69
▼ To Add a Service to a Realm 69
Privileges 70

6 **Data Stores** 71
LDAPv3 Data Store 71
▼ To Create a New LDAPv3 Data Store 72
LDAPv3 Repository Plug-in Attributes 72
AMSDK Repository Plug-in 78
▼ To Create a New AMSDK Repository Plugin 78

7 **Managing Authentication** 81
Configuring Authentication 81
Authentication Module Types 81
Authentication Module Instances 91
Authentication Chaining 92
▼ To Create a New Authentication Chain 92
Authentication Types 94
How Authentication Types Determine Access 94
Realm-based Authentication 96
Organization-based Authentication 98
Role-based Authentication 101
Service-based Authentication 104
User-based Authentication 107
Authentication Level-based Authentication 109
Module-based Authentication 112
The User Interface Login URL 114
Login URL Parameters 114
Account Locking 120
Physical Locking 121
Authentication Service Failover 122
Fully Qualified Domain Name Mapping 123
Possible Uses For FQDN Mapping 123
Persistent Cookie 124
▼ To Enable Persistent Cookies 124

Multi-LDAP Authentication Module Configuration In Legacy Mode 124
▼ To Add An Additional LDAP Configuration 125
Session Upgrade 127
Validation Plug-in Interface 128
▼ To Write and Configure a Validation Plug-in 128
JAAS Shared State 128
Enabling JAAS Shared State 129

8 Managing Policies 131
Overview 131
Policy Management Feature 132
URL Policy Agent Service 132
Policy Types 134
Normal Policy 134
Referral Policy 139
Policy Definition Type Document 139
Policy Element 140
Rule Element 140
Subjects Element 141
Subject Element 142
Referrals Element 142
Referral Element 142
Conditions Element 142
Condition Element 143
Adding a Policy Enabled Service 143
▼ To Add a New Policy Enabled Service 143
Creating Policies 144
▼ To Create Policies with amadmin 144
▼ To Create a Normal Policy With the Access Manager Console 145
▼ To Create a Referral Policy With the Access Manager Console 145
Creating Policies for Peer Realms and Sub Realms 146
Managing Policies 147
Modifying a Normal Policy 147
Modifying a Referral Policy 150
Policy Configuration Service 153

Subjects Result Time To Live 153
Dynamic Attributes 153
amldapuser Definition 153
Adding Policy Configuration Services 153
Resource—Based Authentication 154
Limitations 154

9 Managing Subjects 157
User 157
▼ To Create or Modify a User 157
▼ To Add a User to Roles and Groups 158
▼ To Add Services to an Identity 158
Agents 159
▼ To Create or Modify an Agent 159
Creating a Unique Policy Agent Identity 160
Filtered Role 162
▼ To Create a Filtered Role 162
Roles 162
▼ To Create or Modify a Role 162
▼ To Add Users to a Role or Group 163
Groups 163
▼ To Create or Modify a Group 163

Part III Directory Management and Default Services 165

10 Directory Management 167
Managing Directory Objects 167
Organizations 167
Containers 170
Group Containers 171
Groups 172
People Containers 175
Users 176
Roles 179

11 **Current Sessions** 187

The Current Sessions Interface 187

Session Management 187

Session Information 187

Terminating a Session 188

12 **Password Reset Service** 189

Registering the Password Reset Service 189

▼ To Register Password Reset for Users in a Different Realm 189

Configuring the Password Reset Service 190

▼ To Configure the Service 190

Password Reset Lockout 191

Password Reset for End Users 192

Customizing Password Reset 192

Resetting Forgotten Passwords 192

Password Policies 193

13 **Logging Service** 195

Log Files 195

Access Manager Service Logs 195

Session Logs 196

Console Logs 196

Authentication Logs 196

Federation Logs 196

Policy Logs 196

Agent Logs 197

SAML Logs 197

amAdmin Logs 197

Logging Features 197

Secure Logging 197

Command Line Logging 198

Logging Properties 198

Remote Logging 199

Error and Access Logs 201

Debug Files 202

Debug Levels 202
Debug Output Files 203
Using Debug Files 203
Multiple Access Manager Instances And Debug Files 204

Part IV Command Line Reference 205

14 The amadmin Command Line Tool 207
The amadmin Command Line Executable 207
The amadmin Syntax 208
Using amadmin for Federation Management 211
Using amadmin for Resource Bundles 213

15 The ampassword Command Line Tool 215
The ampassword Command Line Executable 215
▼ To Run ampassword with Access Manager in SSL mode 215

16 The bak2am Command Line Tool 217
The bak2am Command Line Executable 217
The bak2am Syntax 217

17 The am2bak Command Line Tool 219
The am2bak Command Line Executable 219
The am2bak Syntax 219

18 The amserver Command Line Tool 223
The amserver Command Line Executable 223
amserver Syntax 223

19 The VerifyArchive Command Line Tool 225
The VerifyArchive Command Line Executable 225
VerifyArchive Syntax 225

20 The amsecuridd Helper 227

The amsecuridd Helper Command Line Executable 227

amsecuridd Syntax 228

Running the amsecuridd helper 228

Part V Appendixes 231

A AMConfig.properties File 233

About the `AMConfig.properties` File 234

Access Manager Console 234

Access Manager Server Installation 234

am.util 236

amSDK 236

Application Server Installation 236

Authentication 237

Certificate Database 238

Cookies 238

Debugging 239

Directory Server Installation 240

Event Connection 240

Global Services Management 241

Helper Daemons 241

Identity Federation 242

JSS Proxy 243

LDAP Connection 244

Liberty Alliance Interactions 244

Logging Service 247

Logging Properties You Can Add to AMConfig.properties 247

Naming Service 249

Notification Service 249

Policy Agents 249

Policy Client API 251

Profile Service 252

Replication 252

SAML Service 252

Security 253
Session Service 254
SMTP 255
Statistics Service 255

B serverconfig.xml File 257
Overview 257
Proxy User 257
Admin User 258
server-config Definition Type Document 258
iPlanetDataAccessLayer Element 259
ServerGroup Element 259
Server Element 259
User Element 259
BaseDN Element 260
MiscConfig Element 260
Failover Or Multimaster Configuration 261

C Log File Reference 263

D Error Codes 399
Access Manager Console Errors 399
Authentication Error Codes 401
Policy Error Codes 404
amadmin Error Codes 406

Index 413

Preface

The *Sun Java System Access Manager 7 2005Q4 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 2005Q4 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" on page 14
- "Sun Java Enterprise System Product Documentation" on page 15

Access Manager Core Documentation

The Access Manager core documentation set contains the following titles:

- The *Sun Java System Access Manager 7 2005Q4 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 2005Q4 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 2005Q4 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 2005Q4 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 2005Q4 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 2005Q4 Federation and SAML Administration Guide* (this 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 2005Q4 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 2005Q4 C API Reference* provides summaries of data types, structures, and functions that make up the public Access Manager C APIs.
- The *Java API Reference* (part number 819-2141) 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

Sun Function	URL	Description
Documentation	`http://www.sun.com/documentation/`	Download PDF and HTML documents, and order printed documents
Support and Training	`http://www.sun.com/supportraining/`	Obtain technical support, download patches, and learn about Sun courses

Typographic Conventions

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

TABLE P–1 Typographic Conventions

Typeface or Symbol	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*. Perform a *patch analysis*. Do *not* save the file. [Note that some emphasized items appear bold online.]

Shell Prompts in Command Examples

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

TABLE P–2 Shell Prompts

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

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 2005Q4 Deployment Planning Guide*, and the part number is 819-2136.

PART I

Access Manager Configuration

This is part one of the Sun Java System Access Manager™ 7 2005Q4 Administration Guide. It discusses configuration options that you can perform after Access Manager installation. This part contains the following chapters:

- Chapter 1, "Access Manager 7 2005Q4 Configuration Scripts"
- Chapter 2, "Installing and Configuring Third-Party Web Containers"
- Chapter 3, "Configuring Access Manager in SSL Mode"

CHAPTER 1

Access Manager 7 2005Q4 Configuration Scripts

This chapter describes how to configure and deploy Sun Java^{TM} System Access Manager using the amconfig script and the sample silent mode input file (amsamplesilent). Topics include:

- "Access Manager 7 2005Q4 Installation Overview" on page 21
- "Access Manager Sample Configuration Script Input File" on page 23
- "Access Manager amconfig Script" on page 34
- "Access Manager Deployment Scenarios" on page 35
- "Example Configuration Script Input File" on page 39

Access Manager 7 2005Q4 Installation Overview

For a new installation, always install the first instance of Access Manager 7 2005Q4 by running the Sun Java Enterprise System (Java ES) installer. When you run the installer, you can select either of these configuration options for Access Manager:

- The Configure Now option allows you to install and configure the first instance during the installation by the choices (or default values) that you select on the Access Manager installation panels.
- The Configure Later option installs the Access Manager 7 2005Q4 components, and then after installation, you must manually configure them or run the Access Manager scripts as described in "Configuring and Reconfiguring an Instance of Access Manager" on page 37. If you choose this option, then none of the products that you are currently installing will be configured. For example, if you choose to install Access Manager and Application Server and select the Configure Later option, neither application will be configured.

Note – If you are installing BEA WebLogic or IBM WebSphere Application Server as the Access Manager web container, you must choose the Configure Later option when installing Access Manager. See Chapter 2, "Installing and Configuring Third-Party Web Containers," for more information.

For information about the installer, refer to the *Sun Java Enterprise System 2005Q4 Installation Guide for UNIX*.

The Java Enterprise System installer installs the Access Manager 7 2005Q4 `amconfig` script and sample silent mode input file (`amsamplesilent`) in the *AccessManager-base* `/SUNWam/bin` directory on Solaris systems or the *AccessManager-base*`/identity/bin` directory on Linux systems.

AccessManager-base represents the Access Manager base installation directory. On Solaris systems, the default base installation directory is `/opt`, and on Linux systems, it is `/opt/sun`. However, you can specify another directory, if you prefer, when you run the installer.

The `amconfig` script is a top-level script that calls other scripts as needed to perform the requested operation. For more information, see the "Access Manager `amconfig` Script" on page 34.

The sample configuration script input file (`amsamplesilent`) is a template that you can use to create the input file that you must specify when you run the `amconfig` script in silent mode.

This sample configuration script input file is an ASCII text file that contains Access Manager configuration variables. Before you run the `amconfig` script, copy (and rename, if you wish) the `amsamplesilent` file, and then edit the variables in the file based on your system environment. The configuration variables are in the following format:

`variable-name=`*value*

For example:

```
DEPLOY_LEVEL=1
 NEW_INSTANCE=true
 SERVER_HOST=ishost.example.com
```

For a list of the variables you can set in a configuration script input file, see the "Access Manager Sample Configuration Script Input File" on page 23"Access Manager Sample Configuration Script Input File" on page 23.

Caution – The format of the sample configuration script input file used when you run the `amconfig` script in silent mode does not follow the same format or necessarily use the same variable names as a Java Enterprise System silent installation state file. This file contains sensitive data, such as the administrator password. Make sure to protect or delete this file as appropriate.

Access Manager `amconfig` Script Operations

After you install first instance of Access Manager using the Sun Java Enterprise System installer, you can run the `amconfig` script to perform the following operations, depending on the values of the variables in the silent mode input file:

- Deploy and configure the first instance of Access manager or deploy and configure for additional instances of Access Manager on the same host system. For example, after you configure an additional instance of a web container, you can then deploy and configure a new Access Manager instance for that web container instance.
- Reconfigure both the first instance and any additional instances of Access Manager.
- Deploy and configure the Access Manager full server services or only the SDK services, which enables support for these products:
  - BEA WebLogic
  - IBM WebSphere Application Server

  Deploy and configure specific Access Manager components such as the console or Federation Management module.
- Uninstall instances and components of Access Manager that you deployed using the `amconfig` script.

Access Manager Sample Configuration Script Input File

After you run the Java Enterprise System installer, the Access Manager sample configuration script input file (`amsamplesilent`) is available in the *AccessManager-base*`/SUNWam/bin` directory on Solaris systems or the *AccessManager-base*`/identity/bin` directory on Linux systems.

To set configuration variables, first copy and rename the `amsamplesilent` file. Then set the variables in the copy for the operation you want to perform. For an example of this file, see "Example Configuration Script Input File" on page 39.

This sample silent mode input file contains the following configuration variables:

- "Deployment Mode Variable" on page 24

- "Access Manager Configuration Variables" on page 25
- "Web Container Configuration Variables" on page 28
- "Directory Server Configuration Variables" on page 33

Deployment Mode Variable

This section describes the values for the required DEPLOY_LEVEL variable. This variable determines the operation you want the `amconfig` script to perform.

TABLE 1–1 Access Manager DEPLOY_LEVEL Variable

Operation	DEPLOY_LEVEL Variable Value and Description
Install	1 = Full Access Manager installation for a new instance (default) 2 = Install Access Manager console only 3 = Install Access Manager SDK only 4 = Install SDK only and configure the container 5 = Install Federation Management module only 6 = Install server only 7=Install Access Manager and configure the container for deploying with Portal Server. **Caution** DEPLOY_MODE=7 is intended only for deploying Access Manager with Portal Server. For some deployments, you might want to install the console only and server only on a single host server using different web containers. First, run the Java ES installer to install all Access Manager subcomponents using the Configure Later option. Then, run the `amconfig` script to configure both the console and server instances.
Uninstall (unconfigure)	11 = Full uninstall 12 = Uninstall console only 13 = Uninstall SDK only 14 = Uninstall SDK only and unconfigure the container 15 = Uninstall Federation Management module 16 = Uninstall server only Uninstall Access Manager and unconfigure the container when deployed with Portal Server. **Caution** DEPLOY_MODE=7 is intended only when Access Manager is deployed with Portal Server.

TABLE 1–1 Access Manager DEPLOY_LEVEL Variable *(Continued)*

Operation	DEPLOY_LEVEL Variable Value and Description
Re-install (also referred to as re-deploy or re-configure)	21 = Redeploy all (console, password, services, and common) web applications. 26 = Undeploy all (console, password, services, and common) web applications.

Access Manager Configuration Variables

This section describes the Access Manager configuration variables.

TABLE 1–2 Access Manager Configuration Variables

Variable	Description
AM_REALM	Indicates the Access Manager mode: ■ enabled: Access Manager operates in Realm Mode, with Access Manager 7 2005Q4 features and console. ■ disabled: Access Manager operates in Legacy Mode, with Access Manager 6 2005Q1 features and console. Default: enabled **Caution –** Access Manager Realm Mode is enabled by default. If you are deploying Access Manager with Portal Server, Messaging Server, Calendar Server, Delegated Administrator, or Instant Messaging, you must select Legacy Mode (AM_REALM=disabled) before you run the `amconfig` script.
BASEDIR	Base installation directory for Access Manager packages. Default: PLATFORM_DEFAULT For Solaris systems, PLATFORM_DEFAULT is `/opt` For Linux systems, PLATFORM_DEFAULT is `/opt/sun`
SERVER_HOST	Fully qualified host name of the system where Access Manager is running (or will be installed). For a remote SDK installation, set this variable to the host where Access Manager is (or will be) installed and not the remote client host. This variable should match the counterpart variable in the web container configuration. For example, for Application Server 8, this variable should match AS81_HOST.

TABLE 1–2 Access Manager Configuration Variables *(Continued)*

Variable	Description
SERVER_PORT	Access Manager port number. Default: 58080 For a remote SDK installation, set this variable to the port on the host where Access Manager is (or will be) installed and not the remote client host. This variable should match the counterpart variable in the web container configuration. For example, for Application Server 8, this variable should match AS81_PORT.
SERVER_PROTOCOL	Server protocol: http or https. Default: http For a remote SDK installation, set this variable to the protocol on the host where Access Manager is (or will be) installed and not the remote client host. This variable should match the counterpart variable in the web container configuration. For example, for Application Server 8, this variable should match AS81_PROTOCOL.
CONSOLE_HOST	Fully qualified host name of the server where the console is installed. Default: Value provided for the Access Manager host
CONSOLE_PORT	Port of the web container where the console is installed and listens for connections. Default: Value provided for the Access Manager port
CONSOLE_PROTOCOL	Protocol of the web container where the console is installed. Default: Server protocol
CONSOLE_REMOTE	Set to true if the console is remote from the Access Manager services. Otherwise, set to false. Default: false
DS_HOST	Fully qualified host name of Directory Server.
DS_PORT	Directory Server port. Default: 389.
DS_DIRMGRDN	Directory manager DN: the user who has unrestricted access to Directory Server. Default: `"cn=Directory Manager"`
DS_DIRMGRPASSWD	Password for the directory manager See the note about special characters in the description of "Access Manager Configuration Variables" on page 25.
ROOT_SUFFIX	Initial or root suffix of the directory. You must make sure that this value exists in the Directory Server you are using. See the note about special characters in the description of "Access Manager Configuration Variables" on page 25.

TABLE 1–2 Access Manager Configuration Variables *(Continued)*

Variable	Description
ADMINPASSWD	Password for the administrator (`amadmin`). Must be different from the password for `amldapuser`. **Note**: If the password contains special characters such as a slash (/) or backslash (\\), the special character must be enclosed by single quotes (”). For example: `ADMINPASSWD=’\\\\\\\\\\####///’` However, the password cannot have a single quote as one of the actual password characters.
AMLDAPUSERPASSWD	Password for `amldapuser`. Must be different from the password for `amadmin`. See the note about special characters in the description of “Access Manager Configuration Variables” on page 25.
CONSOLE_DEPLOY_URI	URI prefix for accessing the HTML pages, classes and JAR files associated with the Access Manager Administration Console subcomponent. Default: `/amconsole`
SERVER_DEPLOY_URI	URI prefix for accessing the HTML pages, classes, and JAR files associated with the Identity Management and Policy Services Core subcomponent. Default: `/amserver`
PASSWORD_DEPLOY_URI	URI that determines the mapping that the web container running Access Manager will use between a string you specify and a corresponding deployed application. Default: `/ampassword`
COMMON_DEPLOY_URI	URI prefix for accessing the common domain services on the web container. Default: `/amcommon`
COOKIE_DOMAIN	Names of the trusted DNS domains that Access Manager returns to a browser when it grants a session ID to a user. At least one value should be present. In general, the format is the server’s domain name preceded with a period. Example: `.example.com`
JAVA_HOME	Path to the JDK installation directory. Default: `/usr/jdk/entsys-j2se`. This variable provides the JDK used by the command line interface’s (such as `amadmin`) executables. The version must be 1.4.2 or later.

TABLE 1–2 Access Manager Configuration Variables *(Continued)*

Variable	Description
AM_ENC_PWD	Password encryption key: String that Access Manager uses to encrypt user passwords. Default: none. When the value is set to none, `amconfig` will generate a password encryption key for the user, so a password encryption will exist for the installation that is either specified by the user or created through `amconfig` . **Important**: If you are deploying multiple instances of Access Manager or the remote SDK, all instances must use the same password encryption key. When you deploy an additional instance, copy the value from the `am.encryption.pwd` `property` in the `AMConfig.properties` file for the first instance.
PLATFORM_LOCALE	Locale of the platform. Default: `en_US` (US English)
NEW_OWNER	New owner for the Access Manager files after installation. Default: `root`
NEW_GROUP	New group for the Access Manager files after installation. Default: `other` For a Linux installation, set NEW_GROUP to `root`.
PAM_SERVICE_NAME	Name of the PAM service from the PAM configuration or stack that comes with the operating system and is used for the Unix authentication module (normally `other` for Solaris or `password` for Linux). Default: `other`.
XML_ENCODING	XML encoding. Default: `ISO-8859-1`
NEW_INSTANCE	Specifies whether the configuration script should deploy Access Manager to a new user-created web container instance: ■ true = To deploy Access Manager to a new user-created web container instance other than an instance that already exists. ■ false = To configure the first instance or re-configure an instance. Default: false
SSL_PASSWORD	Is not used in this release.

Web Container Configuration Variables

To specify the web container for Access Manager, set the WEB_CONTAINER variable in the silent mode input file. For the versions of the web containers supported by Access Manager 7 2005Q4, see the *Sun Java System Access Manager 7 2005Q4 Release Notes*.

TABLE 1–3 Access Manager WEB_CONTAINER Variable

Value	Web Container
WS6 (default)	“Sun Java System Web Server 6.1 SP5” on page 29

TABLE 1–3 Access Manager WEB_CONTAINER Variable *(Continued)*

Value	Web Container
AS8	"Sun Java System Application Server 8.1" on page 30
WL8	"BEA WebLogic Server 8.1" on page 31
WAS5	"IBM WebSphere 5.1" on page 32

Sun Java System Web Server 6.1 SP5

This section describes the configuration variables for Web Server 6.1 2005Q4 SP5 in the silent mode input file.

TABLE 1–4 Web Server 6.1 Configuration Variables

Variable	Description
WS61_INSTANCE	Name of the Web Server instance on which Access Manager will be deployed or un-deployed. Default: https-*web-server-instance-name* where *web-server-instance-name* is the Access Manager host ("Access Manager Configuration Variables" on page 25 variable)
WS61_HOME	Web Server base installation directory. Default: `/opt/SUNWwbsvr`
WS61_PROTOCOL	Protocol used by the Web Server instance set by the "Sun Java System Web Server 6.1 SP5" on page 29 variable where Access Manager will be deployed: http or https. Default: Access Manager protocol ("Access Manager Configuration Variables" on page 25 variable)
WS61_HOST	Fully qualified host name for the Web Server instance ("Sun Java System Web Server 6.1 SP5" on page 29 variable). Default: Access Manager host instance ("Access Manager Configuration Variables" on page 25 variable)
WS61_PORT	Port on which Web Server listens for connections. Default: Access Manager port number ("Access Manager Configuration Variables" on page 25 variable)
WS61_ADMINPORT	Port on which the Web Server Administration Server listens for connections. Default: 8888

TABLE 1–4 Web Server 6.1 Configuration Variables *(Continued)*

Variable	Description
WS61_ADMIN	User ID of the Web Server administrator. Default: "admin"

Sun Java System Application Server 8.1

This section describes the configuration variables for Application Server 8.1 in the silent mode input file.

TABLE 1–5 Application Server 8.1 Configuration Variables

Variable	Description
AS81_HOME	Path to the directory where Application Server 8.1 is installed. Default: /opt/SUNWappserver/appserver
AS81_PROTOCOL	Protocol used by the Application Server instance: http or https. Default: Access Manager protocol ("Access Manager Configuration Variables" on page 25 variable)
AS81_HOST	Fully qualified domain name (FQDN) on which the Application Server instance listens for connections. Default: Access Manager host ("Access Manager Configuration Variables" on page 25 variable)
AS81_PORT	Port on which Application Server instance listens for connections. Default: Access Manager port number ("Access Manager Configuration Variables" on page 25 variable)
AS81_ADMINPORT	Port on which the Application Server administration server listens for connections. Default: 4849
AS81_ADMIN	Name of the user who administers the Application Server administration server for the domain into which Application Server is being displayed. Default: admin
AS81_ADMINPASSWD	Password for the Application Server administrator for the domain into which Application Server is being displayed. See the note about special characters in the description of "Access Manager Configuration Variables" on page 25.
AS81_INSTANCE	Name of the Application Server instance that will run Access Manager. Default: server

TABLE 1–5 Application Server 8.1 Configuration Variables *(Continued)*

Variable	Description
AS81_DOMAIN	Path to the Application Server directory for the domain to which you want to deploy this Access Manager instance. Default: `domain1`
AS81_INSTANCE_DIR	Path to the directory where Application Server stores files for the instance. Default: `/var/opt/SUNWappserver/domains/domain1`
AS81_DOCS_DIR	Directory where Application Server stores content documents. Default: `/var/opt/SUNWappserver/domains/domain1/docroot`
AS81_ADMIN_IS_SECURE	Specifies whether the Application Server administration instance is using SSL: ■ true: Secure port is enabled (HTTPS protocol). ■ false: Secure port is not enabled (HTTP protocol). Default: true (enabled) In `ampsamplesilent`, there is an additional setting that specified whether the application server administration port is secure: ■ true: The application server administration port is secure (HTTPS protocol). ■ false: The application server administration port is not secure (HTTP protocol). Default: True (enabled).

BEA WebLogic Server 8.1

This section describes the configuration variables for BEA WebLogic Server 8.1 in the silent mode input file.

TABLE 1–6 BEA WebLogic Server 8.1 Configuration Variables

Variable	Description
WL8_HOME	WebLogic home directory. Default: `/usr/local/bea`
WL8_PROJECT_DIR	WebLogic project directory. Default: `user_projects`
WL8_DOMAIN	WebLogic domain name. Default: `mydomain`
WL8_SERVER	WebLogic server name. Default: `myserver`
WL8_INSTANCE	WebLogic instance name. Default: `/usr/local/bea/weblogic81 ($WL8_HOME/weblogic81)`
WL8_PROTOCOL	WebLogic protocol. Default: http

TABLE 1–6 BEA WebLogic Server 8.1 Configuration Variables *(Continued)*

Variable	Description
WL8_HOST	WebLogic host name. Default: Host name of the server
WL8_PORT	WebLogic port. Default: 7001
WL8_SSLPORT	WebLogic SSL port. Default: 7002
WL8_ADMIN	WebLogic administrator. Default: "`weblogic`"
WL8_PASSWORD	WebLogic administrator password. See the note about special characters in the description of "Access Manager Configuration Variables" on page 25.
WL8_JDK_HOME	WebLogic JDK home directory. Default: "BEA WebLogic Server 8.1" on page 31 `/jdk142_04`
WL8_CONFIG_LOCATION	Should be set to the parent directory of the location of the WebLogic start script.

IBM WebSphere 5.1

This section describes the configuration variables for IBM WebSphere Server 5.1 in the silent mode input file.

TABLE 1–7 IBM WebSphere 5.1 Configuration Variables

Variable	Description
WAS51_HOME	WebSphere home directory. Default: `/opt/WebSphere/AppServer`
WAS51_JDK_HOME	WebSphere JDK home directory. Default: `/opt/WebSphere/AppServer/java`
WAS51_CELL	WebSphere cell. Default: hostname value
WAS51_NODE	WebSphere node name. Default: host name of the server where WebSphere is installed. Default: hostname value
WAS51_INSTANCE	WebSphere instance name. Default: `server1`
WAS51_PROTOCOL	WebSphere protocol. Default: http
WAS51_HOST	WebSphere host name. Default: Hostname of the server
WAS51_PORT	WebSphere port. Default: 9080
WAS51_SSLPORT	WebSphere SSL port. Default: 9081
WAS51_ADMIN	WebSphere administrator. Default: "`admin`"
WAS51_ADMINPORT	WebSphere administrator port. Default: 9090

Directory Server Configuration Variables

For the versions of Directory Server supported by Access Manager 7 2005Q4, see the *Sun Java System Access Manager 7 2005Q4 Release Notes*. This section describes the Directory Server configuration variables in the silent mode input file.

TABLE 1–8 Directory Server Configuration Variables

Variable	Description
DIRECTORY_MODE	Directory Server modes: 1 = Use for a new installation of a Directory Information Tree (DIT). 2 = Use for an existing DIT. The naming attributes and object classes are the same, so the configuration scripts load the `installExisting.ldif` and `umsExisting.ldif` files. The configuration scripts also update the LDIF and properties files with the actual values entered during configuration (for example, BASE_DIR, SERVER_HOST, and ROOT_SUFFIX). This update is also referred to as "tag swapping," because the configuration scripts replace the placeholder tags in the files with the actual configuration values. 3 = Use for an existing DIT when you want to do a manual load. The naming attributes and object classes are different, so the configuration scripts do not load the `installExisting.ldif` and `umsExisting.ldif` files. The scripts perform tag swapping (described for mode 2). You should inspect and modify (if needed) the LDIF files and then manually load the LDIF files and services. 4 = Use for an existing multi-server installation. The configuration scripts do not load the LDIF files and services, because the operation is against an existing Access Manager installation. The scripts perform tag swapping only (described for mode 2) and adds a server entry in the platform list. 5 = Use for an existing upgrade. The scripts perform tag swapping only (described for mode 2). Default: 1
USER_NAMING_ATTR	User naming attribute: Unique identifier for the user or resource within its relative name space. Default: `uid`
ORG_NAMING_ATTR	Naming attribute of the user's company or organization. Default: `o`
ORG_OBJECT_CLASS	Organization object class. Default: `sunismanagedorganization`
USER_OBJECT_CLASS	User object class. Default: `inetorgperson`
DEFAULT_ORGANIZATION	Default organization name. Default: none

Access Manager `amconfig` Script

After you run the Java Enterprise System installer, the `amconfig` script is available in the *AccessManager-base* `/SUNWam/bin` directory on Solaris systems or the *AccessManager-base*`/identity/bin` directory on Linux systems.

The `amconfig` script reads a silent configuration input file and then calls other scripts in silent mode, as needed, to perform the requested operation.

To run the `amconfig` script, use this syntax:

```
amconfig -s
          input-file
```

where:

-s runs `amconfig` in silent mode.

`input-file` is the silent configuration input file that contains the configuration variables for the operation you want to perform. For more information, see "Access Manager Sample Configuration Script Input File" on page 23.

Several considerations for running the `amconfig` script are:

- You must be running as superuser (`root`).
- Specify the full path to the `amsamplesilent` file (or copy of the file). For example:

  ```
  # cd /opt/SUNWam/bin
  # ./amconfig -s ./amsamplesilent
  ```

  or

  ```
  # ./amconfig -s /opt/SUNWam/bin/amsamplesilent
  ```

Note – In the Access Manager 7 2005Q4 release, the following scripts are not supported:

- `amserver` with the create argument
- `amserver.`*instance*

Also, by default `amserver start` starts only the authentication `amsecuridd` and `amunixd` helpers. The `amsecuridd` helper is available only on the Solaris OS SPARC platform.

Access Manager Deployment Scenarios

After you have installed the first instance of Access Manager using the Java Enterprise System installer, you can deploy and configure additional Access Manager instances by editing the configuration variables in the silent configuration input file and then running the `amconfig` script.

This section describes the following scenarios:

- "Deploying Additional Instances of Access Manager" on page 35
- "Configuring and Reconfiguring an Instance of Access Manager" on page 37
- "Uninstalling Access Manager" on page 38
- "Uninstalling All Access Manager Instances" on page 38

Deploying Additional Instances of Access Manager

Before you can deploy a new instance of Access Manager, you must create and start the new web container instance using the administration tools for the web container. For information, refer to the specific web container documentation:

- For Web Server, see `http://docs.sun.com/coll/1308.1`
- For Application Server, see `http://docs.sun.com/coll/1310.1`

The steps described in this section only apply to an Access Manager instance that has been installed with the Configure Now option. If you are planning to use WebLogic or WebSphere as web containers, you must use the Configure Later option when installing Access Manager. See Chapter 2, "Installing and Configuring Third-Party Web Containers," for more information.

Deploying an Additional Access Manager Instance

This section describes how to deploy an additional Access Manager instance on a different host server and update the Platform Server List.

▼ To Deploy an Additional Access Manager Instance

1 **Log in as an administrator, depending on the web container for the instance. For example, if Web Server 6.1 will be the web container for the new instance, log in either as superuser (root) or as the user account for the Web Server Administration Server.**

2 **Copy the `amsamplesilent` file to a writable directory and make that directory your current directory. For example, you might create a directory named `/newinstances`.**

Tip Rename the copy of the `amsamplesilent` file to describe the new instance you want to deploy. For example, the following steps use an input file named `amnewws6instance` to install a new instance for Web Server 6.1.

3 **Set the following variables in the new `amnewws6instance` file:**

```
DEPLOY_LEVEL=1
 NEW_INSTANCE=true
```

Set other variables in the `amnewws6instance` file as required for the new instance you want to create. For a description of these variables, refer to the tables in the following sections:

- "Access Manager Configuration Variables" on page 25
  - "Web Container Configuration Variables" on page 28
  - "Directory Server Configuration Variables" on page 33

  Important All Access Manager instances must use the same value for the password encryption key. To set the AM_ENC_PWD variable for this instance, copy the value from the `am.encryption.pwd` property in the `AMConfig.properties` file for the first instance.

  In case you might need to uninstall this instance later, save the `amnewws6instance` file.

4 **Run the `amconfig`, specifying the new `amnewws6instance` file. For example, on Solaris systems:**

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./newinstances/amnewws6instance
```

The `-s` option runs the `amconfig` script in silent mode.

The `amconfig` script calls other configuration scripts as needed, using variables in the `amnewws6instance` file to deploy the new instance.

▼ To Update the Platform Server List

When you crate an additional container instance, you must update the Access Manager Platform Server list to reflect the addition of the container(s).

1 **Log in to the Access Manager Console as the top-level administrator.**

2 **Click on the Service Configuration tab.**

3 **Click on the Platform service.**

4 **Enter the following information for the new instance in the Server List:**

protocol`://`*fqdn*`:`*port*`|`*instance-number*

The instance number should be the next available number that is not in use.

5 **Click Add.**

6 **Click Save.**

Configuring and Reconfiguring an Instance of Access Manager

You can configure an instance of Access Manager that was installed with the Configure Later option or reconfigure the first instance that was installed using Configure Now option in the Java Enterprise System installer by running the `amconfig` script.

For example, you might want to reconfigure an instance to change the Access Manager owner and group.

▼ To Configure or Reconfigure an Instance of Access Manager

1 **Log in as an administrator, depending on the web container for the instance. For example, if Web Server 6.1 is the web container, log in either as superuser (root) or as the user account for Web Server Administration Server.**

2 **Copy the silent configuration input file you used to deploy the instance to a writable directory and make that directory your current directory. For example, to reconfigure an instance for Web Server 6.1, the following steps use an input file named `amnewinstanceforWS61` in the `/reconfig` directory.**

3 **In the `amnewinstanceforWS61` file, set the DEPLOY_LEVEL variable to one of the values described for a "Deployment Mode Variable" on page 24 operation. For example, set DEPLOY_LEVEL=21 to reconfigure a full installation.**

4 **In the `amnewinstanceforWS61` file, set the NEW_INSTANCE variable to false:**

```
NEW_INSTANCE=false
```

5 **Set other variables in the `amnewinstanceforWS61` file to reconfigure the instance. For example, to change the owner and group for the instance, set the NEW_OWNER and NEW_GROUP variables to their new values.**

For a description of other variables, refer to the tables in the following sections:

- "Access Manager Configuration Variables" on page 25
  - "Web Container Configuration Variables" on page 28
  - "Directory Server Configuration Variables" on page 33

6 **Run the `amconfig` script, specifying your edited input file. For example, on Solaris systems:**

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./reconfig/amnewinstanceforWS61
```

The `-s` option runs the script in silent mode. The `amconfig` script calls other configuration scripts as needed, using variables in the `amnewinstanceforWS61` file to reconfigure the instance.

Uninstalling Access Manager

You can uninstall an instance of Access Manager that was installed by running the `amconfig` script. You can also temporarily unconfigure an instance of Access Manager, and unless you remove the web container instance, it is still available for you to re-deploy another Access Manager instance later.

▼ To Uninstall an Instance of Access Manager

1 **Log in as an administrator, depending on the web container for the instance. For example, if Web Server 6.1 is the web container, log in either as superuser (root) or as the user account for Web Server Administration Server.**

2 **Copy the silent configuration input file you used to deploy the instance to a writable directory and make that directory your current directory. For example, to unconfigure an instance for Web Server 6.1, the following steps use an input file named `amnewinstanceforWS61` in the `/unconfigure` directory.**

3 **In the `amnewinstanceforWS61` file, set the DEPLOY_LEVEL variable to one of the values described for an "Deployment Mode Variable" on page 24 operation. For example, set DEPLOY_LEVEL=11 to uninstall (or unconfigure) a full installation.**

4 **Run the `amconfig` script, specifying your edited input file. For example, on Solaris systems:**

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./unconfigure/aminstanceforWS61
```

The `-s` option runs the script in silent mode. The `amconfig` script reads the `amnewinstanceforWS61` file and then uninstalls the instance.

The web container instance is still available if you want to use it to re-deploy another Access Manager instance later.

Uninstalling All Access Manager Instances

This scenario completely removes all Access Manager 7 2005Q4 instances and packages from a system.

▼ To Completely Remove Access Manager 7 2005Q4 From a System

1 **Log in as or become superuser (root).**

2 **In the input file you used to deploy the instance, set the DEPLOY_LEVEL variable to one of the values described for an "Deployment Mode Variable" on page 24 operation. For example, set DEPLOY_LEVEL=11 to uninstall (or unconfigure) a full installation.**

3. **Run the `amconfig` script using the file you edited in "Uninstalling All Access Manager Instances" on page 38. For example on Solaris systems:**

   ```
   # cd opt/SUNWam/bin/
   # ./amconfig -s ./newinstances/amnewws6instance
   ```

   The `amconfig` script runs in silent mode to uninstall the instance.

   Repeat these steps for any other Access Manager instances you want to uninstall, except for the first instance, which is the instance you installed using the Java Enterprise System installer.

4. **To uninstall the first instance and remove all Access Manager packages from the system, run the Java Enterprise System uninstaller. For information about the uninstaller, refer to the** *Sun Java Enterprise System 2005Q4 Installation Guide for UNIX*.

Example Configuration Script Input File

The following section includes an example of an Access Manager configuration script input file for deployment with WebLogic 8.1.

```
DEPLOY_LEVEL=1
BASEDIR=/opt
SERVER_HOST=ide-56.example.company.com
SERVER_PORT=7001
SERVER_PROTOCOL=http
CONSOLE_HOST=$SERVER_HOST
CONSOLE_PORT=$SERVER_PORT
CONSOLE_PROTOCOL=$SERVER_PROTOCOL
CONSOLE_REMOTE=false
DS_HOST=ide-56.example.company.com
DS_PORT=389
DS_DIRMGRDN=”cn=Directory Manager”
DS_DIRMGRPASSWD=11111111
ROOT_SUFFIX=”dc=company,dc=com”
ADMINPASSWD=11111111
AMLDAPUSERPASSWD=00000000
CONSOLE_DEPLOY_URI=/amconsole
SERVER_DEPLOY_URI=/amserver
PASSWORD_DEPLOY_URI=/ampassword
COMMON_DEPLOY_URI=/amcommon
COOKIE_DOMAIN=.iplanet.com
JAVA_HOME=/usr/jdk/entsys-j2se
AM_ENC_PWD=””
PLATFORM_LOCALE=en_US
NEW_OWNER=root
NEW_GROUP=other
XML_ENCODING=ISO-8859-1
```

```
NEW_INSTANCE=false
WEB_CONTAINER=WL8
WL8_HOME=/export/bea8
WL8_PROJECT_DIR=user_projects
WL8_DOMAIN=mydomain
WL8_CONFIG_LOCATION=$WL8_HOME/$WL8_PROJECT_DIR/domains
WL8_SERVER=myserver
WL8_INSTANCE=/export/bea8/weblogic81
WL8_PROTOCOL=http
WL8_HOST=ide-56.example.company.com
WL8_PORT=7001
WL8_SSLPORT=7002
WL8_ADMIN=”weblogic”
WL8_PASSWORD=”11111111”
WL8_JDK_HOME=$WL8_HOME/jdk142_04
DIRECTORY_MODE=1
USER_NAMING_ATTR=uid
ORG_NAMING_ATTR=o
ORG_OBJECT_CLASS=examplemanagedorganization
USER_OBJECT_CLASS=inetorgperson
DEFAULT_ORGANIZATION=
Sample Configuration Script Input File for WebLogic 8.1.x
```

CHAPTER 2

Installing and Configuring Third-Party Web Containers

This chapter describes the procedures for installing and configuring third-party web containers deployed with Sun Java^{TM} System Access Manager. For this release, Access Manager supports BEA WebLogic 8.1 (and its current patches) and IBM WebSphere 5.1 (and its current patches).

WebLogic and WebSphere are not part of the Java Enterprise System, so you must install and configure them independently of the Java ES Install program. In general the procedures are:

- Install, configure, and start the web container instance.
- Install the Directory Server from the Java ES installer.
- Install Access Manager from the Java ES Installer in Configure Later Mode, which will leave Access Manager in an unconfigured state.
- Run the Access Manager configuration scripts to deploy Access Manager in the web container.
- Restart the web container.

Installing and Configuring BEA WebLogic 8.1

Before you install WebLogic, make sure that your host domain is registered in DNS. Also, verify that you are installing the correct version of the WebLogic software. For more information, go to the BEA product site at http://commerce.bea.com/index.jsp.

▼ To Install and Configure WebLogic 8.1

1 **Unpack the downloaded software image, either in `.zip` or `.gz` format. Make sure that the zip/gzip utility is for the correct platform or you may receive a checksum error during the unpackaging.**

2 **Run the installation program from a shell window of your target system.**

Follow the procedures provided by the WebLogic installation utility (detailed installation instructions can be found at http://e-docs.bea.com/wls/docs81/).

During the installation process, make sure that you record the following information, to be used later in the Access Manager configuration:

- FQDN (used in the `WL8_HOST` parameter)
  - installation location
  - port number

3 **Once installation is complete, run the WebLogic configuration tool to configure the domain and server instance from the following location:**

WebLogic-base/WebLogic-instance/`common/bin/quickstart.sh`

By default, WebLogic defines the server instance as `myserver` and the domain as `mydomain`. It is unlikely that you will choose to use these defaults. If you create a new domain and instance, make sure that you record the information for Access Manager configuration and deployment. See the WebLogic 8.1 documentation for instructions.

4 **If you are installing on an administration instance, start WebLogic by using the `startWebLogic.sh` utility from the following location:**

WebLogic-base/WebLogic-Userhome/`domains/` *WebLogic-domain*/`startWebLogic.sh`

If you are installing on a managed instance, start WebLogic by using the following command:

WebLogic-base/WebLogic-Userhome/`domains/` WebLogic-domain/`startManagedWebLogic` WebLogic-managed-instancename admin-url

Installing and Configuring IBM WebSphere 5.1

Before you install WebSphere, make sure that your host domain is registered in DNS and verify that you are installing the correct version of the WebSphere software for your platform. For more information, go to the IBM product support website at http://www-306.ibm.com/software/websphere/support/.

▼ To Install and Configure WebSphere 5.1

1 **Unpack the downloaded software image, either in `.zip` or `.gz` format. Make sure that the zip/gzip utility is for the correct platform or you may receive a checksum error during the unpackaging.**

2 **Run the installation program from a shell window of your target system. If you are planning on installing a patch, install the 5.1 version first and apply the patch later. Detailed installation instructions can be found at http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp.**

During the installation process, make sure that you record the following information to be used later in the Access Manager configuration:

- hostname
  - domain name
  - cell name
  - node name
  - port number
  - installation directory
  - WebSphere instance name
  - administration port

    By default, WebSphere defines the server instance as `server1`, however it is unlikely that you will the default. If you create a new instance, make sure that you record the information for Access Manager configuration and deployment. See the WebSphere 5.1 documentation for instructions.

3 **Verify that the installation was successful.**

a. **Make sure the `server.xml` file exists in the following directory:**

```
/opt/WebSphere/AppServer/config/cells/cell-name/noes/

node-name/servers/server1
```

b. **Use the `startServer.sh` command to start the server, for example:**

`/opt/WebSphere/AppServer/bin/startServer.sh` server1

c. **In a web browser, enter the corresponding URL of the following format to view the sample web application:**

`http://` *fqdn:portnumber/snoop*

4 **Once you have verified a successful installation, stop the server using the `stopServer.sh` utility. For example:**

`opt/WebSphere/AppServer/bin/stopServer.sh` server1

5 **If you are installing WebSphere 5.1 patch, use the `updateWizard.sh` command line utility to install the patch over the original 5.1 instance.**

6 **Restart WebSphere and verify that the installation was successful.**

Using Java ES to Install Directory Server and Access Manager

Access Manager installation involves two separate invocations of the Java Enterprise System (Java ES) Installer.

▼ To Install Directory Server

1 **Run the first Java ES invocation to install Directory Server (either local or remote) with the Configure Now option. The Configure Now option allows you to configure the first instance during the installation by the choices (or default values) that you select.**

2 **Run the second Java ES invocation to install Access Manager with the Configure Later option. This option Installs the Access Manager 2005Q4 components. After installation, you must configure Access Manager.**

WebLogic and WebSphere are installed independently of Java ES, so the Installer does not contain the necessary configuration data to automatically deploy the containers. Because of this, you must select the Configure Later option when installing Access Manager. This option leaves your Access Manager deployment in the following state:

- The active Directory Server (either Local or Remote) does not have Access Manager DIT data loaded.
  - Access Manager configuration files are not automatically loaded.
  - Access Manager web application `.war` files are not generated.
  - Access Manager deployment and post-installation configuration processes are not automatically started and run.

    For detailed installation instructions, refer to the Sun Java Enterprise System Installation Guide located at http://docs.sun.com/doc/819-0056.

Configuring Access Manager

After you have completed Access Manager installation on the target system's local drive, you need to manually configure Access Manager with either WebLogic 8.1 or WebSphere 5.1. This is a three-step process:

▼ To Configure Access Manager

1 **Edit the configuration script input file**

2 **Run the configuration script**

3 **Restart the web container**

Creating the Configuration Script Input File

The Access Manager configuration script input file contains all of the deployment level, Access Manager, web container, and Directory Server variable definitions. Access Manager contains a sample configuration script input file template (`amsamplesilent`) which is available in the *AccessManager-base* `/SUNWam/bin` directory on Solaris systems or the *AccessManager-base* `/identity/bin` directory on Linux systems.

You can use the `amsamplesilent` template to construct your configuration script input file. Instructions for editing the file, as well as the variable definitions, are described in "Access Manager Sample Configuration Script Input File" on page 23.

Before you edit the file, make sure that you have the following information available from your web container installation:

BEA WebLogic and IBM WebSphere

- installation location
- instance name and location
- hostname
- FQDN
- port number to which it is listening
- administration ID
- protocol used

BEA WebLogic only

- administration password
- shared library location
- domain name and location
- project directory name
- JDK location

IBM WebSphere only

- cell name
- node name
- JDK location

Running the Configuration Script

When you have saved the configuration script input file, you run the `amconfig` script to complete the configuration process. For example:

```
AccessManager-base/SUMWam/bin/amconfig -s silentfile
```

silentfile should be the absolute path to the configuration input file.

Running this script performs the following functions:

1. Loads the Access Manager schema to the active Directory Server instance.
2. Loads the Access Manager service data to the Directory Server instance.
3. Generates the Access Manager configuration files used by the active Access Manager instance.
4. Deploys the Access Manager web application data to the web container.
5. Customizes the web container configuration to match the Access Manager requirements.

Restarting the Web Container

After you have completed the configuration process, you must restart the web container. Refer to your product's documentation for instructions.

For BEA WebLogic 8.1, see http://e-docs.bea.com/wls/docs81.

For IBM WebSphere 5.1, see http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp.

◆ ◆ ◆ CHAPTER 3

Configuring Access Manager in SSL Mode

Using Secure Socket Layer (SSL) with simple authentication guarantees confidentiality and data integrity. To enable Access Manager in SSL, mode you would typically:

- Configure Access Manager with a secure web container
- Configure Access Manager to a secure Directory Server

Configuring Access Manager With a Secure Sun Java Enterprise System Web Server

To configure Access Manager in SSL mode with Web Server, see the following steps:

▼ To Configure a Secure Web Server

1 **In the Access Manager console, go to the Service Configuration module and select the Platform service. In the Server List attribute, remove the `http://` protocol, and add the `https://` protocol. Click Save.**

Note – Be sure to click Save. If you don't, you will still be able to proceed with the following steps, but all configuration changes you have made will be lost and you will not be able to log in as administrator to fix it.

Steps 2 through 24 describe the Web Server.

2 **Log on to the Web Server console. The default port is 8888.**

3 **Select the Web Server instance on which Access Manager is running, and click Manage.**

This displays a pop-up window explaining that the configuration has changed. Click OK.

4 **Click on the Apply button located top right corner of the screen.**

5 **Click Apply Changes.**

The Web Server should automatically restart. Click OK to continue.

6 **Stop the selected Web Server instance.**

7 **Click the Security Tab.**

8 **Click on Create Database.**

9 **Enter the new database password and click OK.**

Ensure that you write down the database password for later use.

10 **Once the Certificate Database has been created, click on Request a Certificate.**

11 **Enter the data in the fields provided in the screen.**

The Key Pair Field Password field is the same as you entered in Step 9. In the location field, you will need to spell out the location completely. Abbreviations, such as CA, will not work. All of the fields must be defined. In the Common Name field, provide the hostname of your Web Server.

12 **Once the form is submitted, you will see a message such as:**

```
--BEGIN CERTIFICATE REQUEST---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE REQUEST--
```

13 **Copy this text and submit it for the certificate request.**

Ensure that you get the Root CA certificate.

14 **You will receive a certificate response containing the certificate, such as:**

```
--BEGIN CERTIFICATE---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE---
```

15 **Copy this text into your clipboard, or save the text into a file.**

16 **Go to the Web Server console and click on Install Certificate.**

17 **Click on Certificate for this Server.**

18 **Enter the Certificate Database password in the Key Pair File Password field.**

19 **Paste the certificate into the provided text field, or check the radio button and enter the filename in the text box. Click Submit.**

The browser will display the certificate, and provide a button to add the certificate.

20 **Click Install Certificate.**

21 **Click Certificate for Trusted Certificate Authority.**

22 **Install the Root CA Certificate in the same manner described in steps 16 through 21.**

23 **Once you have completed installing both certificates, click on the Preferences tab in the Web Server console.**

24 **Select Add Listen Socket if you wish to have SSL enabled on a different port. Then, select Edit Listen Socket.**

25 **Change the security status from Disabled to Enabled, and click OK to submit the changes, click Apply and Apply Changes.**

Steps 26–29 apply to Access Manager.

26 **Open the** `AMConfig.properties` **file. By default, the location of this file is** `etc/opt/SUNWam/config.`

27 **Replace all of the protocol occurrences of** `http://` **to** `https://`, **except for the Web Server Instance Directory. This is also specified in** `AMConfig.properties`**, but must remain the same.**

28 **Save the** `AMConfig.properties` **file.**

29 **In the Web Server console, click the ON/OFF button for the Access Manager hosting web server instance.**

The Web Server displays a text box in the Start/Stop page.

30 **Enter the Certificate Database password in the text field and select Start.**

Configuring Access Manager with a Secure Sun Java System Application Server

Setting up Access Manager to run on an SSL-enabled Application server is a two-step process. First, secure the Application Server instance to the installed Access Manager, then configure Access Manager itself.

Setting Up Application Server 6.2 With SSL

This section describes the steps to set up Application Server 6.2 in SSL mode.

▼ To Secure the Application Server Instance

1. **Log into the Sun Java System Application Server console as an administrator by entering the following address in your browser:**

   `http://fullservername:port`

   The default port is 4848.

2. **Enter the username and password you entered during installation.**

3. **Select the Application Server instance on which you installed (or will install) Access Manager. The right frame displays that the configuration has changed.**

4. **Click Apply Changes.**

5. **Click Restart. The Application Server should automatically restart.**

6. **In the left frame, click Security.**

7. **Click the Manage Database tab.**

8. **Click Create Database, if it is not selected.**

9. **Enter the new database password and confirm, then click the OK button. Make sure that you write down the database password for later use.**

10. **Once the Certificate Database has been created, click the Certificate Management tab.**

11. **Click the Request link, if it is not selected.**

12 Enter the following Request data for the certificate

a. Select it if this is a new certificate or a certificate renewal. Many certificates expire after a specific period of time and some certificate authorities (CA) will automatically send you renewal notification.

b. Specify the way in which you want to submit the request for the certificate.

If the CA expects to receive the request in an E-mail message, check CA E-mail and enter the E-mail address of the CA. For a list of CAs, click List of Available Certificate Authorities.

If you are requesting the certificate from an internal CA that is using the Certificate Server, click CA URL and enter the URL for the Certificate Server. This URL should point to the certificate server's program that handles certificate requests.

c. Enter the password for your key-pair file (this is the password you specified in step 9).

d. Enter the following identification information:

Common Name. The full name of the server including the port number.

Requestor Name. The name of the requestor.

Telephone Number. The telephone number of the requestor

Common Name . The fully qualified name of the Sun Java System Application Server on which the digital certificate will be installed.

E-mail Address. The E-mail address of the administrator.

Organization Name. The name of your organization. The certificate authority may require any host names entered in this attribute belong to a domain registered to this organization.

Organizational Unit Name. The name of your division, department, or other operational unit of your organization.

Locality Name (city). The name of your city or town.

State Name. The name of the state or province in which your organization operates if your organization is in the United States or Canada, respectively. Do not abbreviate.

Country Code. The two-letter ISO code for your country. For example, the code for the United States is `US`.

13 Click the OK button. A message will be displayed, for example:

```
--BEGIN NEW CERTIFICATE REQUEST---
afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdfla
alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl
--END NEW CERTIFICATE REQUEST--
```

14 Copy all of this text to a file and click OK. Make sure that you get the Root CA certificate.

15 **Select a CA and follow the instructions on that authority's web site to get a digital certificate. You can get the certificate from CMS, Verisign or Entrust.net**

16 **After you receive your digital certificate from the certificate authority, you can copy the text into your clipboard, or save the text into a file.**

17 **Go to the Application Server console and click on the Install link.**

18 **Select Certificate For This Server.**

19 **Enter the Certificate Database password in the Key Pair File Password field.**

20 **Paste the certificate into the provided text field, Message text (with headers), or enter the filename in the Message that is in this file text box. Select the appropriate radio button.**

21 **Click OK button. The browser displays the certificate, and provides a button to add the certificate.**

22 **Click Add Server Certificate.**

23 **Install the Root CA Certificate in the same manner described above. However, select Certificate for Trusted Certificate Authority.**

24 **Once you have completed installing both certificates, expand the HTTP Server node in the left frame**

25 **Select HTTP Listeners under HTTP Server.**

26 **Select** `http-listener-1`**. The browser displays the socket information.**

27 **Change the value of the port used by** `http-listener-1` **from the value entered while installing application server, to a more appropriate value such as 443.**

28 **Select SSL/TLS Enabled.**

29 **Select Certificate Nickname.**

30 **Specify the Return server. This should match the common name specified in Step 12.**

31 **Click Save.**

32 **Select the Application Server instance on which you will install the Access Manager software. The right frame shows that the configuration has changed.**

33 Click Apply Changes.

34 Click Restart. The application server should automatically restart.

Configuring Application Server 8.1 With SSL

The basic steps to configure Application Server 8.1 with SSL are as follows. See the Application Server 8.1 documentation for detailed instructions.

1. Create a secure port on the Application server through the Application Server Administration console. For more information, see "Configuring Security" in the Sun Java System Application Server Enterprise Edition 8.1 Administration Guide at the following location:

   `http://docs.sun.com/app/docs/coll/1310.1`
2. Verify that the certificate authority (CA) that trusts the server's certificate is present in the web container's trust database. Then, obtain and install a server certificate for the web container. For more information, see "Working with Certificates and SSL" in the Sun Java System Application Server Enterprise Edition 8.1 Administration Guide at the following location:

   `http://docs.sun.com/app/docs/coll/1310.1`
3. Restart the web container.

Configuring Access Manager in SSL Mode

This section describes the steps to configure Access Manager in SSL mode. Before you set up SSL for Access Manager, make sure that you configured the web container for your deployment.

▼ To Configure Access Manager in SSL Mode

1 In the Access Manager console, go to the Service Configuration module and select the Platform service. In the Server List attribute, add the same URL with the HTTPS protocol and an SSL-enabled port number. Click Save.

Note – If a single instance of Access Manager is listening on two ports (one in HTTP and one in HTTPS) and you try to access Access Manager with a stalled cookie, Access Manager will become unresponsive. This is not a supported configuration.

---

2 Open the `AMConfig.properties` file from the following default location:

`/etc/opt/SUNWam/config.`

3 **Replace all of the protocol occurrences of `http://` to `https://` and change the port number to an SSL-enabled port number.**

4 **Save the `AMConfig.properties` file.**

5 **Restart the Application Server.**

Configuring AMSDK with a Secure BEA WebLogic Server

The BEA WebLogic Server must first be installed and configured as a web container before you configure it with the AMSDK in SSL. For installation instructions, see the BEA WebLogic server documentation. To configure WebLogic as a web container for Access Manager, see Chapter 1, "Access Manager 7 2005Q4 Configuration Scripts."

▼ To Configure a Secure WebLogic Instance

1 **Create a domain using the quick start menu**

2 **Go to the WebLogic installation directory and generate the certificate request.**

3 **Apply for the server certificate using the CSR text file to a CA.**

4 **Save the approved certificate in to a text file. For example,** `approvedcert.txt.`

5 **Load the Root CA in `cacerts` by using the following commands:**

```
cd jdk141_03/jre/lib/security/
```

```
jdk141_03/jre/bin/keytool -keystore cacerts -keyalg RSA -import -trustcacerts
-alias "<alias name>" -storepass changeit -file /opt/bea81/cacert.txt
```

6 **Load the Server certificate by using the following command:**

```
jdk141_03/jre/bin/keytool -import -keystore <keystorename> -keyalg RSA -import
-trustcacerts -file approvedcert.txt -alias "mykey"
```

7 **Login to WebLogic console with your username and password.**

8 **Browse to the following location:**

yourdomain> Servers> myserver> Configure Keystores

9 **Select Custom Identity and then Java Standard Trust**

10 **Enter the keystore location. For example,** `/opt/bea81/keystore.`

11 **Enter Keystore Password and Keystore Pass Phrase. For example:**

Keystore Password: `JKS/Java Standard Trust` (for WL 8.1 it is only JKS)

Key Store Pass Phrase: `changeit`

12 **Review the SSL Private Key Settings Private Key alias and password.**

Note – You must use the full strength SSL licence or SSL startup will fail

13 **In Access Manager, the following parameters in `AmConfig.properties` are automatically configured during installation. If they are not, you can edit them appropriately:**

```
com.sun.identity.jss.donotInstallAtHighestPriority=true [ this is not
 required for AM 6.3 and above]
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.am.util.SecureRandomFactoryImpl
com.iplanet.security.SSLSocketFactoryImpl=netscape.ldap.factory.JSSESocketFactory
com.iplanet.security.encryptor=com.iplanet.services.util.JCEEncryption
```

If your JDK path is the following:

```
com.iplanet.am.jdk.path=/usr/jdk/entsys-j2se
```

then use the keytool utility to import the root CA in the certificate database. For example:

```
/usr/jdk/entsys-j2se/jre/lib/security
/usr/jdk/entsys-j2se/jre/bin/keytool -keystore cacerts
-keyalg RSA -import -trustcacerts -alias "machinename" -storepass changeit -file
/opt/bea81/cacert.txt
```

The keytool utility is located in the following directory:

```
/usr/jdk/entsys-j2se/jre/bin/keytool
```

14 **Remove `-D"java.protocol.handler.pkgs=com.iplanet.services.comm"` from the Access Manager `amadmin` command line utility.**

15 **Configure Access Manager in SSL Mode. For more information, see "Configuring Access Manager in SSL Mode" on page 53.**

Configuring AMSDK with a Secure IBM WebSphere Application Server

The IBM WebSphere Server must first be installed and configured as a web container before you configure it with the AMSDK in SSL. For installation instructions, see the WebSphere server documentation. To configure WebLogic as a web container for Access Manager, see Chapter 1, "Access Manager 7 2005Q4 Configuration Scripts."

▼ To Configure a Secure WebSphere Instance

1. **Start `ikeyman.sh`, located in the Websphere `/bin` directory.**

2. **From the Signer menu, import the certification authority's (CA) certificate.**

3. **From the Personal Certs menu, generate the CSR.**

4. **Retrieve the certificate created in the previous step.**

5. **Select Personal Certificates and import the server certificate.**

6. **From the WebSphere console, change the default SSL settings and select the ciphers.**

7. **Set the default IBM JSSE SSL provider.**

8. **Enter the following command to import the Root CA certificate from the file you just created into application server JVM Keystore:**

   ```
   $ appserver_root-dir/java/bin/ keytool -import -trustcacerts -alias cmscacert
   -keystore ../jre/lib/security/cacerts -file
   /full_path_cacert_filename.txt
   ```

   app-server-root-dir is the root directory for the application server and *full_path_cacert_filename.txt* is the full path to the file containing the certificate.

9. **In Access Manager, update the following parameters in `AmConfig.properties` to use JSSE:**

   ```
   com.sun.identity.jss.donotInstallAtHighestPriority=true
   com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.
   am.util.SecureRandomFactoryImpl
   com.iplanet.security.SSLSocketFactorImpl=netscape.ldap.factory.
   JSSESocketFactory
   com.iplanet.security.encyptor=com.iplanet.services.unil.JCEEncryption
   ```

10. **Configure Access Manager in SSL Mode. For more information, see "Configuring Access Manager in SSL Mode" on page 53.**

Configuring Access Manager to Directory Server in SSL Mode

To provide secure communications over the network, Access Manager includes the LDAPS communications protocol. LDAPS is the standard LDAP protocol, but it runs on top of the Secure Sockets Layer (SSL). In order to enable SSL communication, you must first configure the Directory Server in SSL mode and then connect Access Manager to Directory Server. The basic steps are as follows:

1. Obtain and install a certificate for your Directory Server, and configure the Directory Server to trust the certification authority's (CA) certificate
2. Turn on SSL in your directory.
3. Configure the authentication, policy and platform services to connect to an SSL-enabled Directory Server.
4. Configure Access Manager to securely connect to the Directory Server backend.

Configuring Directory Server in SSL Mode

In order to configure the Directory Server in SSL mode, you must obtain and install a server certificate, configure the Directory Server to trust the CA's certificate and enable SSL. Detailed instructions on how to complete these tasks are included in Chapter 11, "Managing Authentication and Encryption" in the *Directory Server Administration Guide*. This document can be found in the following location:

http://docs.sun.com/coll/DirectoryServer_04q2 (`http://docs.sun.com/coll/DirectoryServer_04q2`)

If your Directory Server is already SSL-enabled, go to the next section for details on connecting Access Manager to Directory Server.

Connecting Access Manager to the SSL-enabled Directory Server

Once the Directory Server has been configured for SSL mode, you need to securely connect Access Manager to the Directory Server backend.

▼ To Connect Access Manager to Directory Server

1 **In the Access Manager Console, go to the LDAP Authentication service in the Service Configuration module.**

   a. **Change the Directory Server port to the SSL port.**

   b. **Select the Enable SSL Access to LDAP Server attribute.**

2 **Go to the Membership Authentication service in the Service Configuration module.**

   a. **Change the Directory Server port to the SSL port.**

   b. **Select the Enable SSL Access to LDAP Server attribute.**

3 **Go to the Policy Configuration service located in Service Configuration.**

a. **Change the Directory Server port to the SSL port.**

b. **Select the Enable LDAP SSL attribute.**

4 **Open the** `serverconfig.xml` **in a text editor. The file is in the following location:**

`/etc/opt/SUNWam/config`

a. **In the** `<Server>` **element, change the following values:**

`port` - enter the port number of the secure port to which Access Manager listens (636 is the default).

`type`- change SIMPLE to SSL.

b. **Save and close** `serverconfig.xml`**.**

5 **Open the** `AMConfig.properties` **file from the following default location:**

/etc/opt/`SUNWam/config.`

Change the following properties:

a. `com.iplanet.am.directory.port` = `636` **(if using the default)**

b. `ssl.enabed = true`

c. **Save** `AMConfig.properties`**.**

6 **Restart the server**

PART II

Access Control

This is part two of the Sun Java System Access Manager™ 7 2005Q4 Administration Guide. The Access Control interface provides a way to create and manage authentication and authorization services to protect and regulate realm-based resources. When an enterprise user requests information, Access Manager verifies the user's identity and authorizes the user to access the specific resource that the user has requested. The part contains the following chapters:

- Chapter 4, “The Access Manager Console”
- Chapter 5, “Managing Realms”
- Chapter 6, “Data Stores”
- Chapter 7, “Managing Authentication”
- Chapter 8, “Managing Policies”
- Chapter 9, “Managing Subjects”

CHAPTER 4

The Access Manager Console

The Access Manager console is a web interface that allows administrators with different levels of access to, among other things, create realms and organizations, create or delete users to and from those realms and establish enforcement policies that protect and limit access to realms' resources. In addition, administrators can view and terminate current user sessions and manage their federation configurations (create, delete and modify authentication domains and providers). Users without administrative privileges, on the other hand, can manage personal information (name, e-mail address, telephone number, and so forth), change their password, subscribe and unsubscribe to groups, and view their roles. The Access Manager Console has two, basic views:

- "Administration View" on page 61
- "User Profile View" on page 64

Administration View

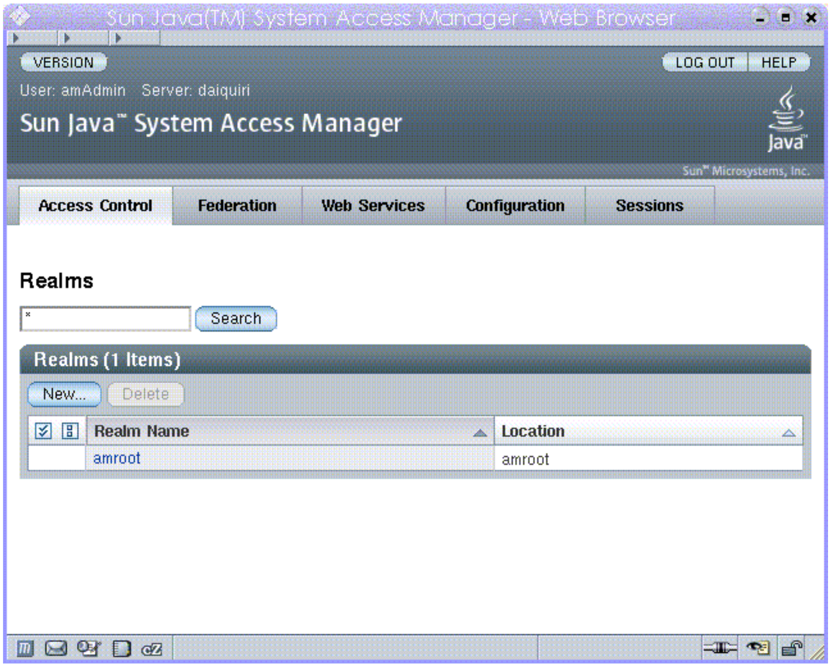
When a user with an administrative role authenticates to Access Manager, the default view is the Administration view. In this view, the administrator can perform most administrative tasks related to Access Manager. Access Manager can be installed in two different modes; Realms mode and Legacy Mode. Each mode has its own console. For more information on Realm and Legacy Modes, see the*Sun Java System Access Manager 7 2005Q4 Technical Overview*.

Realms Mode Console

The Realms mode console enables administrators to manage realm-based access control, default service configuration, Web services and Federation. To access the administrator login screen, use the following address syntax in your browser:

protocol`://`*servername*`/amserver/UI/Login`

`protocol` is either http: or https, depending upon your deployment.



Realm Name	Location
amroot	amroot

FIGURE 4–1 Realms Mode Administration View

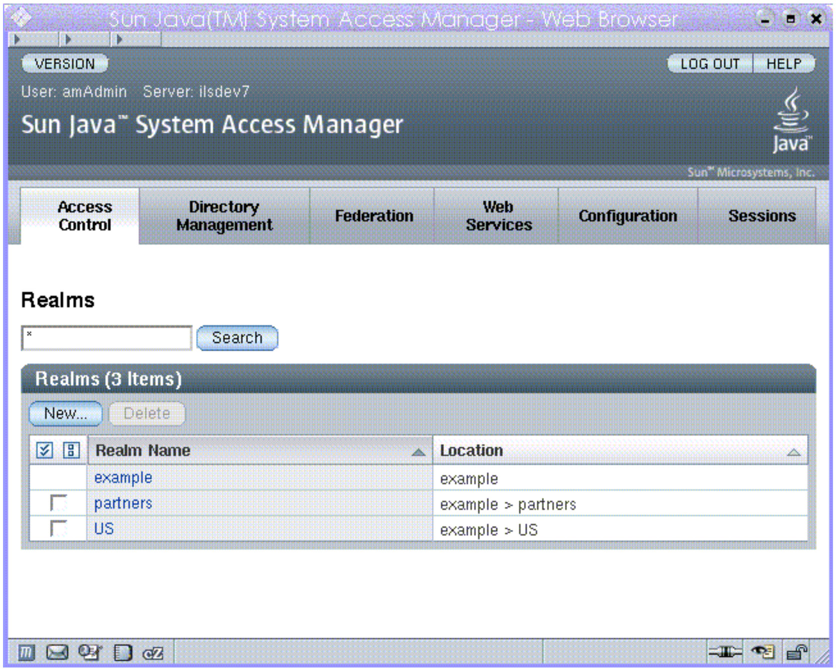
Legacy Mode Console

Legacy Mode console is based on the Access Manager 6.3 architecture. This legacy Access Manager architecture uses the LDAP directory information tree (DIT) that comes with Sun Java System Directory Server. In Legacy Mode, both user information and access control information are stored in LDAP organizations. When you choose Legacy Mode, an LDAP organization is the equivalent of an access control realm. Realm information is integrated within LDAP organizations. In Legacy Mode, the Directory Management tab is available for Access Manager-based identity management.

To access the administrator login screen, use the following address syntax in your browser:

protocol`://`*servername*`/amserver/console`

`protocol` is either http: or https, depending upon your deployment.



Realm Name	Location
example	example
partners	example > partners
US	example > US

FIGURE 4–2 Legacy Mode Administration View

Legacy Mode 6.3 Console

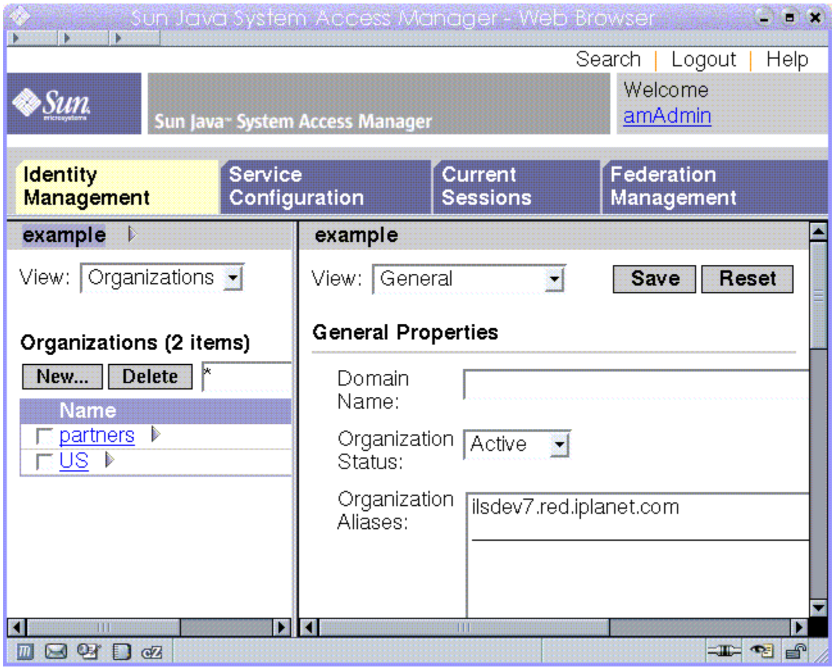
Some features of Access Manager 6.3 are not available in the Access Manager 7.0 console. Because of this, administrators can log into the 6.3 console through a 7.0 Legacy deployment. This console is typically used where Access Manager is built upon Sun Java System Portal Server or other Sun Java System communication products that require the use of Sun Java System Directory Server as the central identity repository. Other features, such Delegated Administration and Class of Service, are accessed only through this console.

Note – Do not interchange between using the 6.3 and 7.0 Legacy mode consoles.

To access the 6.3 console, use the following address syntax in your browser:

protocol`://`*servername*`/amconsole`

`protocol` is either http: or https, depending upon your deployment.



View: Organizations

View: General

Domain Name:

Organization Status: Active

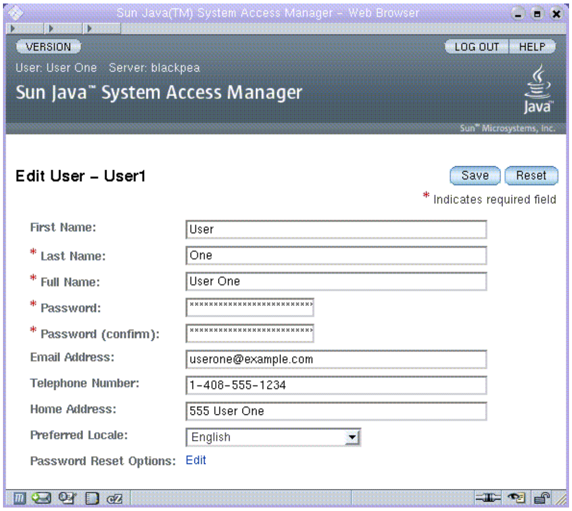
Organization Aliases: ilsdev7.red.iplanet.com

FIGURE 4–3 Legacy 6.3–based Console

User Profile View

When a user who has not been assigned an administrative role authenticates to the Access Manager the default view is the user's own User Profile. The User Profile view can be accessed in either Realm or Legacy Mode. The user must enter the user's own username and password at the Login page in order to access this view.

In this view the user can modify the values of the attributes particular to the user's personal profile. This can include, but is not limited to, name, home address and password. The attributes displayed in the User Profile View can be extended.



User: User One   Server: blackpea

Sun Java™ System Access Manager

Edit User – User1

* Indicates required field

First Name:	User
* Last Name:	One
* Full Name:	User One
* Password:	***************************
* Password (confirm):	***************************
Email Address:	userone@example.com
Telephone Number:	1-408-555-1234
Home Address:	555 User One
Preferred Locale:	English
Password Reset Options:	Edit

FIGURE 4–4 User Profile View

CHAPTER 5

Managing Realms

An access control realm is a group of authentication properties and authorization policies you can associate with a user or group of users. Realm data is stored in a proprietary information tree that Access Manager creates within a data store you specify. The Access Manager framework aggregates policies and properties contained in each realm within the Access Manager information tree. By default, Access Manager 7 automatically inserts the Access Manager information tree as a special branch in Sun Java Enterprise System Directory Server, apart from the user data. You can use access control realms while using any LDAPv3 database.

For more information on realms, see the *Sun Java System Access Manager 7 2005Q4 Technical Overview*.

In the Realms tab, you can configure the following properties for access control:

- "Authentication" on page 68
- "Services" on page 69
- "Privileges" on page 70

Creating and Managing Realms

This section describes how to create and manage realms.

▼ To Create a New Realm

1 **Select New from the Realms list under the Access Control tab.**

2 **Define the following general attributes:**

Name Enter a name for the Realm.

Parent Defines the location of the realm that you are creating. Select the parent realm under which the new realm will exist.

3 **Define the following realm attributes:**

Realm Status — Choose a status of active or inactive. The default is active. This can be changed at any time during the life of the realm by selecting the Properties icon. Choosing inactive disables user access when logging in.

Realm/DNS Aliases — Allows you to add alias names for the DNS name for the realm. This attribute only accepts “real” domain aliases (random strings are not allowed).

4 **Click OK to save or Cancel to return to the previous page.**

General Properties

The General Properties page displays the basic attributes for a realm. To modify these properties, click the realm from the Realm Names list under the Access Control tab. Then, edit the following properties:

Realm Status — Choose a status of active or inactive. The default is active. This can be changed at any time during the life of the realm by selecting the Properties icon. Choosing inactive disables user access when logging in.

Realm/DNS Aliases — Allows you to add alias names for the DNS name for the realm. This attribute only accepts “real” domain aliases (random strings are not allowed).

Once you edit the properties, click Save.

Authentication

The general authentication service must be registered as a service to a realm before any user can log in using the other authentication modules. The core authentication service allows the Access Manager 7 administrator to define default values for a realm's authentication parameters. These values can then be used if no overriding value is defined in the specified authentication module. The default values for the Core Authentication Service are defined in the `amAuth.xml` file and stored in Directory Server after installation.

For more information, see Chapter 7, “Managing Authentication”

Services

In Access Manager, a service is a group of attributes that are managed together by the Access Manager console. The attributes can be just bits of related information such as an employee's name, job title, and email address. But attributes are typically used as configuration parameters for a software module such as a mail application or payroll service.

Through the Services tab, you can add and configure a number of Access Manager default services to a realm. You can add the following services:

- Administration
- Discovery Service
- Globalization Settings
- Password Reset
- Session
- User

Note – Access Manager enforces that required attributes in service .xml files have some default values. If you have services with required attributes with no values, you need to add default values and reload the service.

▼ To Add a Service to a Realm

1. **Click the name of the realm for which you wish to add a new service.**

2. **Select the Services tab.**

3. **Click Add in the Services list.**

4. **Select the service you wish to add for the realm.**

5. **Click Next.**

6. **Configure the service by defining the realm attributes. See Configuration in the online help for a description of the service attributes.**

7. **Click Finish.**

8. **To edit the properties of a service, click the name in the Service list.**

Privileges

Privileges define the access permissions to roles or groups that exist within a realm. The roles or groups are used as policy subject definitions for the Access Manager Identity Subject type. To assign or modify privileges, click the name of the role or group you wish to edit. The privileges you can assign are:

- Read and write access only for policy properties
- Read and write access to all realm and policy properties
- Read only access to all properties and services

CHAPTER 6

Data Stores

A data store is a database where you can store user attributes and user configuration data.

Access Manager provides an identity repository plug-in that connects to an identity repository framework. This new model enables you to view and retrieve Access Manager user information without having to make changes in your existing user database. The Access Manager framework integrates data from the identity repository plug-in with data from other Access Manager plug-ins to form a virtual identity for each user. Access Manager can then use the universal identity in authentication and authorization processes among more than one identity repository. The virtual user identity is destroyed when the user's session ends.

LDAPv3 Data Store

You can create a new, data store instance for any generic LDAPv3 repository when Access Manager is installed in both Realms and Legacy mode. You should choose the LDAPv3 repository type under the following conditions:

- When roles, class of service (CoS), and compatibility with previous versions of Access Manager are not required.
- When you want to use an existing directory.
- When you want to use a directory server other than Sun Java System Directory Server for the identity repository.
- When you do not want Access Manager to write to identity repositories.
- When you want to use a flat Directory Information Tree (DIT).

▼ To Create a New LDAPv3 Data Store

The following section describes the steps to connect a generic LDAPv3 data store.

1. **Select the realm to which you wish to add a new data store.**

2. **Click the Data Store tab.**

3. **Click New from the Data Stores list.**

4. **Enter a name for the data store.**

5. **Define the attributes for the LDAPv3 repository plug-in.**

6. **Click Finish.**

LDAPv3 Repository Plug-in Attributes

The following attributes are used to configure a LDAPv3 repository plug-in:

- "Primary LDAP Server" on page 73
- "LDAP Bind DN" on page 73
- "LDAP Bind Password" on page 73
- "LDAP Bind Password (confirm)" on page 73
- "LDAP Organization DN" on page 73
- "Enable LDAP SSL" on page 74
- "LDAP Connection Pool Minimum Size" on page 74
- "LDAP Connection Pool Maximum Size" on page 74
- "Maximum Results Returned from Search" on page 74
- "Search Timeout" on page 74
- "LDAP Follows Referral" on page 74
- "LDAPv3 Repository Plugin Class Name" on page 74
- "Attribute Name Mapping" on page 74
- "LDAPv3 Plugin Supported Types and Operations" on page 74
- "LDAP Users Search Attribute" on page 75
- "LDAP Users Search Filter" on page 75
- "LDAP User Object Class" on page 75
- "LDAP User Attributes" on page 75
- "LDAP Groups Search Attribute" on page 75
- "LDAP Groups Search Filter" on page 75
- "LDAP Groups Container Naming Attribute" on page 75
- "LDAP Groups Container Value" on page 76
- "LDAP Groups Object Class" on page 76
- "LDAP Groups Attributes" on page 76

- "Attribute Name for Group Membership" on page 76
- "Attribute Name of Group Member" on page 76
- "Attribute Name of Group Member URL" on page 76
- "LDAP People Container Naming Attribute" on page 76
- "LDAP People Container Value" on page 76
- "LDAP Agents Search Attribute" on page 77
- "LDAP Agents Container Naming Attribute" on page 77
- "LDAP Agents Container Value" on page 77
- "LDAP Agents Search Filter" on page 77
- "LDAP Agents Object Class" on page 77
- "LDAP Agents Attributes" on page 77
- "Persistent Search Base DN" on page 77
- "Persistent Search Maximum Idle Time Before Restart" on page 77
- "Maximum Number of Retries After Error Codes" on page 78
- "The Delay Time Between Retries" on page 78
- "LDAPException Error Codes to Retry On" on page 78

Primary LDAP Server

Enter the name of the LDAP server to which you will be connection. The format should be `hostname.domainname:portnumber`.

If more than one `host:portnumber` entries are entered, an attempt is made to connect to the first host in the list. The next entry in the list is tried only if the attempt to connect to the current host fails.

LDAP Bind DN

Specifies the DN name that Access Manager will use to authenticate to the LDAP server to which you are currently connected. The user with the DN name used to bind should have the correct add/modification/delete privileges that you configured in the LDAPv3 Supported Types and Operations attribute.

LDAP Bind Password

Specifies the DN password that Access Manager will use to authenticate to the LDAP server to which you are currently connected

LDAP Bind Password (confirm)

Confirm the password.

LDAP Organization DN

The DN to which this data store repository will map. This will be the base DN of all operations performed in this data store.

Enable LDAP SSL

When enabled, Access Manager will connect to the primary server using the HTTPS protocol.

LDAP Connection Pool Minimum Size

Specifies the initial number of connections in the connection pool. The use of connection pool avoids having to create a new connection each time.

LDAP Connection Pool Maximum Size

Specifies the maximum number of connections to allowed.

Maximum Results Returned from Search

Specifies the maximum number of entries returned from a search operation. If this limit is reached, Directory Server returns any entries that match the search request.

Search Timeout

Specifies the maximum number of seconds allocated for a search request. If this limit is reached, Directory Server returns any search entries that match the search request.

LDAP Follows Referral

If enabled, this option specifies that referrals to other LDAP servers are followed automatically.

LDAPv3 Repository Plugin Class Name

Specifies the location of the class file which implements the LDAPv3 repository.

Attribute Name Mapping

Enables common attributes known to the framework to be mapped to the native data store. For example, if the framework uses `inetUserStatus` to determine user status, it is possible that the native data store actually uses `userStatus`. The attribute definitions are case-sensitive.

LDAPv3 Plugin Supported Types and Operations

Specifies the operations that are permitted to or can be performed on this LDAP server. The default operations that are the only operations that are supported by this LDAPv3 repository plug-in. The following are operations supported by LDAPv3 Repository Plugin:

- group — read, create, edit, delete
- realm — read, create, edit, delete, service
- user — read, create, edit, delete, service
- agent — read, create, edit, delete

You can remove permissions

from the above based on your LDAP server settings and the tasks, but you can not add more permissions.

LDAP Users Search Attribute

This field defines the attribute type for which to conduct a search on a user. For example, if the user's dn is `uid=k user5,ou=people,dc=iplanet,dc=com`, then the naming attribute is uid. `(uid=*)` will be appended to the search filter for user.

LDAP Users Search Filter

Specifies the search filter to be used to find user entries. for example, if LDAP Users Search Attribute is uid and LDAP Users Search Filter is `(objectClass=inetorgperson)`, then the actual user search filter will be: `(&(uid=*)(objectClass=inetorgperson))`.

LDAP User Object Class

Specifies the object classes for a user. When a user is created, this list of user object classes will be added to the user's attributes list.

LDAP User Attributes

Defines the list of attributes associated with a user. Any attempt to read/write user attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined in Directory Server before you define the object classes and attribute schema here.

LDAP Groups Search Attribute

This field defines the attribute type for which to conduct a search on a group. For example, if the group dn is `cn=group1,ou=groups,dc=iplanet,dc=com`, the naming attribute for group is cn and `(cn=*)` will be appended to the group search filter.

LDAP Groups Search Filter

Specifies the search filter to be used to find group entries. for example, if "LDAP Groups Search Attribute" is `cn` and "LDAP Groups Search Filter" is `(objectclass=groupOfUniqueNames)`, the actual group search filter will be `(&(cn=*)(objectclass=groupOfUniqueNames))`.

LDAP Groups Container Naming Attribute

Specifies the naming attribute for a group container, if groups resides in a container. Otherwise, this attribute is left empty. For example, if a group DN of `cn=group1,ou=groups,dc=iplanet,dc=com`resides in `ou=groups`, then the group container naming attribute is `ou`.

LDAP Groups Container Value

Specifies the value for the group container. For example, a group DN of `cn=group1,ou=groups,dc=iplanet,dc=com` resides in a container name `ou=groups`, then the group container value would be `groups`.

LDAP Groups Object Class

Specifies the object classes for groups. When a group is created, this list of group object classes will be added to the group's attributes list.

LDAP Groups Attributes

Defines the list of attributes associated with a group. Any attempt to read/write group attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined in Directory Server before you define the object classes and attribute schema here.

Attribute Name for Group Membership

Specifies the name of the attribute whose values are the names of all the groups to which DN belongs. The default is `memberOf`.

Attribute Name of Group Member

Specifies the attribute name whose values is a DN belonging to this group. The default is `uniqueMember`.

Attribute Name of Group Member URL

Specifies the name of the attribute whose value is an LDAP URL which resolves to members belonging to this group. The default is `memberUrl`.

LDAP People Container Naming Attribute

Specifies the naming attribute of the people container if a user resides in a people container. This field is left blank if the user does not reside in a people container. For example, given a user dn `uid=kuser5,ou=people,dc=iplanet,dc=com,` if `ou=people` is the name of the people container, then the naming attribute is`ou`.

LDAP People Container Value

Specifies the value of the people container. The default is `people`. For example, given a user dn `uid=kuser5,ou=people,dc=iplanet,dc=com`, if `ou=people` is the name of the people container, then the naming attribute is `ou` and `people` is the "LDAP People Container Value."

LDAP Agents Search Attribute

This field defines the attribute type for which to conduct a search on an agent. The default is uid. For example, if the agent's dn is uid=kagent1,ou=agents,dc=iplanet,dc=com, then the agent's naming attribute is uid. (uid=*) will be appended to the search filter for the agent.

LDAP Agents Container Naming Attribute

The naming attribute of the agent container if the agent resides in a agent container. This field is left blank if the agent does not reside in agent container. For example, given a user dn uid=kagent1,ou=agents,dc=iplanet,dc=com, the agent naming attribute is ou.

LDAP Agents Container Value

Specifies the value of the agent container. It is left blank if the agent does not reside in agent container. In the previous example, the agents container value would be agents.

LDAP Agents Search Filter

Defines the filter used to search for an agent. The LDAP Agent Search attribute is prepended to this field to form the actual agent search filter.

For example, if the LDAP Agents Search Attribute is uid and LDAP Users Search Filter is (objectClass=sunIdentityServerDevice), then the actual user search filter will be: (&(uid=*)(objectClass=sunIdentityServ erDevice))

LDAP Agents Object Class

Defines the object classes for agents. When an agent is created, the list of user object classes will be added to the agent's attributes list

LDAP Agents Attributes

Defines the list of attributes associated with an agent. Any attempt to read/write agent attributes that are not on this list is not allowed. The attributes are case-sensitive. The object classes and attribute schema must be defined in Directory Server before you define the object classes and attribute schema here.

Persistent Search Base DN

Defines the base DN to use for persistent search. Some LDAPv3 servers only support persistent search at the root suffix level.

Persistent Search Maximum Idle Time Before Restart

Defines the maximum idle time before restarting the persistence search. The value must be greater than 1. Values less than or equal to 1 will restart the search irrespective of the idle time of the connection.

If Access Manager is deployed with a load balancer, some load balancers will time out if it has been idle for a specified amount of time. In this case, you should set the Persistent Search Maximum Idle Time Before Restart to a value less than the specified time for the load balancer.

Maximum Number of Retries After Error Codes

Defines the maximum number of retries for the persistent search operation if it encounters the error codes specified in LDAPException Error Codes to Retry On.

The Delay Time Between Retries

Specifies the time to wait before each retry. This only applies to persistent search connection.

LDAPException Error Codes to Retry On

Specifies the error codes to initiate a retry for the persistent search operation. This attribute is only applicable for the persistent search, and not for all LDAP operations.

AMSDK Repository Plug-in

The AMSDK identity repositories is automatically intermingled with the Access Manager information tree when Access Manager is installed in Legacy mode. In Realms mode, you can choose to install the AMSDK repository, but the identity repositories are not intermingled with the Access Manager information tree. You should choose the AMSDK repository type under the following conditions:

- To exploit Sun Java System Directory Server-specific features, such as roles and CoS.
- To obtain compatibility with previous versions of Access Manager.

▼ To Create a New AMSDK Repository Plugin

1. **Select the realm in which you wish to configure the Access Manager repository plug-in.**

2. **Click the Data Store tab.**

3. **Click New from the Data Stores list.**

4. **Enter a name for the repository plug-in.**

5. **Select Access Manager Repository Plugin.**

6. **Click Next.**

7 **Define the following fields:**

Access Manager Plugin Class Name	Specifies the location of the class file which implements the Access Manager repository plug-in.
Access Manager Organization	The DN that points an organization in the Directory Server to be managed by Access Manager. This will be the base DN of all operations performed in this data store.

8 **Click Finish.**

◆ ◆ ◆ CHAPTER 7

Managing Authentication

The Authentication Service provides a web-based user interface for all of the default authentication types installed in the Access Manager deployment. This interface provides a dynamic and customizable means for gathering authentication credentials by displaying the login requirement screens (based on the invoked authentication module) to a user requesting access. The interface is built using Sun Java System™ Application Framework (sometimes referred to as *JATO*), a Java 2 Enterprise Edition (J2EE) presentation framework used to help developers build functional web applications.

Configuring Authentication

This section describes how to configure authentication for your deployment. The first section outlines the default authentication module types and provides any necessary pre-configuration instructions. You can configure multiple configuration instances of the same authentication module type for realms, users, roles, and so forth. Additionally, you can add authentication chains so that authentication must pass the criteria for multiple instance before authentication is successful. This section includes:

- "Authentication Module Types" on page 81
- "Authentication Module Instances" on page 91
- "Authentication Chaining" on page 92
- "To Create a New Authentication Chain" on page 92

Authentication Module Types

An authentication module is a plug-in that collects user information such as a user ID and password, and then checks the information against entries in a database. If a user provides information that meets the authentication criteria, then the user is granted access to the requested resource. If the user provides information that does not meet authentication criteria, the user is denied access to the requested resource. Access Manager is installed with 15 types of authentication modules:

- "Core" on page 82
- "Active Directory" on page 82
- "Anonymous" on page 83
- "Certificate" on page 83
- "HTTP Basic" on page 83
- "JDBC" on page 84
- "LDAP" on page 84
- "Membership" on page 84
- "MSISDN" on page 84
- "RADIUS" on page 84
- "SafeWord" on page 86
- "SAML" on page 87
- "SecurID" on page 87
- "Windows Desktop SSO" on page 88
- "Windows NT" on page 91
- "UNIX" on page 87

Note – Some of the authentication module types require pre-configuration before they can be used as authentication instances. The configuration steps, if necessary, are listed in the module type descriptions.

Core

Access Manager provides, by default, fifteen different authentication modules, as well as a Core authentication module. The Core authentication module provides overall configuration for the authentication module. Before adding and enabling Active Directory, Anonymous, Certificate-based, HTTP Basic, JDBC, LDAP, any authentication module, the Core authentication must be added and enabled. Both the Core and LDAP Authentication modules are automatically enabled for the default realm.

Clicking the Advanced Properties button displays the Core authentication attributes that can be defined for the realm. The global attributes are not applicable to the realm so they are not displayed.

Active Directory

The Active Directory authentication module performs authentication in a similar manner to the LDAP module, but uses Microsoft's Active Directory™ server (as opposed to Directory Server in LDAP authentication module). Although the LDAP authentication module can be configured for an Active Directory server, this module allows you have both LDAP and Active Directory authentication exist under the same realm.

Note – For this release, the Active Directory authentication module only supports user authentication. Password policy is only supported in the LDAP authentication module.

Anonymous

By default, when this module is enabled, a user can log in to Access Manager as an *anonymous* user. A list of anonymous users can also be defined for this module by configuring the Valid Anonymous User List attribute. Granting anonymous access means that it can be accessed without providing a password. Anonymous access can be limited to specific types of access (for example, access for read or access for search) or to specific subtrees or individual entries within the directory.

Certificate

Certificate-based Authentication involves using a personal digital certificate (PDC) to identify and authenticate a user. A PDC can be configured to require a match against a PDC stored in Directory Server, and verification against a Certificate Revocation List.

There are a number of things that need to be accomplished before adding the Certificate-based Authentication module to a realm. First, the web container that is installed with the Access Manager needs to be secured and configured for Certificate-based Authentication. Before enabling the Certificate-based module, see Chapter 6, "Using Certificates and Keys" in the *Sun ONE Web Server 6.1 Administrator's Guide* (located at `http://docs.sun.com/source/817-1831-10/agcert.html`) for the initial Web Server configuration steps. If using Application Server see the *Sun ONE Application Server Administrator's Guide to Security* (located at `http://docs.sun.com/source/816-7158-10/sgcerts.html`).

Note – Each user that will authenticate using the certificate-based module must request a PDC for the user's browser. Instructions are different depending upon the browser used. See your browser's documentation for more information.

In order to add this module, you must log in to Access Manager as the realm Administrator and have Access Manager and the web container configured for SSL and with client authentication enabled. For more information, see Chapter 3, "Configuring Access Manager in SSL Mode."

HTTP Basic

This module uses basic authentication, which is the HTTP protocol's built-in authentication support. The web server issues a client request for username and password, and sends that information back to the server as part of the authorized request. Access Manager retrieves the username and password and then internally authenticates the user to the LDAP authentication module. In order for HTTP Basic to function correctly, the LDAP authentication module must be added (adding the HTTP Basic module alone will not work). Once the user successfully authenticates, the user will be able to re-authenticate without being prompted for username and password.

JDBC

The Java Database Connectivity (JDBC) Authentication module provides a mechanism to allow Access Manager to authenticate users through any SQL databases that provide JDBC technology-enabled drivers. The connection to the SQL database can be either directly through a JDBC driver, or a JNDI connection pool.

Note – This module has been tested on MySQL4.0 and Oracle 8i.

LDAP

With the LDAP Authentication module, when a user logs in, he or she is required to bind to the LDAP Directory Server with a specific user DN and password. This is the default authenticating module for all realm-based authentication. If the user provides a user ID and password that are in the Directory Server, the user is allowed access to, and is set up with, a valid Access Manager session. Both the Core and LDAP Authentication modules are automatically enabled for the default realm

Membership

Membership authentication is implemented similarly to personalized sites such as `my.site.com`, or `mysun.sun.com`. When this module is enabled, a user creates an account and personalizes it without the aid of an administrator. With this new account, the user can access it as a added user. The user can also access the viewer interface, saved on the user profile database as authorization data and user preferences.

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.

RADIUS

Access Manager can be configured to work with a RADIUS server that is already installed. This is useful if there is a legacy RADIUS server being used for authentication in your enterprise. Enabling the RADIUS authentication module is a two-step process:

1. Configure the RADIUS server.

   For detailed instructions, see the RADIUS server documentation.

2. Register and enable the RADIUS authentication module.

Configuring RADIUS with Sun Java System Application Server

When the RADUIS client forms a socket connection to its server, by default, only the connect permission of the SocketPermissions is allowed in the Application Server's `server.policy` file. In order for RADUIS authentication to work correctly, permissions need to be granted for the following actions:

- accept
- connect
- listen
- resolve

To grant a permission for a socket connection, you must add an entry into Application Server's `server.policy` file. A SocketPermission consists of a host specification and a set of actions specifying ways to connect to that host. The host is specified as the following:

```
host = hostname | IPaddress:portrange:portrange = portnumber
| -portnumberportnumber-portnumber
```

The host is expressed as a DNS name, as a numerical IP address, or as local host (for the local machine). The wildcard "*" may be included once in a DNS name host specification. If it is included, it must be in the left-most position, as in `*.example.com`.

The port (or port range) is optional. A port specification of the form `N-`, where `N` is a port number, signifies all ports numbered `N` and above. A specification of the form `-N` indicates all ports numbered `N` and below.

The `listen` action is only meaningful when used with a localhost. The `resolve` (resolve host/IP name service lookups) action is implied when any of the other actions are present.

For example, when creating SocketPermissions, note that if the following permission is granted to some code, it allows that code to connect to `port 1645` on `machine1.example.com,` and to accept connections on that port:

```
permission java.net.SocketPermission machine1.example.com:1645, "connect,accept";
```

Similarly, if the following permission is granted to some code, it allows that code to accept connections on, connect to, or listen to any port between 1024 and 65535 on the local host:

```
permission java.net.SocketPermission "machine1.example.com:1645", "connect,accept";
permission java.net.SocketPermission "localhost:1024-", "accept,connect,listen";
```

Note – Granting code permission to accept or make connections to remote hosts may cause problems, because malevolent code can then more easily transfer and share confidential data among parties who may not otherwise have access to the data. Make sure to give only appropriate permissions by specifying exact port number instead of allowing a range of port numbers

SafeWord

Access Manager can be configured to handle SafeWord Authentication requests to Secure Computing's SafeWord™ or SafeWord PremierAccess™ authentication servers. Access Manager provides the client portion of SafeWord authentication. The SafeWord server may exist on the system on which Access Manager is installed, or on a separate system.

Configuring SafeWord with Sun Java System Application Server

When the SafeWord client forms a socket connection to its server, by default, only the `connect` permission of the SocketPermissions is allowed in the Application Server's `server.policy` file. In order for SafeWord authentication to work correctly, permissions need to be granted for the following actions:

- accept
- connect
- listen
- resolve

To grant a permission for a socket connection, you must add an entry into Application Server's `server.policy` file. A SocketPermission consists of a host specification and a set of actions specifying ways to connect to that host. The host is specified as the following:

```
host = (hostname | IPaddress)[:portrange] portrange =
portnumber | -portnumberportnumber-[portnumber]
```

The host is expressed as a DNS name, as a numerical IP address, or as localhost (for the local machine). The wildcard "*" may be included once in a DNS name host specification. If it is included, it must be in the left-most position, as in `*.example.com`.

The port (or portrange) is optional. A port specification of the form `N-`, where `N` is a port number, signifies all ports numbered `N` and above. A specification of the form `-N` indicates all ports numbered `N` and below.

The `listen` action is only meaningful when used with a localhost. The `resolve` (resolve host/IP name service lookups) action is implied when any of the other actions are present.

For example, when creating SocketPermissions, note that if the following permission is granted to some code, it allows that code to connect to `port 1645` on `machine1.example.com,` and to accept connections on that port:

```
permission java.net.SocketPermission machine1.example.com:5030, "connect,accept";
```

Similarly, if the following permission is granted to some code, it allows that code to accept connections on, connect to, or listen to any port between 1024 and 65535 on the local host:

```
permission java.net.SocketPermission "machine1.example.com:5030", "connect,accept";
permission java.net.SocketPermission "localhost:1024-", "accept,connect,listen";
```

Note – Granting code permission to accept or make connections to remote hosts may cause problems, because malevolent code can then more easily transfer and share confidential data among parties who may not otherwise have access to the data. Make sure to give only appropriate permissions by specifying exact port number instead of allowing a range of port numbers

---

SAML

The Security Assertion Markup Language (SAML) authentication module receives and validates SAML Assertions on a target server. SAML SSO will only work if this module is configured on the target machine, including after an upgrade (for example, Access Manager 2005Q1 to Access Manager 2005Q4).

SecurID

Access Manager can be configured to handle SecurID Authentication requests to RSA's ACE/Server authentication servers. Access Manager provides the client portion of SecurID authentication. The ACE/Server may exist on the system on which Access Manager is installed, or on a separate system. In order to authenticate locally-administered userids (see `admintool` (1M)), root access is required.

SecurID Authentication makes use of an authentication *helper*, `amsecuridd`, which is a separate process from the main Access Manager process. Upon startup, this helper listens on a port for configuration information. If Access Manager is installed to run as `nobody`, or a userid other than root, then the *AccessManager-base*`/SUNWam/share/bin/amsecuridd` process must still execute as root. For more information on the `amsecuridd` helper, see Chapter 20, "The amsecuridd Helper."

Note – For this release of Access Manager, 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 SPARC systems.

UNIX

Access Manager can be configured to process authentication requests against Unix userids and passwords known to the Solaris or Linux system on which Access Manager is installed. While there is only one realm attribute, and a few global attributes for Unix authentication, there are some system-oriented considerations. In order to authenticate locally-administered userids (see admintool (1M)), root access is required

Unix Authentication makes use of an authentication *helper*, amunixd, which is a separate process from the main Access Manager process. Upon startup, this helper listens on a port for configuration information. There is only one Unix helper per Access Manager to serve all of its realms.

If Access Manager is installed to run as nobody, or a userid other than root, then the *AccessManager-base*/SUNWam/share/bin/amunixd process must still execute as root. The Unix authentication module invokes the amunixd daemon by opening a socket to localhost:58946 to listen for Unix authentication requests. To run the amunixd helper process on the default port, enter the following command:

```
./amunixd
```

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

```
./amunixd [-c portnm] [ipaddress]
```

The ipaddress and portnumber is located in the UnixHelper.ipadrs (in IPV4 format) and UnixHelper.port attributes in AMConfig.properties . You can run amunixd through the amserver command line utility (amserver runs the process automatically, retrieving the port number and IP address from AMConfig.properties).

The passwd entry in the /etc/nsswitch.conf file determines whether the /etc/passwd and /etc/shadow files, or NIS are consulted for authentication.

Windows Desktop SSO

The Windows Desktop SSO Authentication module is a Kerberos-based authentication plug-in module used for Windows 2000™. It allows a user who has already authenticated to a Kerberos Distribution Center (KDC) to authenticate to Access Manager without re-submitting the login criteria (Single Sign-on).

The user presents the Kerberos token to the Access Manager through the SPNEGO (Simple and Protected GSS-API Negotiation Mechanism) protocol. In order to perform Kerberos-based Single Sign-on to Access Manager through this authentication module, the user must, on the client side, support the SPNEGO protocol to authenticate itself. In general, any user that supports this protocol should be able to use this module to authenticate to Access Manager. Depending on the availability of the token on the client side, this module provides a SPENGO token or a Kerberos token (in both cases, the protocols are the same). Microsoft Internet Explorer (5.01 or later) running on Windows 2000 (or later) currently supports this protocol. In addition, Mozilla 1.4 on Solaris (9 and 10) has SPNEGO support, but the token returned is only a KERBEROS token, because SPNEGO is not supported on Solaris.

Note – You must use JDK 1.4 or above to utilize the new features of Kerberos V5 authentication module and Java GSS API to perform Kerberos based SSO in this SPNEGO module.

Known Restriction with Internet Explorer

If you are using Microsoft Internet Explorer 6.x when for WindowsDesktopSSO authentication and the browser does not have access to the user's Kerberos/SPNEGO token that matches the (KDC) realm configured in the WindowsDesktopSSO module, the browser will behave incorrectly to other modules after it fails authenticating to the WindowsDesktopSSO module. The direct cause of the problem is that after Internet Explorer fails the WindowsDesktopSSO module, the browser becomes incapable of passing callbacks (of other modules) to Access Manager, even if the callbacks are prompted, until the browser is restarted. Therefore all the modules coming after WindowsDesktopSSO will fail due to null user credentials.

See the following documentation for related information:

http://support.microsoft.com/default.aspx?scid=kb;en-us;308074 (`http://support.microsoft.com/default.aspx?scid=kb;en-us;308074`)

http://www.wedgetail.com/jcsi/sso/doc/guide/troubleshooting.html#ieNTLM (`http://support.microsoft.com/default.aspx?scid=kb;en-us;308074`)

Configuring Windows Desktop SSO

Enabling Windows Desktop SSO Authentication is a two-step process:

1. Create a User in the Windows 2000 Domain Controller.
2. Setup Internet Explorer.

▼ To Create a User in the Windows 2000 Domain Controller

1 In the domain controller, create a user account for the Access Manager authentication module.

a. From the Start menu, go to Programs>Administration Tools.

b. Select Active Directory Users and Computers.

c. Create a new user with the Access Manager host name as the User ID (login name). The Access Manager host name should not include the domain name.

2 Associate the user account with a service provider name and export the keytab files to the system in which Access Manager is installed. To do so, run the following commands:

```
ktpass -princ host/hostname.domainname@DCDOMAIN -pass password -mapuser userName-out
hostname.host.keytab
```

```
ktpass -princ HTTP/hostname.domainname@DCDOMAIN -pass
password -mapuser userName-out hostname
.HTTP.keytab
```

The `ktpass` command accepts the following parameters:

hostname. The host name (without the domain name) on which Access Manager runs.

domainname . The Access Manager domain name.

DCDOMAIN. The domain name of the domain controller. This may be different from the Access Manager domain name.

password . The password of the user account. Make sure that password is correct, as `ktpass` does not verify passwords.

userName. The user account ID. This should be the same as hostname.

Note – Make sure that both keytab files are kept secure.

The service template values should be similar to the following example:

Service Principal: `HTTP/machine1.EXAMPLE.COM@ISQA.EXAMPLE.COM`

Keytab File Name: `/tmp/machine1.HTTP.keytab`

Kerberos Realm: `ISQA.EXAMPLE.COM`

Kerberos Server Name: `machine2.EXAMPLE.com`

Return Principal with Domain Name: `false`

Authentication Level: `22`

3 **Restart the server.**

▼ To Set Up Internet Explorer

These steps apply to Microsoft Internet Explorer™ 6 and later. If you are using an earlier version, make sure that Access Manager is in the browser's internet zone and enable Native Windows Authentication.

1 **In the Tool menu, go to Internet Options>Advanced/Security>Security.**

2 **Select the Integrated Windows Authentication option.**

3 **Go to Security>Local Internet.**

a. **Select Custom Level. In the User Authentication/Logon panel, select the Automatic Logon Only in Intranet Zone option.**

b. **Go to Sites and select all of the options.**

c. **Click Advanced and add the Access Manager to the local zone (if it is not added already).**

Windows NT

Access Manager can be configured to work with an Windows NT /Windows 2000 server that is already installed. Access Manager provides the client portion of NT authentication.

1. Configure the NT server. For detailed instructions, see the Windows NT server documentation.
2. Before you can add and enable the Windows NT authentication module, you must obtain and install a Samba client to communicate with Access Manager on your Solaris system.

Installing the Samba Client

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

```
AccessManager-base/SUNWam/bin
```

Samba Client is a file and print server for blending Windows and UNIX machines together without requiring a separate Windows NT/2000 Server. More information, and the download itself, can be accessed at http://wwws.sun.com/software/download/products/3e3af224.html.

Red Hat Linux ships with a Samba client, located in the following directory:

```
/usr/bin
```

In order to authenticate using the Windows NT Authentication module for Linux, copy the client binary to the following Access Manager directory:

```
AccessManager-base/sun/identity/bin
```

Note – If you have multiple interfaces, extra configuration is required. Multiple interfaces can be set by configuration in the `smb.conf` file so it passes to the `mbclient`.

Authentication Module Instances

Multiple authentication module instances can be crated for the realm, based on the default authentication modules. You can add individually configured multiple instances of the same authentication module.

▼ To Create a New Authentication Module Instance

1. **Click the name of the realm for which you wish to add a new authentication module instance.**

2. **Select the Authentication tab.**

   Note – The Administrator Authentication Configuration button 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.

3. **Click New in the Module Instances list.**

4. **Enter a Name for the authentication module instance. The names must be unique.**

5. **Select the Type of authentication module type for the realm.**

6. **Click Create.**

7. **Click the name of the newly created module instance and edit the properties for that module. See the Authentication section in the online help for definitions for the properties for each module type.**

8. **Repeat these steps to add multiple module instances.**

Authentication Chaining

One or more authentication modules can be configured so a user must pass authentication credentials to all of them. This is referred to as *authentication chaining* . Authentication chaining in Access Manager is achieved using the JAAS framework integrated in the Authentication Service. Module chaining is configured under the Authentication Configuration service.

▼ To Create a New Authentication Chain

1. **Click the name of the realm for which you wish to add a new authentication chain.**

2. **Select the Authentication tab.**

3. **Click New in the Authentication Chaining list.**

4 **Enter a name for the authentication chain.**

5 **Click Create.**

6 **Click Add to define the authentication module instance that you wish to include in the chain. To do so, select the module instance name from the Instance list. The module instance names displayed in this list are created in the Module Instances attribute.**

7 **Select the criteria for the chain. These flags establish an enforcement criteria for the authentication module for which they are defined. There is hierarchy for enforcement. Required is the highest and Optional is the lowest:**

Requisite	The module instance is required to succeed. If it succeeds, authentication continues down the Authentication Chaining list. If it fails, control immediately returns to the application (authentication does not proceed down the Authentication Chaining list).
Required	Authentication to this module is required to succeed. If any of the required modules in the chain fails, the whole authentication chain will ultimately fail. However, whether a required module succeeds or fails, the control will continue down to the next module in the chain.
Sufficient	The module instance is not required to succeed. If it does succeed, control immediately returns to the application (authentication does not proceed down the module instance list). If it fails, authentication continues down the Authentication Chaining list.
Optional	The module instance is not required to succeed. If it succeeds or fails, authentication still continues to proceed down the Authentication Chaining list.

8 **Enter options for the chain. This enables additional options for the module as a key=value pair. Multiple options are separated by a space.**

9 **Define the following attributes:**

Successful Login URL	Specifies the URL that the user will be redirected to upon successful authentication.
Failed Login URL	Specifies the URL that the user will be redirected to upon unsuccessful authentication.
Authentication Post Processing Class	Defines the name of the Java class used to customize the post authentication process after a login success or failure.

10 **Click Save.**

Authentication Types

The Authentication Service provides different ways in which authentication can be applied. These different authentication methods can be accessed by specifying Login URL parameters, or through the authentication APIs (see Chapter 5, "Using Authentication APIs and SPIs," in *Sun Java System Access Manager 7 2005Q4 Developer's Guide* in the Developer's Guide for more information). Before an authentication module can be configured, the Core authentication service attribute realm Authentication Modules must be modified to include the specific authentication module name.

The Authentication Configuration service is used to define authentication modules for any of the following authentication types:

- "Realm-based Authentication" on page 96
- "Organization-based Authentication" on page 98
- "Role-based Authentication" on page 101
- "Service-based Authentication" on page 104
- "User-based Authentication" on page 107
- "Authentication Level-based Authentication" on page 109
- "Module-based Authentication" on page 112

Once an authentication module is defined for one of these authentication types, the module can be configured to supply redirect URLs, as well as a post-processing Java class specification, based on a successful or failed authentication process.

How Authentication Types Determine Access

For each of these methods, the user can either pass or fail the authentication. Once the determination has been made, each method follows this procedure. Step 1 through Step 3 follows a successful authentication; Step 4 follows both successful and failed authentication.

1. Access Manager confirms whether the authenticated user(s) is defined in the Directory Server data store and whether the profile is active.

   The User Profile attribute in the Core Authentication module can be defined as `Required`, `Dynamic, Dynamic with User Alias, or Ignored`. Following a successful authentication, Access Manager confirms whether the authenticated user(s) is defined in the Directory Server data store and, if the User Profile value is `Required`, confirms that the profile is active. (This is the default case.) If the User Profile is `Dynamically Configured, the` Authentication Service will create the user profile in the Directory Server data store. If the User Profile is set to `Ignore`, the user validation will not be done.
2. Execution of the Authentication Post Processing SPI is accomplished.

The Core Authentication module contains an Authentication Post Processing Class attribute which may contain the authentication post-processing class name as its value. `AMPostAuthProcessInterface` is the post-processing interface. It can be executed on either successful or failed authentication or on logout.

3. The following properties are added to, or updated in, the session token and the user's session is activated.

   realm. This is the DN of the realm to which the user belongs.

   Principal. This is the DN of the user.

   Principals. This is a list of names to which the user has authenticated. (This property may have more then one value defined as a pipe separated list.)

   UserId. This is the user's DN as returned by the module, or in the case of modules other than LDAP or Membership, the user name. (All Principals must map to the same user. The UserID is the user DN to which they map.)

   Note – This property may be a non-DN value.

   UserToken. This is a user name. (All Principals must map to the same user. The UserToken is the user name to which they map.)

   Host. This is the host name or IP address for the client.

   authLevel. This is the highest level to which the user has authenticated.

   AuthType. This is a pipe separated list of authentication modules to which the user has authenticated (for example, `module1|module2|module3).`

   clientType. This is the device type of the client browser.

   Locale. This is the locale of the client.

   CharSet. This is the determined character set for the client.

   Role. Applicable for role-based authentication only, this is the role to which the user belongs.

   Service. Applicable for service-based authentication only, this is the service to which the user belongs.

4. Access Manager looks for information on where to redirect the user after either a successful or failed authentication.

URL redirection can be to either an Access Manager page or a URL. The redirection is based on an order of precedence in which Access Manager looks for redirection based on the authentication method and whether the authentication has been successful or has failed. This order is detailed in the URL redirection portions of the following authentication methods sections.

URL Redirection

In the Authentication Configuration service, you can assign URL redirection for successful or unsuccessful authentication. The URLs, themselves, are defined in the Login Success URL and Login Failure URL attributes in this service. In order to enable URL redirection, you must add the Authentication Configuration service to your realm to make it available to configure for a role, realm, or user. Make sure that you add an authentication module, such as LDAP - REQUIRED, when adding the Authentication Configuration service.

Realm-based Authentication

This method of authentication allows a user to authenticate to an realm or sub-realm. It is the default method of authentication for Access Manager . The authentication method for an realm is set by registering the Core Authentication module to the realm and defining the realm Authentication Configuration attribute.

Realm-based Authentication Login URLs

The realm for authentication can be specified in the User Interface Login URL by defining the `realm` Parameter or the `domain` Parameter. The realm of a request for authentication is determined from the following, in order of precedence:

1. The `domain` parameter.
2. The `realm` parameter.
3. The value of the `DNS Alias Names` attribute in the Administration Service.

   After calling the correct realm, the authentication module(s) to which the user will authenticate are retrieved from the realm Authentication Configuration attribute in the Core Authentication Service. The login URLs used to specify and initiate realm-based authentication are:

   ```
   http://server_name.domain_name:port/amserver/UI/Login
   http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name
   http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name
   ```

   If there is no defined parameter, the realm will be determined from the server host and domain specified in the login URL.

Realm-based Authentication Redirection URLs

Upon a successful or failed organization-based authentication, Access Manager looks for information on where to redirect the user. Following is the order of precedence in which the application will look for this information.

Successful realm-based Authentication Redirection URLs

The redirection URL for successful realm-based authentication is determined by checking the following places in order of precedence:

1. A URL set by the authentication module.
2. A URL set by a `goto` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute as a global default.
7. A URL set in the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
8. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
9. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.
10. A URL set in the `iplanet-am-auth-login-success-url` attribute as a global default.

Failed Realm-based Authentication Redirection URLs

The redirection URL for failed realm-based authentication is determined by checking the following places in the following order:

1. A URL set by the authentication module.
2. A URL set by a `gotoOnFail` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-failure-url` attribute of the user's entry (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute of the user's role entry.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute of the user's realm entry.

6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute as a global default.
7. A URL set for the `iplanet-am-user-failure-url` attribute in the user's entry (`amUser.xml`).
8. A URL set for the `iplanet-am-auth-login-failure-url` attribute of the user's role entry.
9. A URL set for the `iplanet-am-auth-login-failure-url` attribute of the user's realm entry.
10. A URL set for the `iplanet-am-auth-login-failure-url` attribute as the global default.

To Configure Realm-Based Authentication

Authentication modules are set for realms by first adding the Core Authentication service to the realm.

▼ To Configure The Realms's Authentication Attributes

1 **Navigate to the realm for which you wish to add the Authentication Chain.**

2 **Click the Authentication tab.**

3 **Select the Default Authentication Chain from the pull down menu.**

4 **Select the Administrator Authentication Chain from the pull down menu. This attribute can be used if the authentication module for administrators needs to be different from the module for end users. The default authentication module is LDAP.**

5 **Once you have defined the authentication chains, click Save.**

Organization-based Authentication

This authentication type only applies to Access Manager deployments that have been installed in Legacy mode.

This method of authentication allows a user to authenticate to an organization or sub-organization. It is the default method of authentication for Access Manager . The authentication method for an organization is set by registering the Core Authentication module to the organization and defining the Organization Authentication Configuration attribute.

Organization-based Authentication Login URLs

The organization for authentication can be specified in the User Interface Login URL by defining the `org` Parameter or the `domain` Parameter. The organization of a request for authentication is determined from the following, in order of precedence:

1. The `domain` parameter.
2. The `org` parameter.
3. The value of the `DNS Alias Names` (Organization alias names) attribute in the Administration Service.

   After calling the correct organization, the authentication module(s) to which the user will authenticate are retrieved from the Organization Authentication Configuration attribute in the Core Authentication Service. The login URLs used to specify and initiate organization-based authentication are:

   ```
   http://server_name.domain_name:port/amserver/UI/Login
   http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name
   http://server_name.domain_name:port/amserver/UI/Login?org=org_name
   ```

   If there is no defined parameter, the organization will be determined from the server host and domain specified in the login URL.

Organization-based Authentication Redirection URLs

Upon a successful or failed organization-based authentication, Access Manager looks for information on where to redirect the user. Following is the order of precedence in which the application will look for this information.

Successful Organization-based Authentication Redirection URLs

The redirection URL for successful organization-based authentication is determined by checking the following places in order of precedence:

1. A URL set by the authentication module.
2. A URL set by a `goto` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's organization entry.
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute as a global default.

7. A URL set in the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
8. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
9. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's organization entry.
10. A URL set in the `iplanet-am-auth-login-success-url` attribute as a global default.

Failed Organization-based Authentication Redirection URLs

The redirection URL for failed organization-based authentication is determined by checking the following places in the following order:

1. A URL set by the authentication module.
2. A URL set by a `gotoOnFail` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-failure-url` attribute of the user's entry (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute of the user's role entry.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute of the user's organization entry.
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute as a global default.
7. A URL set for the `iplanet-am-user-failure-url` attribute in the user's entry (`amUser.xml`).
8. A URL set for the `iplanet-am-auth-login-failure-url` attribute of the user's role entry.
9. A URL set for the `iplanet-am-auth-login-failure-url` attribute of the user's organization entry.
10. A URL set for the `iplanet-am-auth-login-failure-url` attribute as the global default.

To Configure Organization-Based Authentication

Authentication modules are set for an organization by first adding the Core Authentication service to the organization.

▼ To Configure The Organizations's Authentication Attributes

1 **Navigate to the organization for which you wish to add the Authentication Chain.**

2 **Click the Authentication tab.**

3 **Select the Default Authentication Chain from the pull down menu.**

4 **Select the Administrator Authentication Chain from the pull down menu. This attribute can be used if the authentication module for administrators needs to be different from the module for end users. The default authentication module is LDAP.**

5 **Once you have defined the authentication chains, click Save.**

Role-based Authentication

This method of authentication allows a user to authenticate to a role (either static or filtered) within an realm or sub realm.

Note – The Authentication Configuration Service must first be registered to the realm before it can be registered as an instance to the role.

For authentication to be successful, the user must belong to the role and they must authenticate to each module defined in the Authentication Configuration Service instance configured for that role. For each instance of role-based authentication, the following attributes can be specified:

Conflict Resolution Level. This sets a priority level for the Authentication Configuration Service instance defined for different roles that both may contain the same user. For example, if `User1` is assigned to both `Role1` and `Role2`, a higher conflict resolution level can be set for `Role1` so when the user attempts authentication, `Role1` will have the higher priority for success or failure redirects and post-authentication processes.

Authentication Configuration. This defines the authentication modules configured for the role's authentication process.

Login Success URL. This defines the URL to which a user is redirected on successful authentication.

Login Failed URL. This defines the URL to which a user is redirected on failed authentication.

Authentication Post Processing Classes. This defines the post-authentication interface.

Role-based Authentication Login URLs

Role-based authentication can be specified in The User Interface Login URL by defining a role Parameter. After calling the correct role, the authentication module(s) to which the user will authenticate are retrieved from the Authentication Configuration Service instance defined for the role.

The login URLs used to specify and initiate this role-based authentication are:

```
http://server_name.domain_name:port/amserver/UI/Login?role=role_name
http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name&role=role_name
```

If the realm Parameter is not configured, the realm to which the role belongs is determined from the server host and domain specified in the login URL itself.

Role-based Authentication Redirection URLs

Upon a successful or failed role-based authentication, Access Manager looks for information on where to redirect the user. Following is the order of precedence in which the application will look for this information.

Successful Role-based Authentication Redirection URLs

The redirection URL for successful role-based authentication is determined by checking the following places in the following order:

1. A URL set by the authentication module.
2. A URL set by a `goto` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the role to which the user has authenticated.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of another role entry of the authenticated user. (This option is a fallback if the previous redirection URL fails.)
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.
7. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute as a global default.
8. A URL set in the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
9. A URL set in the `iplanet-am-auth-login-success-url` attribute of the role to which the user has authenticated.

10. A URL set in the iplanet-am-auth-login-success-url attribute of another role entry of the authenticated user. (This option is a fallback if the previous redirection URL fails.)
11. A URL set in the iplanet-am-auth-login-success-url attribute of the user's realm entry.
12. A URL set in the iplanet-am-auth-login-success-url attribute as a global default.

Failed Role-based Authentication Redirection URLs

The redirection URL for failed role-based authentication is determined by checking the following places in the following order:

1. A URL set by the authentication module.
2. A URL set by a goto Login URL parameter.
3. A URL set in the clientType custom files for the iplanet-am-user-failure-url attribute of the user's profile (amUser.xml).
4. A URL set in the clientType custom files for the iplanet-am-auth-login-failure-url attribute of the role to which the user has authenticated.
5. A URL set in the clientType custom files for the iplanet-am-auth-login-failure-url attribute of another role entry of the authenticated user. (This option is a fallback if the previous redirection URL fails.)
6. A URL set in the clientType custom files for the iplanet-am-auth-login-failure-url attribute of the user's realm entry.
7. A URL set in the clientType custom files for the iplanet-am-auth-login-failure-url attribute as a global default.
8. A URL set in the iplanet-am-user-failure-url attribute of the user's profile (amUser.xml).
9. A URL set in the iplanet-am-auth-login-failure-url attribute of the role to which the user has authenticated.
10. A URL set in the iplanet-am-auth-login-failure-url attribute of another role entry of the authenticated user. (This option is a fallback if the previous redirection URL fails.)
11. A URL set in the iplanet-am-auth-login-failure-url attribute of the user's realm entry.
12. A URL set in the iplanet-am-auth-login-failure-url attribute as a global default.

▼ To Configure Role-Based Authentication

1 Navigate to the realm (or organization) to which you will add the authentication configuration service.

2 Click the Subjects tab.

3 **Filtered Roles or Roles.**

4 **Select the role for which to set the authentication configuration.**

If the Authentication Configuration service has not been added to the role, click Add, select Authentication Service and click Next.

5 **Select the Default Authentication Chain that you wish to enable from the pull down menu.**

6 **Click Save.**

Note – If you are creating a new role, the Authentication Configuration service is not automatically assigned to it. Make sure that you select the Authentication Configuration service option at the top of the role profile page before you create it.

When role-based authentication is enabled, the LDAP authentication module can be left as the default, as there is no need to configure Membership.

Service-based Authentication

This method of authentication allows a user to authenticate to a specific service or application registered to an realm or sub realm. The service is configured as a Service Instance within the Authentication Configuration Service and is associated with an Instance Name. For authentication to be successful, the user must authenticate to each module defined in the Authentication Configuration service instance configured for the service. For each instance of service-based authentication, the following attributes can be specified:

Authentication Configuration. This defines the authentication modules configured for the service's authentication process.

Login Success URL. This defines the URL to which a user is redirected on successful authentication.

Login Failed URL. This defines the URL to which a user is redirected on failed authentication.

Authentication Post Processing Classes. This defines the post-authentication interface.

Service-based Authentication Login URLs

Service-based authentication can be specified in the User Interface Login URL by defining a service Parameter. After calling the service, the authentication module(s) to which the user will authenticate are retrieved from the Authentication Configuration service instance defined for the service.

The login URLs used to specify and initiate this service-based authentication are:

```
http://server_name.domain_name:port/amserver/UI/
Login?service=auth-chain-name
```

and

```
http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name&service=auth-chain-name
e
```

If there is no configured `org` parameter, the realm will be determined from the server host and domain specified in the login URL itself.

Service-based Authentication Redirection URLs

Upon a successful or failed service-based authentication, Access Manager looks for information on where to redirect the user. Following is the order of precedence in which the application will look for this information.

Successful Service-based Authentication Redirection URLs

The redirection URL for successful service-based authentication is determined by checking the following places in the following order:

1. A URL set by the authentication module.
2. A URL set by a `goto` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the service to which the user has authenticated.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.
7. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute as a global default.
8. A URL set in the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
9. A URL set in the `iplanet-am-auth-login-success-url` attribute of the service to which the user has authenticated.
10. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
11. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.

12. A URL set in the iplanet-am-auth-login-success-url attribute as a global default.

Failed Service-based Authentication Redirection URLs

The redirection URL for failed service-based authentication is determined by checking the following places in the following order:

1. A URL set by the authentication module.
2. A URL set by a goto Login URL parameter.
3. A URL set in the clientType custom files for the iplanet-am-user-failure-url attribute of the user's profile (amUser.xml).
4. A URL set in the clientType custom files for the iplanet-am-auth-login-failure-url attribute of the service to which the user has authenticated.
5. A URL set in the clientType custom files for the iplanet-am-auth-login-failure-url attribute of the user's role entry.
6. A URL set in the clientType custom files for the iplanet-am-auth-login-failure-url attribute of the user's realm entry.
7. A URL set in the clientType custom files for the iplanet-am-auth-login-failure-url attribute as a global default.
8. A URL set in the iplanet-am-user-failure-url attribute of the user's profile (amUser.xml).
9. A URL set in the iplanet-am-auth-login-failure-url attribute of the service to which the user has authenticated.
10. A URL set in the iplanet-am-auth-login-failure-url attribute of the user's role entry.
11. A URL set in the iplanet-am-auth-login-failure-url attribute of the user's realm entry.
12. A URL set in the iplanet-am-auth-login-failure-url attribute as a global default.

▼ To Configure Service-Based Authentication

Authentication modules are set for services after adding the Authentication Configuration service. To do so:

1. **Chose the realm to which you wish to configure service-based authentication.**

2. **Click the Authentication tab.**

3. **Create the authentication module instances.**

4. **Create the authentication chains.**

5 **Click Save.**

6 **To access service-based authentication for the realm, enter the following address:**

`http://`*server_name.domain_name:port*`/amserver/UI/Login?realm=`*realm_name&service=auth-cha*

User-based Authentication

This method of authentication allows a user to authenticate to an authentication process configured specifically for the user. The process is configured as a value of the User Authentication Configuration attribute in the user's profile. For authentication to be successful, the user must authenticate to each module defined.

User-based Authentication Login URLs

User-based authentication can be specified in the User Interface Login URL by defining a user Parameter. After calling the correct user, the authentication module(s) to which the user will authenticate are retrieved from the User Authentication Configuration instance defined for the user.

The login URLs used to specify and initiate this role-based authentication are:

```
http://server_name.domain_name:port/amserver/UI/Login?user=user_name
http://server_name.domain_name:port/amserver/UI/Login?org=org_name&user=user_name
```

If there is no configured realm Parameter, the realm to which the role belongs will be determined from the server host and domain specified in the login URL itself.

User Alias List Attribute

On receiving a request for user-based authentication, the Authentication service first verifies that the user is a valid user and then retrieves the Authentication Configuration data for them. In the case where there is more then one valid user profile associated with the value of the user Login URL parameter, all profiles must map to the specified user. The User Alias Attribute (`iplanet-am-user-alias-list`) in the User profile is where other profiles belonging to the user can be defined. If mapping fails, the user is denied a valid session. The exception would be if one of the users is a top-level admin whereby the user mapping validation is not done and the user is given top—level Admin rights.

User-based Authentication Redirection URLs

Upon a successful or failed user-based authentication, Access Manager looks for information on where to redirect the user. Following is the order of precedence in which the application will look for this information.

Successful User-based Authentication Redirection URLs

The redirection URL for successful user-based authentication is determined by checking the following places in order of precedence:

1. A URL set by the authentication module.
2. A URL set by a `goto` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute as a global default.
7. A URL set in the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
8. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
9. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.
10. A URL set in the `iplanet-am-auth-login-success-url` attribute as a global default.

Failed User-based Authentication Redirection URLs

The redirection URL for failed user-based authentication is determined by checking the following places in the following order:

1. A URL set by the authentication module.
2. A URL set by a `gotoOnFail` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-failure-url` attribute of the user's entry (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute of the user's role entry.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute of the user's realm entry.
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute as a global default.
7. A URL set for the `iplanet-am-user-failure-url` attribute in the user's entry (`amUser.xml`).
8. A URL set for the `iplanet-am-auth-login-failure-url` attribute of the user's role entry.

9. A URL set for the `iplanet-am-auth-login-failure-url` attribute of the user's realm entry.
10. A URL set for the `iplanet-am-auth-login-failure-url` attribute as the global default.

▼ To Configure User-Based Authentication

1 **Navigate to the realm in which you wish to configure authentication for the user.**

2 **Click the Subjects tab and click Users.**

3 **Click the name of the user you wish to modify**

The User Profile is displayed.

Note – If you are creating a new user, the Authentication Configuration service is not automatically assigned to the user. Make sure that you select the Authentication Configuration service option in the Service profile before you create the user. If this option is not selected, the user will not inherit the authentication configuration defined at for the role.

---

4 **In the User Authentication Configuration attribute, select the authentication chain you wish to apply.**

5 **Click Save.**

Authentication Level-based Authentication

Each authentication module can be associated with an integer value for its *authentication level*. Authentication levels can be assigned by clicking the authentication module's Properties arrow in Service Configuration, and changing the corresponding value for the module's Authentication Level attribute. Higher authentication levels define a higher level of trust for the user once that user has authenticated to one or more authentication modules.

The authentication level will be set on a user's SSO token after the user has successfully authenticated to the module. If the user is required to authenticate to multiple authentication modules, and does so successfully, the highest authentication level value will be set in user's SSO token.

If a user attempts to access a service, the service can determine if the user is allowed access by checking the authentication level in user's SSO token. It then redirects the user to go through the authentication modules with a set authentication level.

Users can also access authentication modules with specific authentication level. For example, a user performs a login with the following syntax:

```
http://hostname:port/deploy_URI/UI/Login?authlevel=
auth_level_value
```

All modules whose authentication level is larger or equal to *auth_level_value* will be displayed as an authentication menu for the user to choose. If only one matching module is found, then the login page for that authentication module will be directly displayed.

This method of authentication allows an administrator to specify the security level of the modules to which identities can authenticate. Each authentication module has a separate Authentication Level attribute and the value of this attribute can be defined as any valid integer. With Authentication Level-based authentication, the Authentication Service displays a module login page with a menu containing the authentication modules that have authentication levels equal to or greater then the value specified in the Login URL parameter. Users can select a module from the presented list. Once the user selects a module, the remaining process is based on Module-based Authentication.

Authentication Level-based Authentication Login URLs

Authentication level-based authentication can be specified in the User Interface Login URL by defining the authlevel Parameter. After calling the login screen with the relevant list of modules, the user must choose one with which to authenticate. The login URLs used to specify and initiate authentication level-based authentication are:

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=authentication_level
```

and

```
http://server_name.domain_name:port/amserver/UI/
Login?realm=realm_name&authlevel=authentication_level
```

If there is no configured `realm` parameter, the realm to which the user belongs will be determined from the server host and domain specified in the login URL itself.

Authentication Level-based Authentication Redirection URLs

Upon a successful or failed authentication level-based authentication, Access Manager looks for information on where to redirect the user. Following is the order of precedence in which the application will look for this information.

Successful Authentication Level-based Authentication Redirection URLs

The redirection URL for successful authentication level-based authentication is determined by checking the following places in order of precedence:

1. A URL set by the authentication module.

2. A URL set by a `goto` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute as a global default.
7. A URL set in the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
8. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
9. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.
10. A URL set in the `iplanet-am-auth-login-success-url` attribute as a global default.

Failed Authentication Level-based Authentication Redirection URLs

The redirection URL for failed authentication level-based authentication is determined by checking the following places in the following order:

1. A URL set by the authentication module.
2. A URL set by a `gotoOnFail` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-failure-url` attribute of the user's entry (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute of the user's role entry.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute of the user's realm entry.
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute as a global default.
7. A URL set for the `iplanet-am-user-failure-url` attribute in the user's entry (`amUser.xml`).
8. A URL set for the `iplanet-am-auth-login-failure-url` attribute of the user's role entry.
9. A URL set for the `iplanet-am-auth-login-failure-url` attribute of the user's realm entry.
10. A URL set for the `iplanet-am-auth-login-failure-url` attribute as the global default.

Module-based Authentication

Users can access a specific authentication module using the following syntax:

```
http://hostname:port/deploy_URI/UI/Login?module=
module_name
```

Before the authentication module can be accessed, the Core authentication service attribute realm Authentication Modules must be modified to include the authentication module name. If the authentication module name is not included in this attribute, the "authentication module denied" page will be displayed when the user attempts to authenticate.

This method of authentication allows a user to specify the module to which they will authenticate. The specified module must be registered to the realm or sub-realm that the user is accessing. This is configured in the realm Authentication Modules attribute of the realm's Core Authentication Service. On receiving this request for module-based authentication, the Authentication Service verifies that the module is correctly configured as noted, and if the module is not defined, the user is denied access.

Module-based Authentication Login URLs

Module-based authentication can be specified in the User Interface Login URL by defining a module Parameter. The login URLs used to specify and initiate module-based authentication are:

```
http://server_name.domain_name:port/amserver/UI/Login?module=authentication_module_name
http://server_name.domain_name:port/amserver/UI/
Login?org=org_name&module=authentication_module_name
```

If there is no configured `org` parameter, the realm to which the user belongs will be determined from the server host and domain specified in the login URL itself.

Module-based Authentication Redirection URLs

Upon a successful or failed module-based authentication, Access Manager looks for information on where to redirect the user. Following is the order of precedence in which the application will look for this information.

Successful Module-based Authentication Redirection URLs

The redirection URL for successful module-based authentication is determined by checking the following places in order of precedence:

1. A URL set by the authentication module.
2. A URL set by a `goto` Login URL parameter.

3. A URL set in the `clientType` custom files for the `iplanet-am-user-success-url` attribute of the user's profile (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-success-url` attribute as a global default.
7. A URL set in the `iplanet-am-user-success-url` attribute of the user's profile `(amUser.xml).`
8. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's role entry.
9. A URL set in the `iplanet-am-auth-login-success-url` attribute of the user's realm entry.
10. A URL set in the `iplanet-am-auth-login-success-url` attribute as a global default.

Failed Module-based Authentication Redirection URLs

The redirection URL for failed module-based authentication is determined by checking the following places in the following order:

1. A URL set by the authentication module.
2. A URL set by a `gotoOnFail` Login URL parameter.
3. A URL set in the `clientType` custom files for the `iplanet-am-user-failure-url` attribute of the user's entry (`amUser.xml`).
4. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute of the user's role entry.
5. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute of the user's realm entry.
6. A URL set in the `clientType` custom files for the `iplanet-am-auth-login-failure-url` attribute as a global default.
7. A URL set for the `iplanet-am-auth-login-failure-url` attribute of the user's role entry.
8. A URL set for the `iplanet-am-auth-login-failure-url` attribute of the user's realm entry.
9. A URL set for the `iplanet-am-auth-login-failure-url` attribute as the global default.

The User Interface Login URL

The Authentication Service user interface is accessed by entering a login URL into the Location Bar of a web browser. This URL is:

`http://`*AccessManager-root/.domain_name:port* `/`*service_deploy_uri* `/UI/Login`

Note – During installation, the *service_deploy_uri* is configured as `amserver`. This default service deployment URI will be used throughout this document.

The user interface login URL can also be appended with Login URL Parameters to define specific authentication methods or successful/failed authentication redirection URLs.

Login URL Parameters

A URL parameter is a name/value pair appended to the end of a URL. The parameter starts with a question mark (`?`) and takes the form `name=value`. A number of parameters can be combined in one login URL, for example:

```
http://server_name.domain_name:port/amserver/UI/
Login?module=LDAP&locale=ja&goto=http://www.sun.com
```

If more than one parameter exists, they are separated by an ampersand (&). The combinations though must adhere to the following guidelines:

- Each parameter can occur only once in one URL. For example, `module=LDAP&module=NT` is not computable.
- Both the `org` parameter and the `domain` parameter determine the login realm. In this case, only one of the two parameters should be used in the login URL. If both are used and no precedence is specified, only one will take effect.
- The parameters `user`, `role`, `service`, `module` and `authlevel` are for defining authentication modules based on their respective criteria. Due to this, only one of them should be used in the login URL. If more than one is used and no precedence is specified, only one will take effect.

The following sections describe parameters that, when appended to the User Interface Login URL and typed in the Location bar of a web browser, achieve various authentication functionality.

Note – To simplify an authentication URL and parameters for distribution throughout an realm, an administrator might configure an HTML page with a simple URL that possesses links to the more complicated login URLs for all configured authentication methods.

goto Parameter

A `goto=`*successful_authentication_URL* parameter overrides the value defined in the Login Success URL of the Authentication Configuration service. It will link to the specified URL when a successful authentication has been achieved. A `goto=logout_URL` parameter can also be used to link to a specified URL when the user is logging out. For an example of a successful authentication URL:

```
http://server_name.domain_name:port/amserver/
UI/Login?goto=http://www.sun.com/homepage.html
```

An example `goto` logout URL:

```
http://server_name.domain_name:port/amserver/
UI/Logout?goto=http://www.sun.com/logout.html.
```

Note – There is an order of precedence in which Access Manager looks for successful authentication redirection URLs. Because these redirection URLs and their order are based on the method of authentication, this order (and related information) is detailed in the Authentication Types section.

gotoOnFail Parameter

A `gotoOnFail=failed_authentication_URL` parameter overrides the value defined in the Login Failed URL of the Authentication Configuration service. It will link to the specified URL if a user has failed authentication. An example `gotoOnFail` URL might be `http://`*server_name.domain_name*`:`*port*
`/amserver/UI/Login?gotoOnFail=http://www.sun.com/auth_fail.html`.

Note – There is an order of precedence in which Access Manager looks for failed authentication redirection URLs. Because these redirection URLs and their order are based on the method of authentication, this order (and related information) is detailed in Authentication Types section.

realm Parameter

The `org=`*realmName* parameter allows a user to authenticate as a user in the specified realm.

Note – A user who is not already a member of the specified realm will receive an error message when they attempt to authenticate with the `realm` parameter. A user profile, though, can be dynamically created in the Directory Server if all of the following are TRUE:

- The User Profile attribute in the Core Authentication Service must be set to `Dynamic` or `Dynamic with User Alias.`
- The user must successfully authenticate to the required module.
- The user does not already have a profile in Directory Server.

From this parameter, the correct login page (based on the realm and its locale setting) will be displayed. If this parameter is not set, the default is the top-level realm. For example, an `org` URL might be:

```
http://server_name.domain_name:port/amserver/UI/Login?realm=sun
```

org Parameter

The `org=`*orgName* parameter allows a user to authenticate as a user in the specified organization.

Note – A user who is not already a member of the specified organization will receive an error message when they attempt to authenticate with the `org` parameter. A user profile, though, can be dynamically created in the Directory Server if all of the following are TRUE:

- The User Profile attribute in the Core Authentication Service must be set to `Dynamic` or `Dynamic with User Alias.`
- The user must successfully authenticate to the required module.
- The user does not already have a profile in Directory Server.

From this parameter, the correct login page (based on the organization and its locale setting) will be displayed. If this parameter is not set, the default is the top-level organization. For example, an `org` URL might be:

```
http://server_name.domain_name:port/amserver/UI/Login?org=sun
```

user Parameter

The `user=`*userName* parameter forces authentication based on the module configured in User Authentication Configuration attribute of the user's profile. For example, one user's profile can be configured to authenticate using the Certification module while another user might be configured to authenticate using the LDAP module. Adding this parameter sends the user to their configured authentication process rather than the method configured for their organization. For example:

```
http://server_name.domain_name:port/amserver/UI/Login?user=jsmith
```

role Parameter

A `role`=roleName parameter sends the user to the authentication process configured for the specified role. A user who is not already a member of the specified role will receive an error message when they attempt to authenticate with this parameter. For example:

```
http://server_name.domain_name:port/amserver/UI/Login?role=manager.
```

locale Parameter

Access Manager has the capability to display localized screens (translated into languages other than English) for the authentication process as well as for the console itself. The `locale=`*localeName* parameter allows the specified locale to take precedence over any other defined locales. The login locale is displayed by the client after searching for the configuration in the following places, order-specific:

1. Value of locale parameter in Login URL

   The value of the `locale=`*localeName* parameter takes precedence over all other defined locales.
2. Locale defined in user's profile

   If there is no URL parameter, the locale is displayed based on the value set in the User Preferred Language attribute of the user profile.
3. Locale defined in the HTTP header

   This locale is set by the web browser.
4. Locale defined in Core Authentication Service

   This is the value of the Default Auth Locale attribute in the Core Authentication module.
5. Locale defined in Platform Service

   This is the value of the Platform Locale attribute in the Platform service.

Operating system locale

The locale derived from this pecking order is stored in the user's session token and Access Manager uses it for loading the localized authentication module only. After successful authentication, the locale defined in the User Preferred Language attribute of the user's profile is used. If none is set, the locale used for authentication will be carried over. For example:

```
http://server_name.domain_name:port/amserver/UI/Login?locale=ja.
```

Note – Information on how to localize the screen text and error messages can be found in the Access Manager.

module Parameter

The `module=`*moduleName* parameter allows authentication via the specified authentication module. Any of the modules can be specified although they must first be registered under the realm to which the user belongs and selected as one of that realm's authentication modules in the Core Authentication module. For example:

```
http://server_name.domain_name:port/amserver/UI/Login?module=Unix.
```

Note – The authentication module names are case-sensitive when used in a URL parameter.

service Parameter

The `service=`*serviceName* parameter allows a user to authenticate via a service's configured authentication scheme. Different authentication schemes can be configured for different services using the Authentication Configuration service. For example, an online paycheck application might require authentication using the more secure Certificate Authentication module while an realm's employee directory application might require only the LDAP Authentication module. An authentication scheme can be configured, and named, for each of these services. For example:

```
http://server_name.domain_name:port/amserver/UI/Login?service=sv1.
```

Note – The Authentication Configuration service is used to define a scheme for service-based authentication.

arg Parameter

The `arg=`*newsession* parameter is used to end a user's current session and begin a new one. The Authentication Service will destroy a user's existing session token and perform a new login in one request. This option is typically used in the Anonymous Authentication module. The user first authenticates with an anonymous session, and then hits the register or login link. For example:

```
http://server_name.domain_name:port/amserver/UI/Login?arg=newsession.
```

authlevel Parameter

An `authlevel=`*value* parameter tells the Authentication Service to call a module with an authentication level equal to or greater than the specified authentication level value. Each authentication module is defined with a fixed integer authentication level. For example:

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=1.
```

Note – The Authentication Level is set in each module's specific profile. .

---

domain Parameter

This parameter allows a user to login to an realm identified as the specified domain. The specified domain must match the value defined in the Domain Name attribute of the realm's profile. For example:

```
http://server_name.domain_name:port/amserver/UI/Login?domain=sun.com.
```

Note – A user who is not already a member of the specified domain/realm will receive an error message when they attempt to authenticate with the `org` parameter. A user profile, though, can be dynamically created in the Directory Server if all of the following points are TRUE:

- The User Profile attribute in the Core Authentication Service must be set to `Dynamic` or `Dynamic With User Alias .`
- The user must successfully authenticate to the required module.
- The user does not already have a profile in Directory Server.

---

iPSPCookie Parameter

The `iPSPCookie=yes` parameter allows a user to login with a persistent cookie. A persistent cookie is one that continues to exist after the browser window is closed. In order to use this parameter, the realm to which the user is logging in must have Persistent Cookies enabled in their Core Authentication module. Once the user authenticates and the browser is closed, the user can login with a new browser session and will be directed to console without having to re-authenticate. This will work until the value of the Persistent Cookie Max Time attribute specified in the Core Service elapses. For example:

```
http://server_name.domain_name:port/amserver/UI/Login?org=example&iPSPCookie=yes
```

IDTokenN Parameters

This parameter option to enables a user to pass authentication credentials using a URL or HTML forms. With the `IDTokenN=`*value* parameters, a user can be authenticated without accessing the Authentication Service User Interface. This process is called *Zero Page Login*. Zero page login works only for authentication modules that use one login page. The values of `IDToken0, IDToken1, ..., IDTokenN` map to the fields on the authentication module's login page. For example, the LDAP authentication module might use `IDToken1` for the `userID` information, and `IDToken2` for password information. In this case, the LDAP module IDTokenN URL would be:

```
http://server_name.domain_name:port/amserver/UI/
Login?module=LDAP&IDToken1=userID&IDToken2=password
```

(`module=LDAP` can be omitted if LDAP is the default authentication module.)

For Anonymous authentication, the login URL parameter would be:

```
http://server_name.domain_name:port/amserver/UI/Login?module=Anonymous&IDToken1=anonymousUserID.
```

Note – The token names `Login.Token0, Login.Token1, ..., Login.TokenN` (from previous releases) are still supported but will be deprecated in a future release. It is recommended to use the new `IDTokenN` parameters.

Account Locking

The Authentication Service provides a feature where a user will be *locked out* from authenticating after *n* failures. This feature is turned off by default, but can be enabled using the Access Manager console.

Note – Only modules that throw an Invalid Password Exception can leverage the Account Locking feature.

The Core Authentication service contains attributes for enabling and customizing this feature including (but not limited to):

- **Login Failure Lockout Mode** which enables account locking.
- **Login Failure Lockout Count** which defines the number of tries that a user may attempt to authenticate before being locked out. This count is valid per user ID only; the same user ID needs to fail for the given count after which that user ID would be locked out.
- **Login Failure Lockout Interval** defines (in minutes) the amount of time in which the Login Failure Lockout Count value must be completed before a user is locked out.
- **Email Address to Send Lockout Notification** specifies an email address to which user lockout notifications will be sent.

- **Warn User After N Failure** specifies the number of authentication failures that can occur before a warning message will be displayed to the user. This allows an administrator to set additional login attempts after the user is warned about an impending lockout.
- **Login Failure Lockout Duration** defines (in minutes) how long the user will have to wait before attempting to authenticate again after lockout.
- **Lockout Attribute Name** defines which LDAP attribute in the user's profile will be set to `inactive` for Physical Locking.
- **Lockout Attribute Value** defines to what the LDAP attribute specified in **Lockout Attribute Name** will be set: `inactive` or `active`.

Email notifications are sent to administrators regarding any account lockouts. (Account locking activities are also logged.)

Note – For special instructions when using this feature on a Microsoft® Windows 2000 operating system, see "Simple Mail Transfer Protocol (SMTP)" in Appendix A, "AMConfig.properties File."

Access Manager supports two types of account locking are supported: Physical Locking and Memory Locking, defined in the following sections.

Physical Locking

This is the default locking behavior for Access Manager The locking is initiated by changing the status of a LDAP attribute in the user's profile to inactive. The `Lockout Attribute Name` attribute defines the LDAP attribute used for locking purposes.

Note – An aliased user is one that is mapped to an existing LDAP user profile by configuring the User Alias List Attribute (`iplanet-am-user-alias-list in amUser.xml`) in the LDAP profile. Aliased users can be verified by adding `iplanet-am-user-alias-list` to the Alias Search Attribute Name field in the Core Authentication Service. That said, if an aliased user is locked out, the actual LDAP profile to which the user is aliased will be locked. This pertains only to physical lockout with authentication modules other than LDAP and Membership.

Memory Locking

Memory locking is enabled by changing the `Login Failure Lockout Duration` attribute to a value greater then 0. The user's account is then locked in memory for the number of minutes specified. The account will be unlocked after the time period has passed. Following are some special considerations when using the memory locking feature:

- If Access Manager is restarted, all accounts locked in memory are unlocked.
- If a user's account is locked in memory and the administrator changes the account locking mechanism to physical locking (by setting the lockout duration back to 0), the user's account will be unlocked in memory and the lock count reset.
- After memory lockout, when using authentication modules other than LDAP and Membership, if the user attempts to login with the correct password, a *User does not have profile in this realm error.* is returned rather than a *User is not active.* error.

Note – If the Failure URL attribute is set in the user's profile, neither the lockout warning message nor the message indicating that their account has been locked will not be displayed; the user will be redirected to the defined URL.

Authentication Service Failover

Authentication service failover automatically redirects an authentication request to a secondary server if the primary server fails because of a hardware or software problem or if the server is temporarily shut down.

An authentication context must first be created on an instance of Access Manager where the authentication service is available. If this instance of Access Manager is not available, an authentication context can then be created on a different instance of Access Manager through the authentication failover mechanism. The authentication context will check for server availability in the following order:

1. The authentication service URL is passed to the AuthContext API. For example:

   ```
   AuthContext(orgName, url)
   ```

   If this API is used, it will only use the server referenced by the URL. No failover will occur even if the authentication service is available on that server.
2. The authentication context will check the server defined in the `com.iplanet.am.server*` attribute of the `AMConfig.properties` file.
3. If step 2 fails, then the authentication context queries the platform list from a server where the Naming service is available This platform list is automatically created when multiple instances of Access Manager are installed (generally, for failover purposes) sharing a one instance of Directory Server.

   For example, if the platform list contains URLs for `Server1`, `Server2` and `Server3`, then the authentication context will loop through `Server1` , `Server2` and `Server3` until authentication succeeds on one of them.

The platform list may not always be obtained from the same server, as it depends on the availability of the Naming service. Furthermore, Naming service failover may occur first. Multiple Naming service URLs are specified in the `com.iplanet.am.naming.url property` (in `AMConfing.properties`). The first available Naming service URL will be used to identify the server, which will contain the list of servers (in its platform server list) on which authentication failover will occur.

Fully Qualified Domain Name Mapping

Fully Qualified Domain Name (FQDN) mapping enables the Authentication Service to take corrective action in the case where a user may have typed in an incorrect URL (such as specifying a partial host name or IP address to access protected resources). FQDN mapping is enabled by modifying the `com.sun.identity.server.fqdnMap` attribute in the `AMConfig.properties` file. The format for specifying this property is:

`com.sun.identity.server.fqdnMap[`*invalid-name* `]=`*valid-name*

The value *invalid-name* would be a possible invalid FQDN host name that may be typed by the user, and *valid-name* would be the actual host name to which the filter will redirect the user. Any number of mappings can be specified (as illustrated in Code Example 1-1) as long as they conform to the stated requirements. If this property is not set, the user would be sent to the default server name configured in the `com.iplanet.am.server.host=` *server_name* property also found in the `AMConfig.properties` file.

EXAMPLE 7–1 FQDN Mapping Attribute In `AMConfig.properties`

```
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
```

Possible Uses For FQDN Mapping

This property can be used for creating a mapping for more than one host name which may be the case if applications hosted on a server are accessible by more than one host name. This property can also be used to configure Access Manager to not take corrective action for certain URLs. For example, if no redirect is required for users who access applications by using an IP address, this feature can be implemented by specifying a map entry such as:

`com.sun.identity.server.fqdnMap[`*IP address* `]=`*IP address.*

Note – If more than one mapping is defined, ensure that there are no overlapping values in the invalid FQDN name. Failing to do so may result in the application becoming inaccessible.

Persistent Cookie

A persistent cookie is one that continues to exist after the web browser is closed, allowing a user to login with a new browser session without having to re-authenticate. The name of the cookie is defined by the `com.iplanet.am.pcookie.name` property in `AMConfig.properties`; the default value is `DProPCookie`. The cookie value is a 3DES-encrypted string containing the userDN, realm name, authentication module name, maximum session time, idle time, and cache time.

▼ To Enable Persistent Cookies

1. **Turn on the `Persistent Cookie Mode` in the Core Authentication module.**

2. **Configure a time value for the `Persistent Cookie Maximum Time` attribute in the Core Authentication module.**

3. **Append the iPSPCookie Parameter with a value of `yes` to the User Interface Login URL.**

   Once the user authenticates using this URL, if the browser is closed, they can open a new browser window and will be redirected to the console without re-authenticating. This will work until the time defined in Step 2 elapses.

   Persistent Cookie Mode can be turned on using the Authentication SPI method:

   `AMLoginModule.setPersistentCookieOn()`.

Multi-LDAP Authentication Module Configuration In Legacy Mode

As a form of failover or to configure multiple values for an attribute when the Access Manager console only provides one value field, an administrator can define multiple LDAP authentication module configurations under one realm. Although these additional configurations are not visible from the console, they work in conjunction with the primary configuration if an initial search for the requesting user's authorization is not found. For example, one realm can define a search through LDAP servers for authentication in two different domains or it can configure multiple user naming attributes in one domain. For the latter, which has only one text field in the console, if a user is not found using the primary search criteria, the LDAP module will then search using the second scope. Following are the steps to configure additional LDAP configurations.

▼ To Add An Additional LDAP Configuration

1 **Write an XML file including the complete set of attributes and new values needed for second (or third) LDAP authentication configuration.**

The available attributes can be referenced by viewing the `amAuthLDAP.xml` located in `etc/opt/SUNWam/config/xml`. This XML file created in this step though, unlike the `amAuthLDAP.xml`, is based on the structure of the `amadmin.dtd`. Any or all attributes can be defined for this file. Code Example 1-2 is an example of a sub-configuration file that includes values for all attributes available to the LDAP authentication configuration.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
  Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.
  Use is subject to license terms.
-->
<!DOCTYPE Requests
    PUBLIC "-//iPlanet//Sun ONE Access Manager 6.0 Admin CLI DTD//EN"
    "jar://com/iplanet/am/admin/cli/amAdmin.dtd"
>
<!--
  Before adding subConfiguration load the schema with
GlobalConfiguration defined and replace corresponding
 serviceName and subConfigID in this sample file OR load
 serviceConfigurationRequests.xml before loading this sample
-->
<Requests>
<realmRequests DN="dc=iplanet,dc=com">
    <AddSubConfiguration subConfigName = "ssc"
        subConfigId = "serverconfig"
        priority = "0" serviceName="iPlanetAMAuthLDAPService">

              <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-server"/>
            <Value>vbrao.red.iplanet.com:389</Value>
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-base-dn"/>
            <Value>dc=iplanet,dc=com</Value>
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="planet-am-auth-ldap-bind-dn"/>
```

```
                <Value>cn=amldapuser,ou=DSAME Users,dc=iplanet,dc=com</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-bind-passwd"/>
                <Value>
                      plain text password</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-user-naming-attribute"/>
                <Value>uid</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-user-search-attributes"/>
                <Value>uid</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-search-scope"/>
                <Value>SUBTREE</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-ssl-enabled"/>
                <Value>false</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-return-user-dn"/>
                <Value>true</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-auth-level"/>
                <Value>0</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-server-check"/>
                <Value>15</Value>
            </AttributeValuePair>

        </AddSubConfiguration>

    </realmRequests>
    </Requests>
```

2 Copy the plain text password as the value for the iplanet-am-auth-ldap-bind-passwd in the XML file created in Step 1.

The value of this attribute is formatted in bold in the code example.

3 **Load the XML file using the `amadmin` command line tool.**

```
./amadmin -u amadmin -w administrator_password -v -t name_of_XML_file.
```

Note that this second LDAP configuration can not be seen or modified using the console.

Tip – There is a sample available for multi-LDAP configuration. See the `serviceAddMultipleLDAPConfigurationRequests .xml` command line template in `/AccessManager-base /SUNWam/samples/admin/cli/bulk-ops/`. Instructions can be found in `Readme.html` at `/AccesManager-base /SUNWam/samples/admin/cli/`.

Session Upgrade

The Authentication service enables you to upgrade a valid session token based on a second, successful authentication performed by the same user to one realm. If a user with a valid session token attempts to authenticate to a resource secured by his current realm and this second authentication request is successful, the session is updated with the new properties based on the new authentication. If the authentication fails, the user's current session is returned without an upgrade. If the user with a valid session attempts to authenticate to a resource secured by a different realm, the user will receive a message asking whether they would like to authenticate to the new realm. The user can, at this point, maintain the current session or attempt to authenticate to the new realm. Successful authentication will result in the old session being destroyed and a new one being created.

During session upgrade, if a login page times out, redirection to the original success URL will occur. Timeout values are determined based on:

- The page timeout value set for each module (default is 1 minute)
- `com.iplanet.am.invalidMaxSessionTime` property in `AMConfig.properties` (default is 10 minutes)
- `iplanet-am-max-session-time` (default is 120 minutes)

The values of `com.iplanet.am.invalidMaxSessionTimeout` and `iplanet-am-max-session-time` should be greater than the page timeout value, or the valid session information during session upgrade will be lost and URL redirection to the previous successful URL will fail.

Validation Plug-in Interface

An administrator can write username or password validation logic suitable to their realm, and plug this into the Authentication Service. (This functionality is supported only by the LDAP and Membership authentication modules.) Before authenticating the user or changing the password, Access Manager will invoke this plug-in. If the validation is successful, authentication continues; if it fails, an authentication failed page will be thrown. The plug-in extends the `com.iplanet.am.sdk.AMUserPasswordValidation` class which is part of the Service Management SDK. Information on this SDK can be found in the `com.iplanet.am.sdk` package in the Access Manager Javadocs.

▼ To Write and Configure a Validation Plug-in

1. **The new plug-in class will extend the** `com.iplanet.am.sdk. AMUserPasswordValidation` **class and implement the** `validateUserID()` **and** `validatePassword()` **methods.** `AMException` **should be thrown if validation fails.**

2. **Compile the plug-in class and place the** `.class` **file in the desired location. Update the classpath so that it is accessible by the Access Manager during runtime.**

3. **Login to the Access Manager console as top-level administrator. Click on the Service Management tab, and get to the attributes for the Administration Service. Type the name of the plug-in class (including the package name) in the** `UserID & Password Validation Plugin Class` **field.**

4. **Logout and login.**

JAAS Shared State

The JAAS shared state provides sharing of both user ID and password between authentication modules. Options are defined for each authentication module for:

- Realm (or, Oraganization)
- User
- Service
- Role

Upon failure, the module prompts for its required credentials. After failed authentication, the module stops running, or the logout shared state clears.

Enabling JAAS Shared State

To configure the JAAS shared state:

- Use the `iplanet-am-auth-shared-state-enabled` option.
- The usage for the shared state option is:`iplanet-am-auth-shared-state-enabled=true`
- The default for this option is true.
- This variable is specified in the Options column of the authentication chaining configuration.

Upon failure, the authentication module will prompt for the required credentials as per the `tryFirstPass` option behavior suggested in the JAAS specification.

JAAS Shared State Store Option

To configure the JAAS shared state store option:

- Use the `iplanet-amauth-store-shared-state-enabled` option.
- The usage for the store shared state option is:`iplanet-am-auth-store-shared-state-enabled=true`
- The default for this option is false.
- This variable is specified in the Options column of the authentication chaining configuration.

After a commit, an abort or a logout, the shared state will be cleared.

CHAPTER 8

Managing Policies

This chapter describes the Policy Management feature of Sun Java™ System Access Manager. Access Manager's Policy Management feature enables the top-level administrator or top-level policy administrator to view, create, delete and modify policies for a specific service that can be used across all realms. It also provides a way for a realm or sub realm administrator or policy administrator to view, create, delete and modify policies at the realm level.

This chapter contains the following sections:

- "Overview" on page 131
- "Policy Management Feature" on page 132
- "Policy Types" on page 134
- "Policy Definition Type Document" on page 139
- "Creating Policies" on page 144
- "Managing Policies" on page 147
- "Policy Configuration Service" on page 153
- "Resource—Based Authentication" on page 154

Overview

A *policy* defines rules that specify access privileges to an organization's protected resources. Businesses posses resources, applications and services that they need to protect, manage and monitor. Policies control the access permissions and usage of these resources by defining when and how a user can perform an action on a given resource. A policy defines the resources for a particular principal.

Note – A *principal* can be an individual, a corporation, a role, or a group; anything that can have an identity. for more information, see the Java™ 2 Platform Standard Edition Javadoc (`http://java.sun.com/j2se/1.4.2/docs/api/java/security/Principal.html`).

A single policy can define either binary or non-binary decisions. A binary decision is *yes/no*, *true/ false* or *allow/deny*. A non-binary decision represents the value of an attribute. For example, a mail service might include a `mailboxQuota` attribute with a maximum storage value set for each user. In general, a policy is configured to define what a principal can do to which resource and under what conditions.

Policy Management Feature

The Policy Management feature provides a *policy service* for creating and managing policies. The policy service allows administrators to define, modify, grant, revoke and delete permissions to protect resources within the Access Manager deployment. Typically, a policy service includes a data store, a library of interfaces that allows for the creation, administration and evaluation of policies, and a policy enforcer or *policy agent*. By default, Access Manager uses Sun Java Enterprise System Directory Server for data storage, and provides Java and C APIs for policy evaluation and policy service customization (see the *Sun Java System Access Manager 7 2005Q4 Developer's Guide* for more information). It also allows administrator to use the Access Manager console for policy management. Access Manager provides one policy—enabled service, the URL Policy Agent service, which uses down-loadable policy agents to enforce the policies.

URL Policy Agent Service

Upon installation, Access Manager provides the URL Policy Agent service to define policies to protect HTTP URLs. This service allows administrators to create and manage policies through a policy enforcer or *policy agent.*

Policy Agents

The Policy Agent is the Policy Enforcement Point (PEP) for a server on which an enterprise's resources are stored. The policy agent is installed separately from Access Manager onto a web server and serves as an additional authorization step when a user sends a request for a web resource that exists on the protected web server. This authorization is in addition to any user authorization request which the resource performs. The agent protects the web server, and in turn, the resource is protected by the authorization plug-in.

For example, a Human Resources web server protected by a remotely-installed Access Manager might have an agent installed on it. This agent would prevent personnel without the proper policy from viewing confidential salary information or other sensitive data. The policies are defined by the Access Manager administrator, stored within the Access Manager deployment and used by the policy agent to allow or deny users access to the remote web server's content.

The most current Access Manager Policy Agents can be downloaded from the Sun Microsystems Download Center.

More information on installing and administrating the policy agents can be found in the *Sun Java System Access Manager Policy Agent 2.2 User's Guide*.

Note – Policy is evaluated in no particular order although as they are evaluated, if one action value evaluates to *deny*, subsequent policies are not evaluated, unless the Continue Evaluation On Deny Decision attribute is enabled in the Policy Configuration service.

Access Manager Policy agents enforce decisions only on web URLs (`http://...`, or `https//...`). However, agents can be written using the Java and C Policy Evaluation APIs to enforce policy on other resources.

In addition, the Resource Comparator attribute in the Policy Configuration Service would also need to be changed from its default configuration to:

```
serviceType=Name_of_LDAPService
|class=com.sun.identity.policy.plugins.SuffixResourceName|wildcard=*

|delimiter=,|caseSensitive=false
```

Alternately, providing an implementation such as `LDAPResourceName` to implement `com.sun.identity.policy.interfaces.ResourceName` and configuring the Resource Comparator appropriately would also work.

The Policy Agent Process

The process for protected web resources begins when a web browser requests a URL that resides on a server protected by the policy agent. The server's installed policy agent intercepts the request and checks for existing authentication credentials (a session token).

If the agent has intercepted a request and validated the existing session token, the following process is followed.

1. If the session token is valid, the user is allowed or denied access. If the token is invalid, the user is redirected to the Authentication Service, as outlined in the following steps.

   Assuming the agent has intercepted a request for which there is no existing session token, the agent redirects the user to the login page even if the resource is protected using a different authentication method.
2. Once the user's credentials are properly authenticated, the agent issues a request to the Naming Service which defines the URLs used to connect to Access Manager's internal services.
3. If the resource matches the non-enforced list, configured at the agent, access is allowed.
4. The Naming Service returns locators for the policy service, session service and logging service.
5. The agent sends a request to the Policy Service to get policy decisions applicable to the user.

6. Based on the policy decisions for the resource being accessed, the user is either allowed or denied access. If advice on the policy decision indicates a different authentication level or authentication mechanism, the agent redirects the request to the Authentication Service until all criteria is validated.

Policy Types

There are two types of policies that can be configured using Access Manager:

- "Normal Policy" on page 134
- "Referral Policy" on page 139

Normal Policy

In Access Manager, a policy that defines access permissions is referred to as a *normal* policy. A normal policy consists of *rules* , *subjects*, *conditions*, and *response providers*.

Rules

A *rule* contains a resource, one or more actions, and a value. Each action can have one or more values.

- A *resource* defines the specific object that is being protected; for instance, an HTML page or a user's salary information accessed using a human resources service.
- An *action* is the name of an operation that can be performed on the resource; examples of web server actions are POST or GET. An allowable action for a human resources service , for example, can change a home telephone number.
- A *value* defines the permission for the action, for example, allow or deny.

Note – It is acceptable to define an action without resources for some services.

Subjects

A *subject* defines the user or collection of users (for instance, a group or those who possess a specific role) that the policy affects. Subjects are assigned to policies. The general rule for subjects is that the policy would apply only if the user is a member of at least one subject in the policy. The default subjects are:

AM Identity Subject
The identities you create and manage under the Realms Subject tab can be added as values of the subject.

Access Manager Roles
Any LDAP role can be added as a value of this subject. An LDAP Role is any role definition that uses the Directory Server role

capability. These roles have object classes mandated by Directory Server role definition. The LDAP Role Search filter can be modified in the Policy Configuration Service to narrow the scope and improve performance.

Authenticated Users

Any user with a valid SSOToken is a member of this subject. All authenticated users would be member of this Subject, even if they have authenticated to an organization that is different from the organization in which the policy is defined. This is useful if the resource owner would like to give access to resources that is managed for users from other organizations.

LDAP Groups

Any member of an LDAP group can be added as a value of this subject.

LDAP Roles

Any LDAP role can be added as a value of this subject. An LDAP Role is any role definition that uses the Directory Server role capability. These roles have object classes mandated by Directory Server role definition. The LDAP Role Search filter can be modified in the Policy Configuration Service to narrow the scope and improve performance.

LDAP Users

Any LDAP user can be added as a value of this subject.

Organization

Any member of an organization is a member of this subject

Web Services Clients

Valid values are the DNs of trusted certificates in the local JKS keystore, which correspond to the certificates of trusted WSCs. This subject has dependency on the Liberty Web Services Framework and should be used only by Liberty Service Providers to authorize WSCs. A web service client (WSC) identified by the SSOToken is a member of this subject, if the DN of any principal contained in the SSOToken matches any selected value of this subject.

Make sure that you have created the keystore before you add this Subject to a policy. Information on setting up the keystore can be found in the following location:

AccessManager-base
`/SUNWam/samples/saml/xmlsig/keytool.html`

Access Manager Roles Versus LDAP Roles

An Access Manager role is created using Access Manager These roles have object classes mandated by Access Manager. An LDAP role is any role definition that uses the Directory Server role capability. These roles have object classes mandated by Directory Server role definition. All Access Manager roles can be used as Directory Server roles. However, all

Directory Server roles are not necessarily Access Manager roles. LDAP roles can be leveraged from an existing directory by configuring the "Policy Configuration Service" on page 153. Access Manager roles can only be accessed through the hosting Access Manager Policy Service. The LDAP Role Search filter can be modified in the Policy Configuration Service to narrow the scope and improve performance.

Nested Roles

Nested roles can be evaluated correctly as LDAP Roles in the subject of a policy definition.

Conditions

A condition allows you to define constraints on the policy. For example, if you are defining policy for a paycheck application, you can define a condition on this action limiting access to the application only during specific hours. Or, you may wish to define a condition that only grants this action if the request originates from a given set of IP addresses or from a company intranet.

The condition might additionally be used to configure different policies on different URIs on the same domain. For example, `http://org.example.com/hr/*jsp` can only be accessed by `org.example.net` from 9 a.m. to 5 p.m., yet `http://org.example.com/finance/*.jsp` can be accessed by `org.example2.net` from 5 a.m. to 11 p.m. This can be achieved by using an IP Condition along with a Time Condition. And specifying the rule resource as `http://org.example.com/hr/*.jsp`, the policy would apply to all the JSPs under `http://org.example.com/hr` including those in the sub directories.

Note – The terms referral, rule, resource, subject, condition, action and value correspond to the elements *Referral*, *Rule*, *ResourceName*, *Subject*, *Condition* , *Attribute* and *Value* in the `policy.dtd`.

The default conditions you can add are:

Authentication Level

The policy applies if the user's authentication level is greater than or equal to the Authentication level set in the condition.

This attribute indicates the level of trust for authentication.

The authentication level condition can be used to specify levels other than those from the registered authentication module levels for that realm. This is useful when a policy applies to user authenticated from another realm.

For LE Authentication, the policy applies if the user's authentication level is less than or equal to the Authentication level set in the condition. The authentication level condition can be used to specify levels other than those from the registered authentication module levels for that realm. This is useful when a policy applies to user authenticated from another realm.

Authentication Scheme

Choose the authentication scheme(s) for the condition from the pull-down menu. These authentication schemes are the authentication modules defined in the Core authentication service at the realm.

IP Address

Sets the condition based on a range of IP Addresses. The fields you can define are:

- IP Address From/To — Specifies the range of the IP address.
- DNS Name — Specifies the DNS name. This field can be a fully qualified hostname or a string in one of the following formats:

  domainname

  **.domainname*

Session

Sets the condition based on user session data. The fields you can modify are:

- Max Session Time — Specifies the maximum duration to which the policy is applicable starting from when the session was initiated.
- Terminate Session — If selected, the user session will be terminated if the session time exceeds the maximum allowed as defined in the Max Session Time field.

  You can use this condition to protect sensitive resources so that the resources are available only for a limited time after authentication.

Session Property

Decides whether a policy is applicable to the request based on values of properties set in the user's Access Manager session. During policy evaluation, the condition returns true only if the user's session has every property value defined in the condition. For properties defined with multiple values in the condition, it is sufficient if the token has at least one value listed for the property in the condition. For example, you can use this condition to apply policies based on attributes in external repositories. A post-authentication plug-in can set up the session properties based on the external attributes.

Time

Sets the condition based on time constraints. The fields are:

- Date From/To — Specifies the range of the date.
- Time — Specifies the range of time within a day.
- Day — Specifies a range of days.
- Timezone — Specifies a timezone, either standard or custom. Custom timezones can only be a timezone ID recognized by Java (for example, PST). If no value is specified, the default value is the Timezone set in the Access Manager JVM.

Response Providers

Response providers are plug-ins that provide policy-based response attributes. The response provider attributes are sent with policy decisions to the PEP. Access Manager includes one implementation, the `IDResponseProvider.` Custom response providers are not supported in this version of Access Manager. Agents, PEPs, typically pass these response attributes as headers to applications. Applications typically use these attributes to personalize application pages such as a portal page.

Policy Advices

If a policy is not applicable as determined by the condition, the condition can produce advice messages that indicates why the policy was not applicable to the request. These advice messages are propagated in the policy decision to the Policy Enforcement Point. The Policy Enforcement Point can retrieve this advice and try to take the appropriate action, such as redirecting the user back to the authentication mechanism to authenticate to a higher level. The user may then be prompted for higher level authentication and may be able to access to the resource, if the policy becomes applicable, after proper action for the advice is taken.

More information can be found in the following class:

```
com.sun.identity.policy.ConditionDecision.getAdvices()
```

Only `AuthLevelCondiiton` and `AuthSchemeCondition` provide advices if the condition is not satisfied.

`AuthLevelCondition` advice is associated with the following key:

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_LEVEL_CONDITION_ADVICE
```

`AuthSchemeCondition` advice is associated with the following key:

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_SCHEME_CONDITION_ADVICE
```

Custom conditions can also produce advices. However, the Access Manager Policy Agents respond only for Auth Level Advice and Auth Scheme Advice. Custom agents could be written to understand and respond to more advices and existing Access Manager agents can be extended to understand and respond to more advices. For more information, see the *Sun Java System Access Manager Policy Agent 2.2 User's Guide*.

Referral Policy

An administrator may need to delegate one realm's policy definitions and decisions to another realm. (Alternatively, policy decisions for a resource can be delegated to other policy products.) A *referral* policy controls this policy delegation for both policy creation and evaluation. It consists of one or more *rules* and one or more *referrals*.

Rules

A rule defines the resource whose policy definition and evaluation is being referred.

Referrals

The referral defines the organization to which the policy evaluation is being referred. By default, there are two types of referrals: peer realm and sub realm. They delegate to an realm on the same level and an realm on a sub level, respectively. See "Creating Policies for Peer Realms and Sub Realms" on page 146 for more information.

Note – The realm that is referred to can define or evaluate policies only for those resources (or sub-resources) that have been referred to it. This restriction, however, does not apply to the top-level realm.

Policy Definition Type Document

Once a policy is created and configured, it is stored in Directory Server in XML. In Directory Server, the XML-encoded data is stored in one place. Although policy is defined and configured using the `amAdmin.dtd` (or the console), it is actually stored in Directory Server as XML that is based on the `policy.dtd` . The `policy.dtd` contains the policy element tags extracted from the `amAdmin.dtd` (without the policy creation tags). So, when the Policy Service loads policies from Directory Server, it parses the XML based on the `policy.dtd`. The `amAdmin.dtd` is only used when creating policy with the command line. This section describes the structure of `policy.dtd`. The `policy.dtd` exists in the following location:

```
AccessManager-base/SUNWam/dtd (Solairs)
AccessManager-base/identity/dtd (Linux)
```

Note – Throughout the rest of this chapter, only the Solaris directory information will be given. Please note that the directory structure for Linux is different.

Policy Element

Policy is the root element that defines the permissions or *rules* of a policy and to whom/what the rule applies or the *subject*. It also defines whether or not the policy is a *referral* (delegated) policy and whether there are any restrictions (or *conditions*) to the policy. It may contain one or more of the following sub-elements: *Rule*, *Conditions*, *Subjects*,*Referrals*, or *response providers*. The required XML attribute is `name` which specifies the name of the policy. The `referralPolicy` attribute identifies whether or not the policy is a referral policy; it defaults to a normal policy if not defined. Optional XML attributes include *name* and *description*.

Note – When tagging a policy as *referral*, subjects and conditions are ignored during policy evaluation. Conversely, when tagging a policy as *normal*, any Referrals are ignored during policy evaluation.

Rule Element

The *Rule* element defines the specifics of the policy and can take three sub-elements: *ServiceName*, *ResourceName* , or *AttributeValuePair*. It defines the type of service or application for which the policy has been created as well as the resource name and the actions which are performed on it. A rule can be defined without any actions; for example, a referral policy rule doesn't have any actions.

Note – It is acceptable to have a defined policy that does not include a defined *ResourceName* element.

ServiceName Element

The *ServiceName* element defines the name of the service to which the policy applies. This element represents the service type. It contains no other elements. The value is exactly as that defined in the service's XML file (based on the `sms.dtd)`. The XML service attribute for the *ServiceName* element is the name of the service (which takes a string value).

ResourceName Element

The *ResourceName* element defines the object that will be acted upon. The policy has been specifically configured to protect this object. It contains no other elements. The XML service attribute for the *ResourceName* element is the name of the object. Examples of a *ResourceName* might be `http://www.sunone.com:8080/images` on a web server or `ldap://sunone.com:389/dc=example,dc=com` on a directory server. A more specific resource might be `salary://uid=jsmith,ou=people,dc=example,dc=com` where the object being acted upon is the salary information of John Smith.

AttributeValuePair Element

The *AttributeValuePair* element defines an action and its values. It is used as a sub-element to "Subject Element" on page 142, "Referral Element" on page 142 and "Condition Element" on page 143. It contains both the *Attribute* and *Value* elements and no XML service attributes.

Attribute Element

The *Attribute* element defines the name of the action. An action is an operation or event that is performed on a resource. POST or GET are actions performed on web server resources, READ or SEARCH are actions performed on directory server resources. The *Attribute* element must be paired with a *Value* element. The *Attribute* element itself contains no other elements. The XML service attribute for the *Attribute* element is the name of the action.

Value Element

The *Value* element defines the action values. Allow/deny or yes/no are examples of action values. Other action values can be either boolean, numeric, or strings. The values are defined in the service's XML file (based on the `sms.dtd`). The *Value* element contains no other elements and it contains no XML service attributes.

Note – Deny rules always take precedence over allow rules. For example, if one policy denies access and another allows it, the result is a deny (provided all other conditions for both policies are met). It is recommended that deny policies be used with extreme caution as they can lead to potential conflicts. If explicit deny rules are used, policies assigned to a user through different subjects (such as role and/or group membership) may result in denied access. Typically, the policy definition process should only use allow rules. The default deny may be used when no other policies apply.

Subjects Element

The *Subjects* sub-element identifies a collection of principals to which the policy applies; this collection is chosen based on membership in a group, ownership of a role or individual users. It takes the *Subject* sub-element. The XML attributes that can be defined are:

name. This defines a name for the collection.

description. This defines a description of the subject

includeType. This is not currently used.

Subject Element

The *Subject* sub-element identifies a collection of principals to which the policy applies; this collection pinpoints more specific objects from the collection defined by the Subjects element. Membership can be based on roles, group membership or simply a listing of individual users. It contains a sub-element, the "AttributeValuePair Element" on page 141. The required XML attribute is `type`, which identifies a generic collection of objects from which the specifically defined subjects are taken. Other XML attributes include `name` which defines a name for the collection and `includeType` which defines whether the collection is as defined, or whether the policy applies to users who are NOT members of the subject.

Note – When multiple subjects are defined, at least one of the subjects should apply to the user for the policy to apply. When a subject is defined with `includeType` set to false, the user should not be a member of that subject for the policy to apply.

Referrals Element

The *Referrals* sub-element identifies a collection of policy referrals. It takes the *Referral* sub-element. The XML attributes it can be defined with are `name` which defines a name for the collection and `description` which takes a description.

Referral Element

The *Referral* sub-element identifies a specific policy referral. It takes as a sub-element the "AttributeValuePair Element" on page 141. It's required XML attribute is `type` which identifies a generic collection of assignments from which the specifically defined referrals are taken. It can also include the `name` attribute which defines a name for the collection.

Conditions Element

The *Conditions* sub-element identifies a collection of policy restrictions (time range, authentication level, and so forth). It must contain one or more of the *Condition* sub-element. The XML attributes it can be defined with are `name` which defines a name for the collection and `description` which takes a description.

Note – The conditions element is an optional element in a policy.

Condition Element

The *Condition* sub-element identifies a specific policy restriction (time range, authentication level, and sor forth). It takes as a sub-element the "AttributeValuePair Element" on page 141. Its required XML attribute is `type` which identifies a generic collection of restrictions from which the specifically defined conditions are taken. It can also include the `name` attribute which defines a name for the collection.

Adding a Policy Enabled Service

You can define policies for resources of a given service only if the service schema has the `<Policy>` element configures to `sms.dtd`.

By default, Access Manager provides the URL Policy Agent service (`iPlanetAMWebAgentService`). This service is defined in an XML file located in the following directory:

```
/etc/opt/SUNWam/config/xml/
```

You can, however add additional policy services to Access Manager. Once the policy service is created, you add it to Access Manager through the `amadmin` command line utility.

▼ To Add a New Policy Enabled Service

1 **Develop the new policy service in an XML file based on the `sms.dtd`. Access Manager provides two policy service XML files that you may wish to use as the basis for the new policy service file:**

`amWebAgent.xml` - This the XML file for the default URL Policy Agent service. It is located in `/etc/opt/SUNWam/config/xml/`.

`SampleWebService.xml`. - This is the sample policy service file located `inAccessManager-base/samples/policy`.

2 **Save the XML file to the directory from which you will load the new policy service. For example:**

```
/config/xml/newPolicyService.xml
```

3 **Load the new policy service with the `amadmin` command line utility. For example:**

```
AccessManager-base/SUNWam/bin/amadmin
    --runasdn “uid=amAdmin,ou=People,default_org,
root_suffix
    --password password
    --schema /config/xml/newPolicyService.xml
```

4 **After you load the new policy service, you can define rules for the policy definitions through the Access Manager console or by loading a new policy through `amadmin`.**

Creating Policies

You can create, modify and delete policies through the Policy API and the Access Manager console, and create and delete policies through the `amadmin` command line tool. You can also get and list policies in XML using the `amadmin` utility. This section focuses on creating policies through the `amadmin` command line utility and through the Access Manager console. For more information on the Policy APIs, see the *Sun Java System Access Manager 7 2005Q4 Developer's Guide*.

Policies are generally created using an XML file and added to Access Manager through the `amadmin` command line utility and then managed using the Access Manager console (although policies can be created using the console). This is because policies cannot be modified using `amadmin` directly. To modify a policy, you must first delete the policy from Access Manager and then add the modified policy using `amadmin`.

In general, policy is created at the realm (or sub realm) level to be used throughout the realm's tree.

▼ To Create Policies with amadmin

1 **Create the policy XML file based on the `amadmin.dtd`. This file is located in the following directory:**

AccessManager-base `/SUNWam/dtd`

2 **Once the policy XML file is developed, you can use the following command to load it:**

```
AccessManager-base/SUNWam/bin/amadmin
--runasdn "uid=amAdmin,ou=People,default_org,
root_suffix"
--password password
--data policy.xml
```

To add multiple policies simultaneously, place the policies in one XML file, as opposed to having one policy in each XML file. If you load policies with multiple XML files in quick succession, the internal policy index may become corrupted and some policies may not participate in policy evaluation.

When creating policies through `amadmin`, ensure that the authentication module is registered with the realm while creating authentication scheme condition; that the corresponding LDAP objects realms, groups, roles and users) exist while creating realms, LDAP groups, LDAP roles and LDAP user subjects; that Access Manager roles exist while creating `IdentityServerRoles` subjects; and that the relevant realms exist while creating sub realm or peer realm referrals.

Please note that in the text of Value elements in `SubrealmReferral`, `PeerRealmReferral`, `Realm` subject, `IdentityServerRoles` subject, `LDAPGroups` subject`,` `LDAPRoles` subject and `LDAPUsers` subject need to be the full DN.

▼ To Create a Normal Policy With the Access Manager Console

1. **Choose the realm for which you would like to create a policy.**

2. **Click the Policies tab.**

3. **Click New Policy from the Policies list.**

4. **Add a name and a description for the policy.**

5. **If you wish the policy to be active, select Yes in the Active attribute.**

6. **It is not necessary to define all of the fields for normal policies at this time. You may create the policy, then add rules, subjects, conditions, and response providers later. See "Managing Policies" on page 147 for more information.**

7. **Click Create.**

▼ To Create a Referral Policy With the Access Manager Console

1. **Choose the realm for which you would like to create the policy.**

2. **Click New Referral from the Policies tab.**

3 **Add a name and a description for the policy.**

4 **If you wish the policy to be active, select Yes in the Active attribute.**

5 **It is not necessary to define all of the fields for referral policies at this time. You may create the policy, then add rules and referrals later. See "Managing Policies" on page 147 for more information.**

6 **Click Create.**

Creating Policies for Peer Realms and Sub Realms

In order to create policies for peer or sub realms, you must first create a referral policy in the parent (or another peer) realm. The referral policy must contain, in its rule definition, the resource prefix that is being managed by the sub realm. Once the referral policy is created in the parent realm (or another peer realm) normal policies can be created at the sub realm (or peer realm).

In this example, `o=isp` is the parent realm and `o=example.com` is the sub realm that manages resources and sub-resources of `http://www.example.com`.

▼ To Create a Policy for a Sub Realm

1 **Create a referral policy at `o=isp`. For information on referral policies, see the procedure "Modifying a Referral Policy" on page 150.**

The referral policy must define `http://www.example.com` as the resource in the rule, and must contain a `SubRealmReferral` with `example.com` as the value in the referral.

2 **Navigate to the sub realm `example.com`.**

3 **Now that the resource is referred to `example.com` by `isp`, normal policies can be created for the resource `http://www.example.com`, or for any resource starting with `http://www.example.com.`**

To define policies for other resources managed by `example.com`, additional referral policies must be created at o= `isp`.

Managing Policies

Once a normal or referral policy is created and added to Access Manager, you can manage the policy through the Access Manager console by modifying the rules, subjects, conditions and referrals.

Modifying a Normal Policy

Through the Policies tab, you can modify a normal policy that defines access permissions. You can define and configure multiple rules, subjects, conditions and resource comparators. This section lists and describes the steps to do so.

To Add or Modify a Rule to a Normal Policy

1. **If you have already created the policy, click the name of the policy for which you wish to add the rule. If not, see “To Create a Normal Policy With the Access Manager Console” on page 145.**

2. **Under the Rules menu, click New.**

3. **Select one of the following default service types for the rule. You may see a larger list if more services are enabled for the policy:**

   Discovery Service — Defines the authorization actions for Discovery service query and modify protocol invocations by web services clients for a specified resource.

   Liberty Personal Profile Service — Defines the authorization actions for Liberty Personal Profile service query and modify protocol invocations by web services clients for a specified resource.

   URL Policy Agent — Provides the URL Policy Agent service for policy enforcement. This service allows administrators to create and manage policies through a policy enforcer or *policy agent.*

4. **Click Next.**

5. **Enter a name and resource name for the rule.**

   Currently, Policy Agents only support `http://` and `https://` resources and do not support IP addresses in place of the hostname.

   Wildcards are supported for host, port, and resource names. For example:

   ```
   http*://*:*/*.html
   ```

For the URL Policy Agent service, if a port number is not entered, the default port number is 80 for `http://`, and 443 for `https://`.

6. **Select the action for the rule. If you are using the URL Policy Agent service, you can select the following:**
   - GET
   - POST

7. **Select the Action Values.**
   - Allow — Enables you to access the resource matching the resource defined in the rule.
   - Deny — Denies access to the resource matching the resource defined in the rule.
   - Denial rules always take precedence over allow rules. For example, if you have two policies for a given resource, one denying access and the other allowing access, the result is a deny access (provided that the conditions for both policies are met). It is recommended that deny policies be used with extreme caution as they may lead to potential conflicts between the policies. The policy definition process should only use allow rules. If no policy is applicable to a resource, access is automatically denied.

     If explicit deny rules are used, policies that are assigned to a given user through different subjects (such as role and/or group membership) may result in denied access to a resource even if one or more of the policies allow access. For example, if there is a deny policy for a resource applicable to an Employee role and there is another allow policy for the same resource applicable to Manager role, policy decisions for users assigned both Employee and Manager roles would be denied.

     One way to resolve such problems is to design policies using Condition plug-ins. In the case above, a "role condition" that applies the deny policy to users authenticated to the Employee role and applies the allow policy to users authenticated to the Manager role helps differentiate the two policies. Another way could be to use the `authentication level` condition, where the Manager role authenticates at a higher authentication level.

8. **Click Finish.**

▼ To Add or Modify a Subject to a Normal Policy

1. **If you have already created the policy, click the name of the policy for which you wish to add the subject. If you have not yet created the policy, see "To Create a Normal Policy With the Access Manager Console" on page 145.**

2. **Under the Subject list, click New.**

3. **Select one of the default subject types. For descriptions of the subject types, see "Subjects" on page 134**

4 **Click Next.**

5 **Enter a name for the subject.**

6 **Select or deselect the Exclusive field.**

If this field is not selected (default), the policy applies to an identity that is a member of the subject. If the field is selected, the policy applies to an identity that is not a member of the subject.

If multiple subjects exist in the policy, the policy applies to the identity when the identity is a member of at least one subject.

7 **Perform a search in order to display the identities to add to the subject. This step is not applicable for the Authenticated Users subject or Web Services Client subjects.**

The default (*) search pattern will display all entries.

8 **Select the individual identities you wish to add for the subject, or click Add All to add all of the identities at once. Click Add to move the identities to the Selected list. This step is not applicable for the Authenticated Users subject.**

9 **Click Finish.**

10 **To remove a subject from a policy, select the subject and click Delete. You can edit any subject definition by clicking on the subject name.**

▼ To Add a Condition to a Normal Policy

1 **If you have already created the policy, click the name of the policy for which you wish to add the condition. If you have not yet created the policy, see “To Create a Normal Policy With the Access Manager Console” on page 145**

2 **Under the Conditions list, click New.**

3 **Select the condition type and click Next.**

4 **Define the fields for the condition type. For a description of the condition types, see “Conditions” on page 136.**

5 **Click Finish.**

▼ To Add a Response Provider to a Normal Policy

1. **If you have already created the policy, click the name of the policy for which you wish to add the response provider. If you have not yet created the policy, see "To Create a Normal Policy With the Access Manager Console" on page 145.**

2. **Under the Response Providers list, click New.**

3. **Enter a name for the response provider.**

4. **Define the following values:**

   StaticAttribute — The response attribute with name and values defined in the instance of `IDResponseProvider` and stored in the policy.

   DynamicAttribute — The response attributes chosen here need to first be defined in the Policy Configuration Service for the corresponding realm. The attribute names defined should be the same as those existing in the configured datastore. For details on how to define the attributes see the Policy Configuration attribute definitions in the Access Manager online help.

5. **Click Finish.**

6. **To remove response provider from a policy, select the subject and click Delete. You can edit any response provider definition by clicking on the name.**

Modifying a Referral Policy

You can delegate policy definitions and decisions of a realm to different realms using referral policies. Custom referrals can used to get policy decisions from any policy destination point. Once you have created a referral policy, you can add or modify associated the rules, referrals, and resource providers.

▼ To Add or Modify a Rule to a Referral Policy

1. **If you have already created the policy, click the name of the policy for which you wish to add the rule. If not, see "To Create a Referral Policy With the Access Manager Console" on page 145.**

2. **Under the Rules list, click New.**

3. **Select one of the following default service types for the rule. You may see a larger list if more services are enabled for the policy:**

Discovery Service	Defines the authorization actions for Discovery service query and modify protocol invocations by web services clients for a specified resource.
Liberty Personal Profile Service	Defines the authorization actions for Liberty Personal Profile service query and modify protocol invocations by web services clients for a specified resource.
URL Policy Agent	Provides the URL Policy Agent service for policy enforcement. This service allows administrators to create and manage policies through a policy enforcer or *policy agent*.

4 **Click Next.**

5 **Enter a name and resource name for the rule.**

Currently, Policy Agents only support `http://` and `https://` resources and do not support IP addresses in place of the hostname.

Wildcards are supported for resource names, port number, and protocol. For example:

```
http://*:*/*.html
```

For the URL Policy Agent service, if a port number is not entered, the default port number is 80 for `http://`, and 443 for `https://`.

To allow the management of resource for all servers installed on a specific machine, you can define the resource as `http://host*:*`. Additionally, you can define the following resource to grant an administrator to a specific organization authority for all of the services in that organization:

```
http://*.subdomain.domain.topleveldomain
```

6 **Click Finish.**

▼ To Add or Modify Referrals to a Policy

1 **If you have already created the policy, click the name of the policy for which you wish to add the response provider. If you have not yet created the policy, see "To Create a Referral Policy With the Access Manager Console" on page 145.**

2 **Under the Rules list, click New.**

3 **Select the Service type.**

4 **Define the resource in the Rules fields. The fields are:**

Referral— Displays the current referral type.

Name— Enter the name of the referral.

Resource Name— Enter the name of the resource.

Filter— Specifies a filter for the organization names that will be displayed in the Value field. By default, it will display all organization names.

Value — Select the organization name of the referral.

5 **Click Finish.**

To remove a referral from a policy, select the referral and click Delete.

You can edit any referral definition by clicking on the Edit link next to the referral name.

▼ To Add a Response Provider to a Referral Policy

1 **If you have already created the policy, click the name of the policy for which you wish to add the response provider. If you have not yet created the policy, see "To Create a Normal Policy With the Access Manager Console" on page 145.**

2 **Under the Response Providers list, click New.**

3 **Enter a name for the response provider.**

4 **Define the following values:**

StaticAttribute	The response attribute with name and values defined in the instance of `IDResponseProvider` and stored in the policy.
DynamicAttribute	The response attribute with only names selected in the instance of `IDResponseProvider` in the policy. The values are read from `IDRepostitories` based on the user identity request during policy evaluation.

5 **Click Finish.**

6 **To remove response provider from a policy, select the subject and click Delete. You can edit any response provider definition by clicking on the name.**

Policy Configuration Service

The Policy Configuration service is used to configure policy-related attributes for each organization through the Access Manager console. You can also define resource name implementations and Directory Server data stores for use with the Access Manager policy framework. The Directory Server specified in the Policy Configuration Service is used for membership evaluation of LDAP Users, LDAP Groups, LDAP Roles, and organization policy subjects.

Subjects Result Time To Live

To improve policy evaluation performance, membership evaluations are cached for a period of time as defined by the Subjects Result Time To Live attribute in the Policy Configuration service. These cached membership decisions are used until the time defined in the Subjects Result Time To Live attribute has elapsed. Membership evaluation after this is used to reflect the current state of users in the directory.

Dynamic Attributes

These are the allowed dynamic attribute names which are displayed in a list and chosen to define policy response provider dynamic attributes. The names that are defined need to be same as attribute names as defined in the data repository.

amldapuser Definition

`amldapuser` is a user created during installation used by default to the Directory Server specified in the Policy Configuration service. This can be changed, as necessary, by the administrator or policy administrator of the realm.

Adding Policy Configuration Services

When the realm is created, Policy Configuration service attributes are automatically set for the realm. You can, however, modify the attributes as needed.

Resource—Based Authentication

Some organizations require an advanced authentication scenario where a user authenticates against a particular module based on the resource that they are attempting to access. Resource-based authentication is a feature of Access Manager in which a user must authenticate to a specific authentication module protecting the resource, and not to the default authentication module. This feature is only applicable to first time user authentications.

Note – This is a separate feature than the resource-based authentication described in "Session Upgrade" on page 127. That particular feature does not have any limitations.

Limitations

Resource—based authentication contains the following limitations:

- If the policies applicable to the resource have multiple authentication modules, the system will arbitrarily pick one authentication module.
- Level and scheme are the only conditions that can be defined for this policy.
- This feature does not work across different DNS domains.

▼ To Configure Resource—based Authentication

Once both the Access Manager and a policy agent have been installed, resource—based authentication can be configured. To do this, it is necessary to point Access Manager to the Gateway servlet.

1. **Open** `AMAgent.properties`**.**

   `AMAgent.properties` can be found (in a Solaris environment) in `/etc/opt//SUNWam/agents/config/` .

2. **Comment out the following line:**

   ```
   #com.sun.am.policy.am.loginURL = http://Access
   Manager_server_host.domain_name:port/amserver/UI/Login.
   ```

3. **Add the following line to the file:**

   ```
   com.sun.am.policy.am.loginURL =
   http://AccessManager_host.domain_name:port/amserver/gateway
   ```

Note – The gateway servlet is developed using the Policy Evaluation APIs and can be used to write a custom mechanism to accomplish resource-based authentication. See the Chapter 6, “Using the Policy APIs,” in *Sun Java System Access Manager 7 2005Q4 Developer’s Guide* in the Access Manager Developer's Guide.

4 Restart the agent.

CHAPTER 9

Managing Subjects

The Subjects interface enables basic identity management within a realm. Any identity that you create in the Subjects interface can be used in the subject definition in the for a policy created with the Access Manager Identity Subject type.

The identities you can create and modify are:

- "User" on page 157
- "Agents" on page 159
- "Filtered Role" on page 162
- "Roles" on page 162
- "Groups" on page 163

User

A *user* represents an individual's identity. Users can be created and deleted in groups and can be added or removed from roles and/or groups. You can also assign services to the user.

To Create or Modify a User

1. **Click on the User tab.**

2. **Click New.**

3. **Enter data for the following fields:**

   UserId. This field takes the name of the user with which he or she will log into Access Manager. This property may be a non-DN value.

   First Name. This field takes the first name of the user.

   Last Name. This field takes the last name of the user.

Full Name — This field takes the full name of the user.

Password. — This field takes the password for the name specified in the User Id field.

Password (Confirm) — Confirm the password.

User Status. This option indicates whether the user is allowed to authenticate through Access Manager.

4 **Click Create.**

5 **Once the user is created, you can edit the user information by clicking the name of the user. For information on the user attributes, see the User attributes. Other modifications you can perform:**

- "To Create or Modify a User" on page 157
- "To Add a User to Roles and Groups" on page 158
- "To Add Services to an Identity" on page 158

▼ To Add a User to Roles and Groups

1 **Click the name of the user you wish to modify.**

2 **Select Roles or Groups. Only the roles and groups that have already been assigned to the user are displayed.**

3 **Select the roles or groups from the Available list and click Add.**

4 **Once the roles or groups are displayed in the Selected list, click Save.**

▼ To Add Services to an Identity

1 **Select the identity to which you wish to add services.**

2 **Click on the Services tab.**

3 **Click Add.**

4 **Depending on the identity type you selected, the following list of services are displayed:**

- Authentication Configuration
- Discovery Service
- Liberty Personal Profile Service
- Session

- User

5 Select the service you with to add and click Next.

6 Edit the attributes for the service. For a description of the services, click on the service name in Step 4.

7 Click Finish.

Agents

Access Manager Policy Agents protect content on web servers and web proxy servers from unauthorized intrusions. They control access to services and web resources based on the policies configured by an administrator.

The *agent* object defines a Policy Agent profile, and allows Access Manager to store authentication and other profile information about a specific agent that is protecting an Access Manager resource. Through the Access Manager console, administrators can view, create, modify and delete agent profiles.

the agent object creation page is the location where you can define the UID/password with which the the agent authenticated to Access Manager. If you have a multiple AM/WS setup using the same Access Manager, this gives you the option of enabling multiple IDs for different agents and to enable and disable them independently from Access Manager. You can also manage some preference values for the agents centrally, rather than editing the `AMAgent.properties` on each machine.

▼ To Create or Modify an Agent

1 Click the Agents tab.

2 Click New.

3 Enter the values for the following fields:

Name. Enter the name or identity of the agent. This is the name that the agent will use to log into Access Manager. Multi-byte names are not accepted.

Password. Enter the agent password. This password must be different than the password used by the agent during LDAP authentication.

Confirm Password. Confirm the password.

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

4 **Click Create.**

5 **Once you have crated the agent, you can additionally edit the following fields:**

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

Agent Key Value. Set the agent properties with a key/value pair. This property is used by Access Manager to receive agent requests for credential assertions about users. Currently, only one property is valid and all other properties will be ignored. Use the following format:

agentRootURL`=http://` *server_name:port*`/`

Creating a Unique Policy Agent Identity

By default, when you create multiple policy agents in a trusted environment, the policy agents contain the same UID and password. Because the UID and passwords are shared, Access Manager cannot distinguish between the agents, which may leave the session cookie open to interception.

The weakness may be present when an Identity Provider provides authentication, authorization and profile information about a user to application(s) (or Service Providers) that are developed by third parties or by unauthorized groups within the enterprise. Possible security issues are:

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

▼ To Create a Unique Policy Agent Identity

1 **Use the Access Manager administration console to make an entry for each agent.**

2 **Run the following command on the password that was entered during the creation of the agent. This command should be invoked on the host where the agent is installed.**

```
AccessManager-base/SUNWam/agents/bin/crypt_util agent123
```

This will give the following output:

```
WnmKUCg/y3l404ivWY6HPQ==
```

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

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

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

# Cross-Domain Single Sign On URL
# Is CDSSO enabled.
com.sun.am.policy.agents.cdsso-enabled=true

# This is the URL the user will be redirected to after successful login
# in a CDSSO Scenario.
com.sun.am.policy.agents.cdcservletURL = http://server.example.com:port
/amserver/cdcservlet
```

4 Change `AMConfig.properties` **where Access Manager is installed to reflect the new values, and then and restart Access Manager. Example:**

```
com.sun.identity.enableUniqueSSOTokenCookie=true
com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer

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

5 In the Access Manager console, choose Configuration>Platform.

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

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

b. Enter the host name of the Access Manager installation, and then click Add.

Example: `server.example.com`

You should see two cookies set on the browser:

- iPlanetDirectoryPro – server.example.com (hostname)
- sunIdentityServerAuthNServer – example.com (hostname)

Filtered Role

A filtered role is a dynamic role created through the use of an LDAP filter. All users are funneled through the filter and assigned to the role at the time of the role's creation. The filter looks for any attribute value pair (for example, `ca=user*`) in an entry and automatically assign the users that contain the attribute to the role.

▼ To Create a Filtered Role

1. **In the Navigation pane, go the organization where the role will be created.**
2. **Click New.**
3. **Enter a name for the filtered role.**
4. **Enter the information for the search criteria.**

   For example,

   ```
   (&(uid=user1)(|(inetuserstatus=active)(!(inetuserstatus=*))))
   ```

   If the filter is left blank, by default, the following role is created:

   ```
   (objectclass = inetorgperson)
   ```

5. **Click Create to initiate the search based on the filter criteria. The identities defined by the filter criteria are automatically assigned to the role.**
6. **Once the filtered role is created click the name of the role to view the Users that belong to the role. You can also add services to the role by clicking the Services tab.**

Roles

A role's members are LDAP entries that posses the role. The criteria of the role itself is defined as an LDAP entry with attributes, identified by the Distinguished Name (DN) attribute of the entry. Once the role is created, you manually add services and users.

▼ To Create or Modify a Role

1. **Click the Role tab.**
2. **Click New in the Role list.**

3 **Enter a name for the role.**

4 **Click Create.**

▼ To Add Users to a Role or Group

1 **Click the name of the role or group for which you wish to add users.**

2 **Click the Users tab.**

3 **Select the users you wish to add from the Available list and click Add.**

4 **Once the users are displayed in the Selected list, click Save.**

Groups

A *group* represents a collection of users with a common function, feature or interest. Typically, this grouping has no privileges associated with it. Groups can exist at two levels; within an organization and within other managed groups.

▼ To Create or Modify a Group

1 **Click the Group tab.**

2 **Click New from the Group list.**

3 **Enter a name for the group.**

4 **Click Create.**

Once you have created the group, you can add users to the group by clicking the name of the group and then the User tab.

PART III

Directory Management and Default Services

This is part three of the Sun Java System Access Manager 7 2005Q4 Administration Guide. The Directory Management chapter describes how to manage Directory objects when Access Manager is deployed in Legacy Mode. The other chapters describe how to configure and use some of Access Manager's default services. This part contains the following chapters:

- Chapter 10, “Directory Management”
- Chapter 11, “Current Sessions”
- Chapter 12, “Password Reset Service”
- Chapter 13, “Logging Service”

CHAPTER 10

Directory Management

The Directory Management tab is only displayed when you install Access Manager in Legacy mode. This directory management feature provides an identity management solution for Sun Java System Directory Server-enabled Access Manager deployments.

For more information on the Legacy Mode installation option, see the *Sun Java Enterprise System 2005Q4 Installation Guide for UNIX*

Managing Directory Objects

The Directory Management tab contains all the components needed to view and manage the Directory Server objects. This section explains the object types and details how to configure them. User, role, group, organization, sub organization and container objects can be defined, modified or deleted using either the Access Manager console or the command line interface. The console has default administrators with varying degrees of privileges used to create and manage the directory objects. (Additional administrators can be created based on roles.) The administrators are defined within the Directory Server when installed with Access Manager. The Directory Server objects you can manage are:

- "Organizations" on page 167
- "Containers" on page 170
- "Group Containers" on page 171
- "Groups" on page 172
- "People Containers" on page 175
- "Users" on page 176
- "Roles" on page 179

Organizations

An *Organization* represents the top-level of a hierarchical structure used by an enterprise to manage its departments and resources. Upon installation, Access Manager dynamically creates a top-level organization (defined during installation) to manage the Access Manager enterprise configurations. Additional organizations can be created after installation to manage separate enterprises. All created organizations fall beneath the top-level organization.

▼ To Create an Organization

1. **Click the Directory Management tab.**

2. **In the Organizations list, click New.**

3. **Enter the values for the fields. Only Name is required. The fields are:**

Name
Enter a value for the name of the Organization.

Domain Name
Enter the full Domain Name System (DNS) name for the organization, if it has one.

Organization Status
Choose a status of `active` or `inactive` . The default is `active`. This can be changed at any time during the life of the organization by selecting the Properties icon. Choosing `inactive` disables user access when logging in to the organization.

Organization Aliases
This field defines alias names for the organization, allowing you to use the aliases for authentication with a URL login. For example, if you have an organization named `exampleorg`, and define `123` and `abc` as aliases, you can log into the organization using any of the following URLs:

```
http://machine.example.com/amserver/UI/Login?org=exampleorg
```

```
http://machine.example.com/amserver/UI/Login?org=abc
```

```
http://machine.example.com/amserver/UI/Login?org=123
```

Organization alias names must be unique throughout the organization. You can use the Unique Attribute List to enforce uniqueness.

DNS Alias Names
Allows you to add alias names for the DNS name for the organization. This attribute only accepts “real” domain aliases (random strings are not allowed). For example, if you have a DNS named `example.com`, and define `example1.com` and `example2.com` as aliases for an organization named `exampleorg`, you can log into the organization using any of the following URLs:

```
http://machine.example.com/amserver/UI/
```

`Login?org=exampleorg`

`http://machine.example1.com/amserver/`

`UI/Login?org=exampleorg`

`http://machine.example2.com/amserver/`

`UI/Login?org=exampleorg`

Unique Attribute List

Allows you to add a list of unique attribute names for users in the organization. For example, if you add a unique attribute name specifying an email address, you would not be able to create two users with the same email address. This field also accepts a comma-separated list. Any one of the attribute names in the list defines uniqueness. For example, if the field contains the following list of attribute names:

`PreferredDomain, AssociatedDomain`

and `PreferredDomain` is defined as `http://www.example.com` for a particular user, then the entire comma-separated list is defined as unique for that URL. Adding the naming attribute 'ou' to the Unique Attribute List will not enforce uniqueness for the default groups, people containers. (ou=Groups,ou=People).

Uniqueness is enforced for all sub organizations.

4 **Click OK.**

The new organization displays in the Organization list. To edit any of the properties that you defined during creation of the organization, click the name of the organization you wish to edit, change the properties and click Save.

To Delete an Organization

1 **Select the checkbox next to the name of the organization to be deleted.**

2 **Click Delete.**

Note – There is no warning message when performing a delete. All entries within the organization will be deleted and you can not perform an undo.

To Add an Organization to a Policy

Access Manager objects are added to a policy through the policy's subject definition. When a policy is created or modified, organizations, roles, groups, and users can be defined as the subject. Once the subject is defined, the policy will be applied to the object. For more information, see "Managing Policies" on page 147.

Containers

The *container* entry is used when, due to object class and attribute differences, it is not possible to use an organization entry. It is important to remember that the Access Manager container entry and the Access Manager organization entry are not necessarily equivalent to the LDAP object classes `organizationalUnit` and `organization`. They are abstract identity entries. Ideally, the organization entry will be used instead of the container entry.

Note – The display of containers is optional. To view containers you must select Show Containers in the Administration service under Configuration>Console Properties.

▼ To Create a Container

1. **Select the location link of the organization or container where the new container will be created.**
2. **Click the Containers tab.**
3. **Click New in the Containers list.**
4. **Enter the name of the container to be created.**
5. **Click OK.**

▼ To Delete a Container

1. **Click the Containers tab.**
2. **Select the checkbox next to the name of the container to be deleted.**
3. **Click Delete.**

Note – Deleting a container will delete all objects that exist in that Container. This includes all objects and sub containers.

Group Containers

A *group container* is used to manage groups. It can contain only groups and other group containers. The group container Groups is dynamically assigned as the parent entry for all managed groups. Additional group containers can be added, if desired.

Note – The display of group containers is optional. To view group containers you must select Enable Group Containers in the Administration service under Configuration>Console Properties.

▼ To Create a Group Container

1. **Select the location link of the organization or the group container which will contain the new group container.**
2. **Select the Group Containers tab.**
3. **Click New in the Group Containers list.**
4. **Enter a value in the Name field and click OK. The new group container displays in the Group Containers list.**

▼ To Delete a Group Container

1. **Navigate to the organization which contains the group container to be deleted.**
2. **Choose the Group Containers tab.**
3. **Select the checkbox next to the group container to be deleted.**
4. **Click Delete.**

Groups

A *group* represents a collection of users with a common function, feature or interest. Typically, this grouping has no privileges associated with it. Groups can exist at two levels; within an organization and within other managed groups. Groups that exist within other groups are called *sub-groups*. Sub groups are child nodes that "physically" exist within a parent group.

Access Manager also supports *nested groups,* which are "representations" of existing groups contained in a single group. As opposed to sub groups, nested groups can exist anywhere in the DIT. They allow you to quickly set up access permissions for a large number of users.

There are two types of groups you can create; static groups and dynamic groups. Users can only be manually added to static groups, while dynamic groups control the addition of users through a filter. Nested or sub groups can be added to both types.

Static Group

A static group is created based on the Managed Group Type you specify. Group members are added to a group entry using the `groupOfNames` or `groupOfUniqueNames` object class.

Note – By default, the managed group type is dynamic. You can change this default in the Administration service configuration.

Dynamic Group

A dynamic group is created through the use of an LDAP filter. All entries are funneled through the filter and dynamically assigned to the group. The filter would look for any attribute in an entry and return those that contain the attribute. For example, if you were to create a group based on a building number, you can use the filter to return a list all users containing the building number attribute.

Note – Access Manager should be configured with Directory Server to use the referential integrity plug-in. When the referential integrity plug-in is enabled, it performs integrity updates on specified attributes immediately after a delete or rename operation. This ensures that relationships between related entries are maintained throughout the database. Database indexes enhance the search performance in Directory Server. For more information on enabling the plug-in, see the *Sun Java System Access Manager 6 2005Q1 Migration Guide*.

▼ To Create a Static Group

1. **Navigate to the organization, group, or group container where the new group will be created.**

2. **From the Groups list, click New Static.**

3. **Enter a name for the group in the Name field. Click Next.**

4. **Select the Users Can Subscribe to this Group attribute to allow users to subscribe to the group themselves.**

5. **Click OK.**

   Once the group is created, you can edit the Users Can Subscribe to this Group attribute by selecting the name of the group and clicking the General tab.

▼ To Add or Remove Members to a Static Group

1. **From the Groups list, select the group to which you will add members.**

2. **Choose an action to perform in the Select Action menu. The actions you can perform are as follows:**

   New User — This action creates a new user and adds the user to the group when the user information is saved.

   Add User — This action adds an existing user to the group. When you select this action, you create a search criteria which will specify users you wish to add. The fields used to construct the criteria use either an `ANY` or `ALL` operator. `ALL` returns users for all specified fields. `ANY` returns users for any one of the specified fields. If a field is left blank, it will match all possible entries for that particular attribute.

   Once you have constructed the search criteria, click Next. From the returned list of users, select the users you wish to add and click Finish.

   Add Group — This action adds a nested group to the current group. When you select this action, you create a search criteria, including search scope, the name of the group (the "*" wildcard is accepted), and you can specify whether users can subscribe to the group themselves. Once you have entered the information, click Next. From the returned list of groups, select the group you wish to add and click Finish.

   Remove Members — This action will remove members (which includes users and groups) from the group, but will not delete them. Select the member(s) you wish to remove and choose Remove Members from the Select Actions menu.

Delete Members — This action will permanently delete the member you select. Select the member(s) you wish to delete and choose Delete Members.

▼ To Create a Dynamic Group

1. **Navigate to the organization or group where the new group will be created.**

2. **Click the Groups tab.**

3. **Click New Dynamic.**

4. **Enter a name for the group in the Name field.**

5. **Construct the LDAP search filter.**

   By default, Access Manager displays the Basic search filter interface. The Basic fields used to construct the filter use either an `ANY` or `ALL` operator. `ALL` returns users for all specified fields. `ANY` returns users for any one of the specified fields. If a field is left blank it will match all possible entries for that particular attribute.

6. **When you click OK all users matching the search criteria are automatically added to the group.**

▼ To Add or Remove Members to a Dynamic Group

1. **Form the Groups list, click the name of the group to which you will add members.**

2. **Choose an action to perform in the Select Action menu. The actions you can perform are as follows:**

   Add Group — This action adds a nested group to the current group. When you select this action, you create a search criteria, including search scope, the name of the group (the "*" wildcard is accepted), and you can specify whether users can subscribe to the group themselves. Once you have entered the information, click Next. From the returned list of groups, select the group you wish to add and click Finish.

   Remove Members — This action will remove members (which includes groups) from the group, but will not delete them. Select the member(s) you wish to remove and choose Remove Members

   Delete Members — This action will permanently delete the member you select. Select the member(s) you wish to delete and choose Delete Members.

To Add a Group to a Policy

Access Manager objects are added to a policy through the policy's subject definition. When a policy is created or modified, organizations, roles, groups, and users can be defined as the subject in the policy's Subject page. Once the subject is defined, the policy will be applied to the object. For more information, see "Managing Policies" on page 147.

People Containers

A *people container* is the default LDAP organizational unit to which all users are assigned when they are created within an organization. People containers can be found at the organization level and at the people container level as a sub People Container. They can contain only other people containers and users. Additional people containers can be added into the organization, if desired.

Note – The display of people containers is optional. To view People Containers you must select Enable People Containers in the Administration Service.

▼ Create a People Container

1. **Navigate to the organization or people container where the new people container will be created.**
2. **Click New from the People Container list.**
3. **Enter the name of the people container to be created.**
4. **Click OK.**

▼ To Delete a People Container

1. **Navigate to the organization or people container which contains the people container to be deleted.**
2. **Select the checkbox next to the name of the people container to be deleted.**
3. **Click Delete.**

Note – Deleting a people container will delete all objects that exist in that people container. This includes all users and sub people containers.

Users

A *user* represents an individual's identity. Through the Access Manager Identity Management module, users can be created and deleted in organizations, containers and groups and can be added or removed from roles and/or groups. You can also assign services to the user.

Note – If a user in a sub organization is created with the same user ID as `amadmin`, the login will fail for `amadmin`. If this problem occurs, the administrator should change the user's ID through the Directory Server console. This enables the administrator to login to the default organization. Additionally, the DN to Start User Search in the authentication service can be set to the people container DN to ensure that a unique match is returned during the login process.

▼ To Create a User

1. **Navigate to the organization, container or people container where the user is to be created.**

2. **Click the user tab.**

3. **Click New from the user list.**

4. **Enter data for the following values:**

   User ID — This field takes the name of the user with which he or she will log into Access Manager. This property may be a non-DN value.

   First Name — This field takes the first name of the user. The First Name value and the Last Name value identify the user in the Currently Logged In field. This is not a required value.

   Last Name — This field takes the last name of the user. The First Name value and the Last Name value identify the user.

   Full Name — This field takes the full name of the user.

   Password — This field takes the password for the name specified in the User Id field.

   Password (Confirm) — Confirm the password.

   User Status — This option indicates whether the user is allowed to authenticate through Access manager. Only active users can authenticate. The default value is `Active.`

5. **Click OK.**

▼ To Edit the User Profile

When a user who has not been assigned an administrative role authenticates to the Access Manager, the default view is their own User Profile. Additionally, administrators with the proper privileges can edit user profiles. In this view the user can modify the values of the attributes particular to their personal profile. The attributes displayed in the User Profile view can be extended. For more information on adding customized attributes for objects and identities, see the Access Manager Developer's Guide.

1 **Select the user who's profile is to be edited. By default, the General view is displayed.**

2 **Edit the following fields:**

First Name	This field takes the first name of the user.
Last Name	This field takes the last name of the user.
Full Name	This field takes the full name of the user.
Password	Click the Edit link to add and confirm the user password.
Email Address	This field takes the email address of the user.
Employee Number	This field takes the employee number of the user.
Telephone Number	This field takes the telephone number of the user.
Home Address	This field can take the home address of the user.
User Status	This option indicates whether the user is allowed to authenticate through Access Manager. 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.

Note – Changing the user status to Inactive only affects authentication through Access Manager. The Directory Server uses the *nsAccountLock* attribute to determine user account status. User accounts inactivated for Access Manager authentication can still perform tasks that do not require Access Manager. To inactivate a user account in the directory, and not just for Access Manager authentication, set the value of *nsAccountLock* to false. If delegated administrators at your site will be inactivating users on a regular basis, consider adding the *nsAccountLock* attribute to the Access Manager User Profile page. See the *Sun Java System Access Manager 7 2005Q4 Developer's Guide* for details.

Account Expiration Date	If this attribute is present, the authentication service will disallow login if the current date and time has passed the specified Account Expiration Date. The format for this attribute is *mm/dd/yyyy hh:mm*.
User Authentication Configuration	This attribute sets the authentication chain for the user.
User Alias List	The field defines a list of aliases that may be applied to the user. In order to use any aliases configured in this attribute, the LDAP service has to be modified by adding the `iplanet-am-user-alias-list` attribute to the User Entry Search Attributes field in the LDAP service.
Preferred Locale	This field specifies the locale for the user.
Success URL	This attribute specifies the URL that the user will be redirected to upon successful authentication.
Failure URL.	This attribute specifies the URL that the user will be redirected to upon unsuccessful authentication.
Password Reset Options	This is used to select the questions on the forgotten password page, which is used to recover a forgotten password.
User Discovery Resource Offering	Sets the User Discovery service's resource offering for the user.

MSIDSN Number	Defines the user's MSISDN number if using MSISDN authentication.

▼ To Add a User to Roles and Groups

1. **Click the Users tab.**
2. **Click the name of the user you wish to modify.**
3. **Select either the Roles or Groups tab.**
4. **Select the role or group to which you wish to add the user and click Add.**
5. **Click Save.**

Note – To remove a user from Roles or groups, Select roles or groups and click Remove and then Save.

To Add a User to a Policy

Access Manager objects are added to a policy through the policy's subject definition. When a policy is created or modified, organizations, roles, groups, and users can be defined as the subject in the policy's Subject page. Once the subject is defined, the policy will be applied to the object. For more information, see "Managing Policies" on page 147.

Roles

Roles are a Directory Server entry mechanism similar to the concept of a *group*. A group has members; a role has members. A role's members are LDAP entries that possess the role. The criteria of the role itself is defined as an LDAP entry with attributes, identified by the Distinguished Name (DN) attribute of the entry. Directory Server has a number of different types of roles but Access Manager can manage only one of them: the managed role.

Note – The other Directory Server role types can still be used in a directory deployment; they just can not be managed by the Access Manager console. Other Directory Server types can be used in a policy's subject definition. For more information on policy subjects, see "Creating Policies" on page 144.

Users can possess one or more roles. For example, a contractor role which has attributes from the Session Service and the Password Reset Service might be created. When new contractor employees join the company, the administrator can assign them this role rather than setting separate attributes in the contractor entry. If the contractor is working in the Engineering department and requires services and access rights applicable to an engineering employee, the administrator could assign the contractor to the engineering role as well as the contractor role.

Access Manager uses roles to apply access control instructions. When first installed, Access Manager configures access control instructions (ACIs) that define administrator permissions. These ACIs are then designated in roles (such as Organization Admin Role and Organization Help Desk Admin Role) which, when assigned to a user, define the user's access permissions.

Users can view their assigned roles only if the Show Roles on User Profile Page attribute is enabled in the Administration Service.

Note – Access Manager should be configured with Directory Server to use the referential integrity plug-in. When the referential integrity plug-in is enabled, it performs integrity updates on specified attributes immediately after a delete or rename operation. This ensures that relationships between related entries are maintained throughout the database. Database indexes enhance the search performance in Directory Server. For more information on enabling the plug-in, see the *Sun Java System Access Manager 6 2005Q1 Migration Guide*.

There are two types of roles:

- Static — Static roles are created without adding users at the point of the role's creation. Once the role is created, you can then add specific users to it. This gives you more control when adding users to a given role.
- Dynamic – Dynamic roles are created through the use of an LDAP filter. All users are funneled through the filter and assigned to the role at the time of the role's creation. The filter looks for any attribute value pair (for example, `ca=user*`) in an entry and automatically assign the users that contain the attribute to the role.

▼ To Create a Static Role

1. **Go to the organization where the Role will be created.**

2. **Click the Roles tab.**

   A set of default roles are created when an organization is configured, and are displayed in the Roles list. The default roles are:

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

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

Note – When a sub organization is created, remember that the administration roles are created in the sub organization, not in the parent organization.

Container Admin. 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.

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

People Admin. By default, any user entry in an newly created organization is a member of that organization. The People Administrator has read and write access to all user entries in the organization. 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.

Note – 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 organization has already been configured, the Container Admin Role or Container Help Desk Admin defaults would be used.

Group Admin. The Group Administrator created when a group is created 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.

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

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

3 **Click the New Static button.**

4 **Enter a name for the role.**

5 **Enter a description of the role.**

6 **Choose the role type from the Type menu.**

The role can be either an Administrative role or a Service role. The role type is used by the console to determine and here to start the user in the Access Manager console. An administrative role notifies the console that the possessor of the role has administrative privileges; the service role notifies the console that the possessor is an end user.

7 **Choose a default set of permissions to apply to the role from the Access Permission menu. The permissions provide access to entries within the organization. The default permissions shown are in no particular order. The permissions are:**

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 organization. The Organization Policy Administrator can not create a referral policy to a peer organization. Generally, the No Permissions ACI is assigned to Service roles, while Administrative roles are assigned any of the default ACIs.

▼ To Add Users to a Static Role

1 **Click the name of the role to which you wish to add users.**

2 **In the Members list, select Add User from the Select Action menu.**

3 **Enter the information for the search criteria. You can choose to search for users based on one or more the displayed fields The fields are:**

Match	Allows you to select the fields you wish to include for the filter. `ALL` returns users for all specified fields. `ANY` returns users for any one of the specified fields.
First Name	Search for users by their first name.
User ID	Search for a user by User ID.
Last Name	Search for users by their last name.

Full Name	Search for users by their full name.
User Status	Search for users by their status (active or inactive)

4 **Click Next to begin the search. The results of the search are displayed.**

5 **Choose the users from the names returned by selecting the checkbox next to the user name.**

6 **Click Finish.**

The Users are now assigned to the role.

▼ To Create a Dynamic Role

1 **Go to the organization where the Role will be created.**

2 **Click the Roles tab.**

A set of default roles are created when an organization is configured, and are displayed in the Roles list. The default roles are:

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

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

Note – When a sub organization is created, remember that the administration roles are created in the sub organization, not in the parent organization.

Container Admin. 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.

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

People Admin. By default, any user entry in an newly created organization is a member of that organization. The People Administrator has read and write access to all user entries in the organization. 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.

Note – 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 organization has already been configured, the Container Admin Role or Container Help Desk Admin defaults would be used.

Group Admin. The Group Administrator created when a group is created 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.

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

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

3. **Click the New Dynamic button.**

4. **Enter a name for the role.**

5. **Enter a description for the role.**

6. **Choose the role type from the Type menu.**

   The role can be either an Administrative role or a Service role. The role type is used by the console to determine and where to start the user in the Access Manager console. An administrative role notifies the console that the possessor of the role has administrative privileges; the service role notifies the console that the possessor is an end user.

7. **Choose a default set of permissions to apply to the role from the Access Permission menu. The permissions provide access to entries within the organization. The default permissions shown are in no particular order. The permissions are:**

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 organization. The Organization Policy Administrator can not create a referral policy to a peer organization.

Generally, the No Permissions ACI is assigned to Service roles, while Administrative roles are assigned any of the default ACIs.

8 **Enter the information for the search criteria. The fields are:**

Match	Allows you to include an operator for any the fields you wish to include for the filter. `ALL` returns users for all specified fields. `ANY` returns users for any one of the specified fields.
First Name	Search for users by their first name.
User ID	Search for a user by User ID.
Last Name	Search for users by their last name.
Full Name	Search for users by their full name.
User Status	Search for users by their status (active or inactive)

9 **Click OK to initiate the search based on the filter criteria. The users defined by the filter criteria are automatically assigned to the role.**

To Remove Users from a Role

1 **Navigate to the Organization that contains the role to modify.**

Choose Organizations from the View menu in the Identity Management module and select the Roles tab.

2 **Select the role to modify.**

3 **Choose Users from the View menu.**

4 **Select the checkbox next to each user to be removed.**

5 **Click Remove user from the Select Action menu.**

The users are now removed from the role.

To Add a Role to a Policy

Access Manager objects are added to a policy through the policy's subject definition. When a policy is created or modified, organizations, roles, groups, and users can be defined as the subject in the policy's Subject page. Once the subject is defined, the policy will be applied to the object. For more information, see "Managing Policies" on page 147.

CHAPTER 11

Current Sessions

This chapter describes the session management features of Access Manager. The Session Management module provides a solution for viewing user session information and managing user sessions. It keeps track of various session times as well as allowing the administrator to terminate a session. System administrators should ignore the Load Balancer servers listed in the Platform Server list.

The Current Sessions Interface

The Current Sessions module interface allows an administrator, with the appropriate permissions, to view the session information for any user who is currently logged in to Access Manager.

Session Management

The Session Management frame displays the name of the Access Manager that is currently being managed.

Session Information

The Session Information window displays all of the users who are currently logged into Access Manager, and displays the session time for each user. The display fields are:

User ID. Displays the user ID of the user who is currently logged in.

Time Left. Displays the amount of time (in minutes) remaining that the user has for that session before having to re-authenticate.

Max Session Time. Displays the maximum time (in minutes) that the user can be logged in before the session expires and must re-authenticate to regain access.

Idle Time. Displays the time (in minutes) that the user has been idle.

Max Idle Time. Displays the maximum time (in minutes) that a user can remain idle before having to re-authenticate.

The time limits are defined by the administrator in the Session Management Service.

You can display a specific user session, or a specific range of user sessions, by entering a string in the User ID field and clicking Filter. Wildcards are permitted.

Clicking the Refresh button will update the user session display.

Terminating a Session

Administrators with appropriate permissions can terminate a user session at any time.

▼ To Terminate a Session

1. **Select the user session that you wish to terminate.**

2. **Click Terminate.**

CHAPTER 12

Password Reset Service

Access Manager provides a Password Reset service to allow users to reset their password for access to a given service or application protected by Access Manager. The Password Reset service attributes, defined by the top-level administrator, control user validation credentials (in the form of secret questions), control the mechanism for new or existing password notification, and sets possible lockout intervals for incorrect user validation.

This chapter contains the following sections:

- "Registering the Password Reset Service" on page 189
- "Configuring the Password Reset Service" on page 190
- "Password Reset for End Users" on page 192

Registering the Password Reset Service

The Password Reset service does not need to be registered for the realm in which the user resides. If the Password Reset service does not exist in the organization in which the user resides, it will inherit the values defined for the service in Service Configuration.

▼ To Register Password Reset for Users in a Different Realm

1 **Navigate to the realm to which you will register the password for the user.**

2 **Click the realm name and click the Services tab.**

If it has not been added to the realm, click the Add button.

3 **Select the r Password Reset and click Next**

The Password Reset service attributes will be displayed. For attribute definitions, see the online help.

4 **Click Finish.**

Configuring the Password Reset Service

Once the Password Reset service has been registered, the service must be configured by a user with administrator privileges.

▼ To Configure the Service

1 **Select the realm for which the Password Reset service is registered.**

2 **Click the Services tab.**

3 **Click Password Reset from the services list.**

4 **The Password Reset attributes appear, allowing you to define requirements for the Password Reset service. Make sure that the Password Reset service is enabled (it is by default). At a minimum, the following attributes must be defined:**

- User Validation
  - Secret Question
  - Bind DN
  - Bind Password

    The Bind DN attribute must contain a user with privileges for resetting the password (for example, Help Desk Administrator). Due a limitation in Directory Server, Password Reset does not work when the bind DN is `cn=Directory Manager`.

    The remaining attributes are optional. See the online help for a description of the service attributes.

Note – Access Manager automatically installs the Password Reset web application for random password generation. However, you can write your own plug-in classes for password generation and password notification. See the following Readme.html files in the following locations for samples for these plug-in classes.

PasswordGenerator:

```
AccessManager-base/SUNWam/samples/console/PasswordGenerator
```

NotifyPassword:

```
AccessManager-base/SUNWam/samples/console/NotifyPassword
```

5 **Select the Personal Question Enabled attribute if the user is to define his/her unique personal questions. Once the attributes are defined, click Save.**

Password Reset Lockout

The Password Reset service contains a lockout feature that will restrict users to a certain number of attempts to correctly answer their secret questions. The lockout feature is configured through the Password Reset service attributes. See the online help for a description of the service attributes. Password Reset supports two types of lockout, memory lockout and physical lockout.

Memory Lockout

This is a temporary lockout and is in effect only when the value in the Password Reset Failure Lockout Duration attribute is greater than zero and the Enable Password Reset Failure Lockout attribute is enabled. This lockout will prevent users from resetting their password through the Password Reset web application. The lockout lasts for the duration specified in Password Reset Failure Lockout Duration, or until the server is restarted. See the online help for a description of the service attributes.

Physical Lockout

This is a more permanent lockout. If the value set in the Password Reset Failure Lockout Count attribute is set to 0 and the Enable Password Reset Failure Lockout attribute is enabled, the users' account status is changed to inactive when he or she incorrectly answers the secret questions. See the online help for a description of the service attributes.

Password Reset for End Users

The following sections describe the user experience for the Password Reset service.

Customizing Password Reset

Once the Password Reset service has been enabled and the attributes defined by the administrator, users are able to log into the Access Manager console in order to customize their secret questions.

▼ To Customize Password Reset

1. **The user logs into the Access Manager console, providing Username and Password and is successfully authenticated.**

2. **In the User Profile page, the user selects Password Reset Options. This displays the Available Questions Answer Screen.**

3. **The user is presented with the available questions that the administrator defined for the service, such as:**

   - What is your pet's name?
     - What is your favorite TV show?
     - What is your mother's maiden name?
     - What is your favorite restaurant?

4. **The user selects the secret questions, up to the maximum number of questions that the administrator defined for the realm (the maximum amount is defined the Password Reset Service). The user then provides answers to the selected questions. These questions and answers will be the basis for resetting the user's password (see the following section). If the administrator has selected the Personal Question Enabled attribute, text fields are provided, allowing the user to enter a unique secret question and provide an answer.**

5. **The user clicks Save.**

Resetting Forgotten Passwords

In the case where users forget their password, Access Manager uses the Password Reset web application to randomly generate new passwords and notify the user of the new password. A typical forgotten password scenario follows:

▼ To Reset Forgotten Passwords

1 **The user logs into the Password Reset web application from a URL given to them by the administrator. For example:**

`http://`hostname:port `/ampassword` (for the default realm

or

`http://`hostname: port/*deploy_uri* `/UI/PWResetUserValidation?realm=realmname`, where realmname is the name of the realm.

Note – If the Password Reset service is not enabled for a parent realm but is enabled for a sub-realm, users must use the following syntax to access the service:

`http://hostname: port/`*deploy_uri*`/UI/PWResetUserValidation?realm=realmname`

---

2 **The user enters the user id.**

3 **The user is presented with the personal questions that were defined in the Password Reset service and select by the user during customization. If the user has not previously logged into the User Profile page and customized the personal questions, the password will not be generated.**

Once the user answers the questions correctly, the new password is generated and emailed to the user. Attempt notification is sent to the user whether the questions are answered correctly or not. Users must have their email address entered in the User Profile page in order for the new password and attempt notification to be received.

Password Policies

A secure password policy minimizes the risks associated with easily-guessed passwords by enforcing the following:

- Users must change their passwords according to a schedule.
- Users must provide non-trivial passwords.
- Accounts may be locked after a number of binds with the wrong password.

Directory Server provides several ways to set password policy at any node in a tree and there are several ways to set the policy. For details refer following Directory Server documentation:

http://docs.sun.com/source/816-6700-10/aci.html#14773

http://docs.sun.com/source/816-6698-10/useracct.html#14386

◆ ◆ ◆ CHAPTER 13

Logging Service

Sun Java™ System Access Manager 7 2005Q4 provides a Logging Service to record information such as user activity, traffic patterns, and authorization violations. In addition, the debug files allow administrators to troubleshoot their installation.

Log Files

The log files record a number of events for each of the services it monitors. These files should be checked by the administrator on a regular basis. The default directory for the log files is `/var/opt/SUNWam/logs` for SPARC systems and `/var/opt/sun/identity` for Linux systems. The log file directory can be configured in the Logging Service by using the Access Manager console.

See "How the Logging Feature Works" in *Sun Java System Access Manager 7 2005Q4 Technical Overview* in the Sun Java System Access Manager Technical Overview for a detailed list of the default log file types, the information that is recorded, and log file formats.

For attribute definitions for the Logging Service, see the online help by clicking the Help button in the Access Manager Console.

Access Manager Service Logs

There are two different types of service log files: access and error. Access log files may contain records of action attempts and successful results. Error log files record errors that occur within the Access Manager services. Flat log files are appended with the `.error` or `.access` extension. Database column names end with `_ERROR` or `_ACCESS` for Oracle databases, or `_error` or `_access` for MySQL databases. For example, a flat file logging console events is named `amConsole.access`, while a database column logging the same events is named `AMCONSOLE_ACCESS.` The following sections describe the log files recorded by the Logging Service.

Session Logs

The Logging Service records the following events for the Session Service:

- Login
- Logout
- Session Idle TimeOut
- Session Max TimeOut
- Failed To Login
- Session Reactivation
- Session Destroy

The session logs are prefixed with `amSSO.`

Console Logs

The Access Manager console logs record the creation, deletion and modification of identity-related objects, policies and services including, among others, organizations, organizational units, users, roles, policies and groups. It also records modifications of user attributes including passwords and the addition or removal of users to or from roles and groups. Additionally, the console logs write delegation and data store activities. The console logs are prefixed with `amConsole.`

Authentication Logs

Authentication component logs user logins and logouts. The authentication logs are prefixed with `amAuthentication.`

Federation Logs

The Federation component logs federation-related events including, but not limited to, the creation of an Authentication Domain and the creation of a Hosted Provider. The federation logs are prefixed with `amFederation.`

Policy Logs

The Policy component records policy-related events including, but not limited to, policy administration (policy creation, deletion and modification) and policy evaluation. The policy logs are prefixed with `amPolicy`.

Agent Logs

The policy agent logs are responsible for logging exceptions regarding log resources that were either allowed or denied to a user. The agent logs are prefixed with `amAgent`. `amAgent` logs reside on the agent server only. Agent events are logged on the Access Manager server in the Authentication Logs. For more information on this function, see the documentation for the policy agent in question.

SAML Logs

The SAML component records SAML-related events including, but not limited to, assertion and artifact creation or removal, response and request details, and SOAP errors. The session logs are prefixed with `amSAML`.

amAdmin Logs

The command line logs record event errors that occur during operations using the command line tools. These include, but are not limited to, loading a service schema, creating policy and deleting users. The command line logs are prefixed with `amAdmin.`

Logging Features

The Logging Service has a number of special features which can be enabled for additional functionality. They include To Enable Secure Logging, Command Line Logging and Remote Logging.

Secure Logging

This optional feature adds additional security to the logging function. Secure Logging enables detection of unauthorized changes to, or tampering of, the security logs. No special coding is required to leverage this feature. Secure Logging is accomplished by using a pre-registered certificate configured by the system administrator. This Manifest Analysis and Certification (MAC) is generated and stored for every log record. A special "signature" log record is periodically inserted that represents the signature for the contents of the log written to that point. The combination of the two records ensures that the logs have not been tampered with.

▼ To Enable Secure Logging

1 **Create a certificate with the name `Logger` and install it in the deployment container running Access Manager. See the documentation for the deployment container for details.**

2 **Turn on Secure Logging in the Logging Service configuration using the Access Manager console and save the change. The administrator can also modify the default values for the other attributes in the Logging Service.**

If the logging directory is changed from the default (`/var/opt/SUMWam/logs`), make sure that the permissions are set to 0700. The logging service will create the directory, if it does not exist, but it will create the directory with permissions set to 0755.

Additionally, if you specify a different directory from the default, you must change the following parameter to the new directory in the web container's `server.policy` file:

```
permission java.io.FilePermission “/var/opt/SUNWam/logs/*”,”delete,write”
```

3 **Create a file in the** ***AccessManager-base*****/`SUNWam/config` directory that contains the certificate database password and name it `.wtpass`.**

Note – The file name and the path to it is configurable in the `AMConfig.properties` file. For more information see the "Certificate Database" in Appendix A, “AMConfig.properties File.”

Ensure that the deployment container user is the only administrator with read permissions to this file for security reasons.

---

4 **Restart the server.**

The secure log directory should be cleared, as some misleading verification errors may be written to the `/var/opt/SUNWam/debug/amLog` file when the secure logging was started.

To detect unauthorized changes or tampering of the security logs, look for error messages that are written by the verification process to `/var/opt/SUNWam/debug/amLog`. To manually check for tampering, run the `VerifyArchive` utility. See Chapter 19, “The VerifyArchive Command Line Tool,” for more information.

Command Line Logging

The `amadmin` command line tool has the ability to create, modify and delete identity objects (organizations, users, and roles, for example) in Directory Server. This tool can also load, create, and register service templates. The Logging Service can record these actions by invoking the `-t` option. If the `com.iplanet.am.logstatus` property in `AMConfig.properties` is enabled (ACTIVE) then a log record will be created. (This property is enabled by default.) The command line logs are prefixed with `amAdmin.` See Chapter 14, “The amadmin Command Line Tool,” for more information.

Logging Properties

There are properties in the `AMConfig.properties` file that affect logging output:

`com.iplanet.am.logstatus=ACTIVE`	This property will enable or disable logging. The default is ACTIVE.
`iplanet-am-logging.`*service*`.level=` *level*	*service* is the service's normal debug file name. *level* is one of the `java.util.logging.Level` values and denotes the level of detail recorded in the logs. The levels are SEVERE, WARNING, INFO, CONFIG, FINE, FINER, and FINEST. Most services do not record log levels with higher detail than INFO.

Remote Logging

Access Manager supports remote logging. This allows a client application using a host where the Access Manager SDK is installedto create log records on an instance of Access Manager deployed on a remote machine. Remote logging can be initiated in any of the following scenarios:

1. When the logging URL in the Naming Service of one Access Manager instance points to a remote instance and there is a trust relationship configured between the two, logs will be written to the remote Access Manager instance.
2. When the Access Manager SDK is installed against a remote Access Manager instance and a client (or a simple Java class) running on the SDK server uses the logging APIs, the logs will be written to the remote Access Manager machine.
3. When logging APIs are used by Access Manager agents.

▼ To Enable Remote Logging

1 **If using Sun Java System Web Server, the following environment variables need to be set in the** `server.xml` **configuration file:**

- `java.util.logging.manager=com.sun.identity.log.LogManager`
- `java.util.logging.config.file=/`*AccessManager-base*
  `/SUNwam/lib/LogConfig.properties`
- If the Java™ 2 Platform, Standard Edition being used is 1.4 or later, this is accomplished by invoking the following at the command line:

  `java -cp /`*AccessManager-base* `/SUNWam/lib/am_logging.jar:/`*AccessManager-base*
  `/SUNWam/lib/xercesImpl.jar:/`*AccessManager-base*
  `/SUNWam/lib/xmlParserAPIs.jar:/`*AccessManager-base*
  `/SUNWam/lib/jaas.jar:/`*AccessManager-base*
  `/SUNWam/lib/xmlParserAPIs.jar:/`*AccessManager-base*
  `/SUNWam/lib/servlet.jar:/`*AccessManager-base*

/SUNWam/locale:/*AccessManager-base*/SUNWam/lib/am_services.jar:/ *AccessManager-base*/SUNWam/lib/am_sdk.jar:/ *AccessManager-base*/SUNWam/lib/jss311.jar:/ *AccessManager-base*/SUNWam/lib:.

`-Djava.util.logging.manager=com.sun.identity.log.LogManager`

`-Djava.util.logging.config.file=/`*AccessManager-base* `/SUNwam/lib/LogConfig.properties <logTestClass>`

- If the Java 2 Platform, Standard Edition being used is earlier than 1.4, this is accomplished by invoking the following at the command line:

  java -Xbootclasspath/a:/*AccessManager-base* /SUNWam/lib/jdk_logging.jar -cp /*AccessManager-base* /SUNWam/lib/am_logging.jar:/*AccessManager-base* /SUNWam/lib/xercesImpl.jar:/*AccessManager-base* /SUNWam/lib/xmlParserAPIs.jar:/*AccessManager-base* /SUNWam/lib/jaas.jar:/*AccessManager-base* /SUNWam/lib/xmlParserAPIs.jar:/*AccessManager-base* /SUNWam/lib/servlet.jar:/*AccessManager-base* /SUNWam/locale:/*AccessManager-base*/SUNWam/lib/am_services.jar:/ *AccessManager-base*/SUNWam/lib/am_sdk.jar:/ *AccessManager-base*/SUNWam/lib/jss311.jar:/ *AccessManager-base*/SUNWam/lib:.

  `-Djava.util.logging.manager=com.sun.identity.log.LogManager`

  `-Djava.util.logging.config.file=/`*AccessManager-base* `/SUNwam/lib/LogConfig.properties <logTestClass>`

2 **Ensure that the following parameters are configured in** `LogConfig.properties` **located in** *AccessManager-base*/SUNWam/lib:

- `iplanet-am-logging-remote-handler=com.sun.identity.`

  `log.handlers.RemoteHandler`

- `iplanet-am-logging-remote-formatter=com.sun.`

  `identity.log.handlers.RemoteFormatter`

- `iplanet-am-logging-remote-buffer-size=1`

  Remote logging supports buffering on the basis of the number of log records. This value defines the log buffer size by the number of records. Once the buffer is full, all buffered records will be flushed to the server.

- `iplanet-am-logging-buffer-time-in-seconds=3600`

  This value defines the time-out period in which to invoke the log buffer-cleaner thread.

- `iplanet-am-logging-time-buffering-status=OFF`

  This value defines whether log buffering (and the buffer-cleaner thread) is enabled. By default this feature is turned off.

Note – Whenever a log file is empty, secure logging may show "verification failure." This is because when the number of created files is equal to the archive size, secure logging will archive from this set and start again. It most instances, you can ignore this error. Once the number of records is equal to the archive size, the error will not be displayed.

Error and Access Logs

Two types of Access Manager log files exist: access log files and error log files.

Access log files record general auditing information concerning the Access Manager deployment. A log may contain a single record for an event such as a successful authentication. A log may contain multiple records for the same event. For example, when an administrator uses the console to change an attribute value, the Logging Service logs the attempt to change in one record. Logging Service also logs the results of the execution of the change in a second record.

Error log files record errors that occur within the application. While an operation error is recorded in the error log, the operation attempt is recorded in the access log file.

Flat log files are appended with the `.error` or `.access` extension. Database column names end with `_ERROR` or `_ACCESS`. For example, a flat file logging console events is named `amConsole.access` while a database column logging the same events is named `AMCONSOLE_ACCESS` or `amConsole_access`.

The following table provides a brief description of the log file produced by each Access Manager component.

TABLE 13–1 Access Manager Component Logs

Component	Log Filename Prefix	Information Logged
Session	`amSSO`	Session management attributes values such as login time, logout time, timeout limits.
Administration Console	`amConsole`	User actions performed through the administration console such as creation, deletion and modification of identity-related objects, realms, and policies.
Authentication	`amAuthentication`	User logins and logouts.
Identity Federation	`amFederation`	Federation-related events such as the creation of an Authentication Domain and the creation of a Hosted Provider. The federation logs are prefixed with `amFederation`.

TABLE 13–1 Access Manager Component Logs *(Continued)*

Component	Log Filename Prefix	Information Logged
Authorization (Policy)	`amPolicy`	Policy-related events such as policy creation, deletion, or modification, and policy evaluation.
Policy Agent	`amAgent`	Exceptions regarding resources that were either accessed by a user or denied access to a user. `amAgent` logs reside on the server where the policy agent is installed. Agent events are logged on the Access Manager machine in the Authentication logs.
SAML	`amSAML`	SAML-related events such as assertion and artifact creation or removal, response and request details, and SOAP errors.
Command-line	`amAdmin`	Event errors that occur during operations using the command line tools. Examples are: loading a service schema, creating policy, and deleting users.

See Appendix C, "Log File Reference," for list and description of the Access Manager log files.

Debug Files

The debug files are not a feature of the Logging Service. They are written using different APIs which are independent of the logging APIs. Debug files are stored in `/var/opt/SUNWam/debug`. This location, along with the level of the debug information, is configurable in the `AMConfig.properties` file, located in the *AccessManager-base*`/SUNWam/lib/` directory. For more information on the debug properties, see Appendix A, "AMConfig.properties File."

Debug Levels

There are several levels of information that can be recorded to the debug files. The debug level is set using the `com.iplanet.services.debug.level` property in `AMConfig.properties`.

1. Off—No debug information is recorded.
2. Error—This level is used for production. During production, there should be no errors in the debug files.
3. Warning—Currently, using this level is not recommended.
4. Message—This level alerts to possible issues using code tracing. Most Access Manager modules use this level to send debug messages.

Note – Warning and Message levels should not be used in production. They cause severe performance degradation and an abundance of debug messages.

Debug Output Files

A debug file does not get created until a module writes to it. Therefore, in the default `error` mode no debug files may be generated. The debug files that get created on a basic login with the debug level set to `message` include:

- amAuth
- amAuthConfig
- amAuthContextLocal
- amAuthLDAP
- amCallback
- amClientDetection
- amConsole
- amFileLookup
- amJSS
- amLog
- amLoginModule
- amLoginViewBean
- amNaming
- amProfile
- amSDK
- amSSOProvider
- amSessionEncodeURL
- amThreadManager

The most often used files are the `amSDK, amProfile` and all files pertaining to authentication. The information captured includes the date, time and message type (Error, Warning, Message).

Using Debug Files

The debug level, by default, is set to `error`. The debug files might be useful to an administrator when they are:

- Writing a custom authentication module.
- Writing a custom application using the Access manager SDKs. The `amProfile` and `amSDK` debug files capture this information.
- Troubleshooting access permissions while using the console or SDK. The `amProfile` and `amSDK` debug files also capture this information.
- Troubleshooting SSL.

- Troubleshooting the LDAP authentication module. The amAuthLDAP debug file captures this information.

The debug files should go hand in hand with any troubleshooting guide we might have in the future. For example when SSL fails, someone might turn on debug to message and look in the amJSS debug file for any specific certificate errors.

Multiple Access Manager Instances And Debug Files

Access Manager contains the ammultiserverinstall script that can be used to configure numerous instances of the server. If the multiple server instances are configured to use different debug directories, each individual instance has to have both read and write permissions to the debug directories.

PART IV

Command Line Reference

This is the Command Line Reference, part four of the Sun Java System Access Manager 7 2005Q4 Administration Guide.

All of the command line tools described in this section can be found in the following default locations:

```
AccessManager-base/SUNWam/bin (Solairs)
AccessManager-base/identity/bin (Linux)
```

This section contains the following chapters:

- Chapter 14, “The amadmin Command Line Tool”
- Chapter 15, “The ampassword Command Line Tool”
- Chapter 16, “The bak2am Command Line Tool”
- Chapter 17, “The am2bak Command Line Tool”
- Chapter 18, “The amserver Command Line Tool”
- Chapter 19, “The VerifyArchive Command Line Tool”
- Chapter 20, “The amsecuridd Helper”

CHAPTER 14

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.

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 XML files even if there are errors. For example, if there are three XML files to be loaded at the same time, and the first XML file fails, amadmin will continue to load the remaining files. The continue option only applies to separate requests.

--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.

--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 210.

EXAMPLE 14–1 Portion of sampleMailService.xml

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

--help (-h)

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

--version (-n)

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

Using amadmin for Federation Management

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

--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. XML shall be Liberty meta XSD compliance.

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>
-q|--exportwithsig <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

--exportwithsig (-o)

The name of the file to contain the XML of the entity. This file is digitally signed. The XML must be Liberty meta XSD compliant.

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 15

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 215

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 16

The bak2am Command Line Tool

This chapter provides information on the bak2am command line tool and contains the following section:

- "The bak2am Command Line Executable" on page 217

The bak2am Command Line Executable

Access Manager contains an bak2am utility under AccessManager-base/SUNWam/bin. This utility performs a restore of the Access Manager components that were backed-up by the am2back utility.

The bak2am Syntax

The generic syntax for using the bak2am tool for the Solaris operating system is:

```
./bak2am [ -v | --verbose ] -z | --gzip tar.gz-file
./bak2am [ -v | --verbose ] -t | --tar tar-file
./bak2am -h | --help
./bak2am -n | --version
```

The generic syntax for using the bak2am tool for the Windows 2000 operating system is:

```
bak2am [ -v | --verbose ] -d | --directory directory-name

bak2am -h | --help
bak2am -n | --version
```

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

bak2am Options

--gzip *backup-name*

`--gzip` specifies the full path and filename of the backup file in `tar.gz` format. By default, the path is `AccessManager-base/backup` . This option is for Solaris only.

--tar *backup-name*

`--tar` specifies the full path and filename of the backup file in `tar` format. By default, the path is `AccessManager-base/backup` . This option is for Solaris only.

--verbose

`--verbose` is used to run the backup utility in verbose mode.

--directory

`--directory` specifies the backup directory. By default, the path is `AccessManager-base/backup`. This option is for Windows 2000 only.

--help

`--help` is an argument that displays the syntax for the `bak2am` command.

--version

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

CHAPTER 17

The am2bak Command Line Tool

This chapter provides information on the `am2bak` command line tool.

The am2bak Command Line Executable

Access Manager contains an `am2bak` utility under `AccessManager-base/SUNWam/bin`. This utility performs a backup of either all or optional components of Access Manager. Directory Server must be running while taking the log backup.

The am2bak Syntax

The generic syntax for using the `am2bak` tool for the Solaris operating system is:

```
./am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l | --location location ] [[-c | --config] | [-b | --debug] | [-g | --log] | [-t | --cert] | [-d | --ds] | [-a | --all]]*
```

```
./am2bak -h | --help
```

```
./am2bak -n | --version
```

The generic syntax for using the `am2bak` tool for the Windows 2000 operating system is:

```
am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l | --location location ] [[-c | --config] | [-b | --debug] | [-g | --log] | [-t | --cert] | [-d | --ds] | [-a | --all]]*
```

```
am2bak -h | --help
```

```
am2bak -n | --version
```

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

am2bak Options

--verbose (-v)

`--verbose` is used to run the backup utility in verbose mode.

--backup *backup-name (-k)*

`--backup` *backup-name* defines the name of the backup file. The default is `ambak`.

--location (-l)

`--location` specifies the directory location of the backup. The default location is `AccessManager-base/backup`.

--config (-c)

`--config` specifies backup only for configuration files.

--debug (-b)

`--debug` specifies backup only for debug files.

--log (-g)

`--log` specifies backup only for log files.

--cert (-t)

`--cert` specifies backup only for certificate database files.

--ds (-d)

`--ds` specifies backup only for the Directory Server.

--all (-a)

`--all` specifies a complete backup of the entire Access Manager.

--help (-h)

`--help` is an argument that displays the syntax for the `am2bak` command.

--version (-n)

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

To Run the Backup Procedure

1. **Login as root.**

   The user running this script must have root access.

2. **Run the script ensuring that the correct path is used, if necessary.**

   The script will backup the following Solaris™ Operating Environment files:

   - Configuration and Customization Files:
     - `AccessManager-base/SUNWam/config/`
       - `AccessManager-base/SUNWam/locale/`
       - `AccessManager-base/SUNWam/servers/httpacl`
       - `AccessManager-base/SUNWam/lib/*.properties` (Java property files)
       - `AccessManager-base/SUNWam/bin/amserver.` *instance-name*
       - `AccessManager-base/SUNWam/servers/https-` *all_instances*
       - `AccessManager-base/SUNWam/servers/web-apps-` *all_instances*
       - `AccessManager-base/SUNWam/web-apps/services/WEB-INF/config`
       - `AccessManager-base/SUNWam/web-apps/services/config`
       - `AccessManager-base/SUNWam/web-apps/applications/WEB-INF/classes`
       - `AccessManager-base/SUNWam/web-apps/applications/console`
       - `/etc/rc3.d/K55amserver.`*all_instances*
       - `/etc/rc3.d/S55amserver.`*all_instances*
       - `DirectoryServer-base/slapd-` *host* `/config/schema/`
       - `DirectoryServer-base/slapd-` *host* `/config/slapd-collations.conf`
       - `Access Manager/slapd-` *host* `/config/dse.ldif`

       Log And Debug Files:

       - `var/opt/SUNWam/logs` (Access Manager log files)
       - `var/opt/SUNWam/install` (Access Manager installation log files)
       - `var/opt/SUNWam/debug` (Access Manager debug files)

       Certificates:

       - `Access Manager/SUNWam/servers/alias`
       - `Access Manager/alias`

         The script will also backup the following Microsoft® Windows 2000 operating system files:

       Configuration and Customization Files:

- `AccessManager-base/web-apps/services/WEB-INF/config/*`
- `AccessManager-base/locale/*`
- `AccessManager-base/web-apps/applications/WEB-INF/classes/*.properties` (java property files)
- `AccessManager-base/servers/https-` *host*`/config/jvm12.conf`
- `AccessManager-base/servers/https-` *host*`/config/magnus.conf`
- `AccessManager-base/servers/https-` *host*`/config/obj.conf`
- `DirectoryServer-base/slapd-host/config/schema/*.ldif`
- `DirectoryServer-base/slapd-host/config/slapd-collations.conf`
- `DirectoryServer-base/slapd-host/config/dse.ldif`

Log And Debug Files:

- `var/opt/logs` (Access Manager log files)
- `var/opt/debug` (Access Manager debug files)

Certificates:

- `AccessManager-base/servers/alias`
- `AccessManager/alias`

CHAPTER 18

The amserver Command Line Tool

This chapter provides information on the `amserver` command line tool. This chapter contains the following section:

- "The amserver Command Line Executable" on page 223

The amserver Command Line Executable

The `amserver` command line executable starts and stops the `amunixd` and `amsercuridd` helpers, associated with Unix and SecurID authentication modules, respectively.

amserver Syntax

The generic syntax for the tools is:

```
./amserver { start | stop }
```

start

`start` is a command that starts the helper.

stop

`stop` is a command that stops the helper.

CHAPTER 19

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 225

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 20

The amsecuridd Helper

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

- "The amsecuridd Helper Command Line Executable" on page 227
- "Running the amsecuridd helper" on page 228

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 V

Appendixes

This is part five of the Sun Java System Access Manager 7 2005Q4 Administration Guide contains error code listings and file reference. This section contains the following appendixes:

- Appendix A, “AMConfig.properties File”
- Appendix B, “serverconfig.xml File”
- Appendix C, “Log File Reference”
- Appendix D, “Error Codes”

APPENDIX A

AMConfig.properties File

`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 234
- “Access Manager Console” on page 234
- “Access Manager Server Installation” on page 234
- “am.util” on page 236
- “amSDK” on page 236
- “Application Server Installation” on page 236
- “Authentication” on page 237
- “Certificate Database” on page 238
- “Cookies” on page 238
- “Debugging” on page 239
- “Directory Server Installation” on page 240
- “Event Connection” on page 240
- “Global Services Management” on page 241
- “Helper Daemons” on page 241
- “Identity Federation” on page 242
- “JSS Proxy” on page 243
- “LDAP Connection” on page 244
- “Logging Service” on page 247
- “Naming Service” on page 249
- “Notification Service” on page 249
- “Policy Agents” on page 249
- “Policy Client API” on page 251
- “Profile Service” on page 252
- “Replication” on page 252
- “SAML Service” on page 252

- "Security" on page 253
- "Session Service" on page 254
- "SMTP" on page 255
- "Statistics Service" on page 255

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 modify 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 modify the property value.

  Value is set during installation. Example: /var/opt/SUNWam

- `com.iplanet.am.installdir`

  This is a READ-ONLY property. Do not modify 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 false.

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 `amserverscript` 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`

  Default value is `false`. Specifies the Proxy Server to use for a connection. Set to `true` if `LDAPProxy` is supported by the backend storage. If `true`, use the Proxy Server for connection If false, no proxy is used for connection.
- `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 the Platform Server list against the server host that is being accessed. If the server FQDNs of the two servers in the Platform Server list match, Access Manager continues the SSL handshaking. 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
```

Logging to a particular log file can also be turned off. Example:

```
iplanet-am-logging.amConsole.access.evel=OFF
```

TABLE A–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
`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.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.

◆ ◆ ◆ APPENDIX B

serverconfig.xml File

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 257
- "server-config Definition Type Document" on page 258
- "Failover Or Multimaster Configuration" on page 261

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 257 illustrates where the encrypted password is located in serverconfig.xml .

EXAMPLE B–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 257 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 257 illustrates where the encrypted `dsameuser` password is found in `serverconfig.xml`.

EXAMPLE B–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 260 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 259. 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 259, "User Element" on page 259, "BaseDN Element" on page 260 and "MiscConfig Element" on page 260. 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 261.

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 257 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 258 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 B–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 B–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 259“Server Element” on page 259 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 261 illustrates `serverconfig.xml` with automatic failover configuration.

EXAMPLE B–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 B–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>
```

APPENDIX C

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 2005Q4 Technical Overview*.

TABLE C–1 Log Reference for amAdmin Command line utility

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
1	INFO	Unsuccessful login for user.	user id	Unsuccessful login for user.	
2 TEST	INFO	ADMIN EXCEPTION Received	element name*error message*	Received ADMIN EXCEPTION while processing Admin request(s).	Look in amAdmin debug file for more information.
3	INFO	Session destroyed	name of user	Session destroyed.	
11	INFO	Service Schema Loaded	schema name	Successfully loaded service schema.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
31	INFO	Add Resource Bundle of Locale to Directory Server	resource bundle name*resource locale*	Resource Bundle of Locale successfully stored in Directory Server.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
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.	
45	INFO	Modified Sub Configuration of service	name of sub configuration *name of service*	Successfully modified sub configuration of service.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 Sub Configuration in Organization	sub configuration name *service nameorganization DN*	Successfully Modified Service Sub Configuration in Organization.	
92	INFO	Added Service Sub Configuration in Organization	sub configuration name*service nameorganization DN*	Successfully Added Service Sub Configuration in Organization.	
93	INFO	Deleted Service Sub Configuration in Organization	sub configuration name*service nameorganization DN*	Successfully Deleted Service Sub Configuration in Organization.	
94	INFO	Created remote provider in organization	provider name *organization DN*	Successfully created remote provider in organization.	
95	INFO	Modified remote provider in organization	provider name *organization DN*	Successfully modified remote provider in organization.	
96	INFO	Modified hosted provider in organization	provider name *organization DN*	Successfully modified hosted provider in organization.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 organization.	
102	INFO	Attempt to modify service template	DN of service template	Attempted to modify service template.	
103	INFO	Modified service template	DN of service template	Successfully modified service template.	
104	INFO	Attempt to remove service template	DN of service template	Attempted to remove service template.	
105	INFO	Removed service template	DN of service template	Successfully removed service template.	
106	INFO	Attempt to add service template	DN of service template	Attempted to add service template.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	DN of entity	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	Attempted to create role.	
115	INFO	Created role	name of role	Created role.	
116	INFO	Attempt to create group container	name of group container	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	Attempted to create group.	
119	INFO	Create group.	name of group	Created group.	
120	INFO	Attempt to create people container.	DN of people container	Attempted to create people container.	
121	INFO	Create people container.	DN of people container	Created people container.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
122	INFO	Attempt to create service template in organization or role	name of service template*name of organization or role*	Attempted to create service template in organization or role.	
123	INFO	Create service template in organization or role	name of service template*name of organization or role*	Created service template in organization or role.	
124	INFO	Attempt to create container	name of container	Attempted to create container.	
125	INFO	Create container	name of container	Created container.	
126	INFO	Attempt to create user.	name of user	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.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
136	INFO	Attempt to delete container.	name of container	Attempted to delete container.	
137	INFO	Delete container.	name of container	Deleted container.	
138	INFO	Attempt to modify entity	localized name of entity*DN of entity*	Attempted to modify entity.	
139	INFO	Modify entity	localized name of entity*DN of entity*	Modified entity.	
140	INFO	Attempt to modify people container.	DN of people container	Attempted to modify people container.	
141	INFO	Modify people container.	DN of people container	Modified people container.	
142	INFO	Attempt to modify container.	name of container	Attempted to modify container.	
143	INFO	Modify container.	name of container	Modified container.	
144	INFO	Attempt to register service under organization.	name of service*name of organization*	Attempted to register service under organization	
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 C–1 Log Reference for amAdmin Command line utility *(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 totype of identity to add to name of realm*	Attempted to add an Identity to an Identity in a Realm.	
202	INFO	Add an Identity to an Identity in a Realm	name of identity to add*type of identity to add name of identity to add totype of identity to add to name of realm*	Added an Identity to an Identity in a Realm.	

TABLE C–1 Log Reference for amAdmin Command line utility (Continued)

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
203	INFO	Attempt to assign service to an identity in a realm.	name of service*name of identitytype 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 identitytype 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 identityname 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 identityname of realm*	Created identity of a type in a realm.	
209	INFO	Attempt to delete identity of a type in a realm	name of identity*type of identityname 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 identityname 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 identityname of identity name of realm*	Attempted to modify a service for an Identity in a Realm.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
212	INFO	Modify a service for an Identity in a Realm	name of service*type of identityname 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 fromtype 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 fromtype of identity to remove from name of realm*	Removed an Identity from an Identity in a Realm.	
215	INFO	Attempt to set Service Attributes for an Identity in a Realm	name of service*type of identityname 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 identityname 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 identityname of identity name of realm*	Attempted to unassign a service from an Identity in a Realm.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
218	INFO	Unassign a service from an Identity in a Realm	name of service*type of identityname of identity name of realm*	Unassigned a service from an Identity in a Realm.	
219	INFO	Attempt to create organization	name of organization	Attempted to create an organization.	
220	INFO	Create organization	name of organization	Created an organization.	
221	INFO	Attempt to delete sub organization.	name of sub organization	Attempted to delete sub organization.	
222	INFO	Delete sub organization.	name of sub organization	Deleted sub organization.	
223	INFO	Attempt to modify role	name of role	Attempted to modify role.	
224	INFO	Modify role	name of role	Modified role.	
225	INFO	Attempt to modify sub organization.	name of sub organization	Attempted to modify sub organization.	
226	INFO	Modify sub organization.	name of sub organization	Modified sub organization.	
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 servicename 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 servicename of realm*	Added values to a Service Attribute in a Realm.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
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.	
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 servicename 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 servicename 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 servicename of realm*	Attempted to remove values from a service's attribute in a Realm.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
244	INFO	Remove values from a service's attribute in a Realm	name of attribute*name of servicename of realm*	Removed values from a service's attribute in a Realm.	
245	INFO	Attempt to set attributes for a service in a Realm.	name of service*name of realm*	Attempted to set attributes for a service in a Realm.	
246	INFO	Set attributes for a service in a Realm.	name of service*name of realm*	Set attributes for a service in a Realm.	
247	INFO	Attempt to unassign a service from a Realm.	name of service*name of realm*	Attempted to unassign a service from a Realm.	
248	INFO	Unassign a service from a Realm.	name of service*name of realm*	Unassigned a service from a Realm.	
249	INFO	Attempt to assign a Service to an Organization Configuration	name of service*name of realm*	Attempted to assign a Service to an Organization Configuration.	
250	INFO	Assign a Service to an Organization Configuration	name of service*name of realm*	Assigned a Service to an Organization Configuration.	
251	INFO	Assign a Service to an Organization Configuration Not Done	name of service*name of realm*	Assigned a Service to an Organization Configuration, but the service is not one of the org config's assignable services.	

TABLE C–1 Log Reference for amAdmin Command line utility *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
252	INFO	Assign a Service to a Realm Not Done	name of service*name of realm*	Assigned a Service to a Realm, but the service is not one of the realm's assignable services.	
253	INFO	Attempt to unassign a service from an Organization Configuration.	name of service*name of realm*	Attempted to unassign a service from an Organization Configuration.	
254	INFO	Unassign a service from an Organization Configuration.	name of service*name of realm*	Unassigned a service from an Organization Configuration.	
255	INFO	Unassign a service not in the Organization Configuration or Realm.	name of service*name of realm*	Requested to unassign a service not in the Organization Configuration or Realm.	
256	INFO	Attempt to modify a service in an Organization Configuration.	name of service*name of realm*	Attempted to modify a service in an Organization Configuration.	
257	INFO	Modify a service in an Organization Configuration.	name of service*name of realm*	Modified a service in an Organization Configuration.	
258	INFO	Modify a service not in the Organization Configuration or Realm.	name of service*name of realm*	Attempted to modify a service not in the Organization Configuration or Realm.	

TABLE C–2 Log Reference 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 typeuser name*	User authenticated with valid credentials	
102	INFO	Role based authentication is successful	message *authentication typerole name*	User belonging to role authenticated with valid credentials	
103	INFO	Service based authentication is successful	message *authentication typeservice name*	User authenticated with valid credentials to a configured service under realm	
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 typemodule name*	User authenticated with valid credentials to authentication module under realm	

TABLE C–2 Log Reference for Authentication *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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.

TABLE C–2 Log Reference for Authentication *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
213	INFO	User based authentication failed	error message *authentication typeuser 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 typeuser name*	User based Auth. Invalid credentials entered.	Enter the correct password.
215	INFO	Authentication Failed	error message *authentication typeuser name*	Named Configuration (Auth Chain) does not exist for this user	Create and configure a named config for this user

TABLE C–2 Log Reference for Authentication *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
216	INFO	Authentication Failed	error message *authentication typeuser 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 typeuser name*	User based Auth. This user is not active.	Activate the user.
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.

TABLE C–2 Log Reference for Authentication *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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 typerole name*	Role based Auth. Invalid credentials entered.	Enter the correct password.
228	INFO	Authentication Failed	error message *authentication typerole name*	Named Configuration (Auth Chain) does not exist for this role.	Create and configure a named config for this role.

TABLE C–2 Log Reference for Authentication *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
229	INFO	Authentication Failed	error message *authentication typerole 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.
230	INFO	Authentication Failed	error message *authentication typerole name*	Role based Auth. This user is not active.	Activate the user.
231	INFO	Authentication Failed	error message *authentication typerole name*	Role based Auth. Max number of failure attempts exceeded. User is Locked out.	Contact system administrator.
232	INFO	Authentication Failed	error message *authentication typerole name*	Role based Auth. User account has expired.	Contact system administrator.
233	INFO	Authentication Failed	error message *authentication typerole name*	Role based Auth. Login timed out.	Try to login again.
234	INFO	Authentication Failed	error message *authentication typerole name*	Role based Auth. Authentication module is denied.	Configure this module or use some other module.
235	INFO	Authentication Failed	error message *authentication typerole 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 C–2 Log Reference for Authentication *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
237	INFO	Authentication Failed	error message *authentication typerole name*	Role based auth. Org/Realm is not active.	Activate the Org/Realm.
238	INFO	Authentication Failed	error message *authentication typerole 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 typerole 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 typeservice 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 typeservice name*	Named Configuration (Auth Chain) does not exist with this service name.	Create and configure a named config.

TABLE C–2 Log Reference for Authentication *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
243	INFO	Authentication Failed	error message *authentication typeservice 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 typeservice 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 C–2 Log Reference 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.
254	INFO	Authentication level based authentication failed	error message *authentication type* *authentication level value*	There are no authentication module(s) having authentication level value greater than or equal to specified authentication level *Incorrect/invalid credentials presented to one or more authentication modules having authentication level greater than or equal to specified authentication levelUser locked out/not active*	Configure one or more authentication modules having authentication level value greater than or equal to required authentication level*Enter correct/valid credentials to one or more authentication modules having authentication level greater than or equal to specified authentication level*

TABLE C–2 Log Reference for Authentication *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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.

TABLE C–2 Log Reference for Authentication *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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 presentedUser locked out/not active*	Register/configure authentication module under realm*Enter correct/valid credentials to authentication module*

TABLE C–2 Log Reference 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 messag e*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 C–2 Log Reference 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 C–2 Log Reference 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	

TABLE C–3 Log Reference for the Access Manager 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.	
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
11	INFO	Attempt to search for Identities	base realm*identity typesearch pattern search size limitsearch time limit*	Click on Search button in identity search view.	
12	INFO	Searching for Identities succeeded	base realm*identity typesearch pattern search size limitsearch time limit*	Click on Search button in identity search view.	
13	SEVERE	Searching for identities failed	identity name*identity typerealm 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 typerealm 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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
23	SEVERE	Reading of attribute values of an identity failed	identity name*name of attributeserror 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 attributeserror message*	Unable to read attribute values of an identity due to data store error.	Look under data store log for more information.
25	SEVERE	Reading of attribute values of an identity failed	identity name*name of attributeserror 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 attributeserror 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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
53	SEVERE	Reading of identity's memberships information failed.	name of identity *membership identity typeerror 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 typeerror message*	Unable to read identity's memberships information due to data store error.	Look under data store log for more information.
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
133	SEVERE	Reading of service attribute values of an identity failed.	name of identity*name of serviceerror 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 serviceerror 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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
213	SEVERE	Writing of global service default attribute values failed.	name of service*name of attributeerror 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 attributeerror 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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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 deletederror 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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
234	SEVERE	Deletion of sub configuration failed.	name of service *name of base global sub configuration* *name of sub configuration to be deletederror message*	Unable to delete sub configuration due to service management error.	Look under service management log for more information.
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 C–3 Log Reference for the Access Manager 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.
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
313	SEVERE	Creation of policy failed.	name of realm*name of policyerror 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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
314	SEVERE	Creation of policy failed.	name of realm*name of policyerror 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 policyerror 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 policyerror 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.	
332	INFO	Deletion of policy succeeded	name of realm*name of policies*	Click on Delete button in policy main page.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
333	SEVERE	Deletion of policy failed.	name of realm*name of policieserror 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 policieserror 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.	
413	SEVERE	Creation of realm failed.	name of parent realm*name of new realmerror 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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 C–3 Log Reference for the Access Manager 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 privilegeID of subject*	Click on Save button in delegation subject profile page.	
522	INFO	Modification of delegation privilege succeeded.	name of realm*ID of delegation privilegeID of subject*	Click on Save button in delegation subject profile page.	
523	SEVERE	Modification of delegation privilege failed.	name of realm*ID of delegation privilegeID 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 C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
524	SEVERE	Modification of delegation privilege failed.	name of realm*ID of delegation privilegeID of subjecterror 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 C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
613	SEVERE	Getting attribute values of data store failed.	name of realm*name of identity repositoryerror 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 repositoryerror 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 repositorytype 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 repositorytype 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 repositorytype of identity repositoryerror 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
643	SEVERE	Modification of data store failed.	name of realm*name of identity repositoryerror 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 repositoryerror 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 serviceerror 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 serviceerror 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 serviceerror message*	Unable to unassign service from realm due to data store management SDK exception.	Look under data store management log for more information.

TABLE C–3 Log Reference for the Access Manager 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 serviceerror 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 serviceerror 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 serviceerror 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 servicename 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 servicename of attribute schema*	View realm's service profile page.	

TABLE C–3 Log Reference for the Access Manager 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 servicename of attribute schemaerror 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 servicename of attribute schemaerror 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 servicename of attribute schemaerror 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 serviceerror message*	Unable to modify attribute values of service due to service management SDK exception.	Look under service management log for more information.

TABLE C–3 Log Reference for the Access Manager 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 serviceerror 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 serviceerror 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 C–3 Log Reference for the Access Manager 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.	
833	SEVERE	Creation of authentication instance under a realm failed.	name of realm*name of authentication instance type of authentication instanceerror message*	Unable to create authentication instance due to authentication configuration exception.	Look under authentication configuration log for more information.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 serviceerror 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 serviceerror 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.	
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
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 typeerror 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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 domain*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.	
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 providertype of provider*	Click on Save button in provider assignment page.	
1302	INFO	Creation of providers succeeded.	name of provider*role of providertype of provider*	Click on Save button in provider assignment page.	
1303	SEVERE	Creation of provider failed.	name of provider*role of providertype 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 providertype 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 providertype 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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
1334	SEVERE	Modification of provider failed.	name of provider*role of providererror 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.	
1343	SEVERE	Deletion of provider failed.	name of provider*role of providererror 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 providererror 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 typename of attribute schemas*	View service profile page.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
2002	INFO	Getting attribute values of schema type of a service schema succeeded.	name of service*name of schema typename of attribute schemas*	View service profile page.	
2003	SEVERE	Getting attribute values of schema type of a service schema failed.	name of service*name of schema typename of attribute schemaserror 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 typename of attribute schemaserror 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 typename 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 typename of attribute schemas*	View service profile page.	

TABLE C–3 Log Reference for the Access Manager 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 typename 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 typename of attribute schemaserror 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 typename of attribute schemaserror 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 typename 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 typename of attribute schemas*	Click on Save button in service profile page.	

TABLE C–3 Log Reference for the Access Manager 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 typename of attribute schemaserror 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 typename of attribute schemaserror 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 stylesearch pattern*	View client profile page.	
2502	INFO	Getting device names of client detection service succeeded.	name of profile*name of stylesearch 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 realmerror 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 sessionerror 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 C–3 Log Reference for the Access Manager 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 patternerror 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 patternerror message*	Unable to search for containers due to access management SDK exception.	Look under access management SDK log for more information.

TABLE C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
10033	SEVERE	Creation of container under an container failed.	DN of container*Name of containererror 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 containererror 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 C–3 Log Reference for the Access Manager 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 serviceType of template*	View container's service profile page.	
10112	INFO	Getting service template under a container succeeded.	DN of container*Name of serviceType of template*	View container's service profile page.	
10113	SEVERE	Getting service template under a container failed.	DN of container*Name of serviceType 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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
10114	SEVERE	Getting service template under a container failed.	DN of container*Name of serviceType 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.	
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.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 serviceerror 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.	
10153	SEVERE	Deletion of service from container failed.	DN of container*Name of serviceerror 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 for more information.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
10154	SEVERE	Deletion of service from container failed.	DN of container*Name of serviceerror 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.
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.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 patternerror 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 patternerror 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.	
10222	INFO	Searching for group containers under group container succeeded.	DN of group container*Search pattern*	Click on Search button in group container's group containers page.	

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
10223	SEVERE	Searching for group containers under group container failed.	DN of group container*Search patternerror 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 patternerror 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.
10234	SEVERE	Creation of group container under organization failed.	DN of organization *Name of group container error message*	Unable to create group container due to access management SDK exception.	Look under access management SDK log for more information.

TABLE C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 containererror 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 containererror 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 patternerror 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 patternerror 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 patternerror 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 C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
10324	SEVERE	Searching for groups under static group failed.	DN of static group*search patternerror 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 patternerror 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 patternerror 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 grouperror 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 grouperror 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 grouperror 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 C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
10374	SEVERE	Creation of group under group container failed.	DN of group container*Name of grouperror 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 grouperror 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 grouperror 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 grouperror 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 patternerror 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 patternerror 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 C–3 Log Reference for the Access Manager 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 groupserror 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 groupserror message*	Unable to remove nested group due to access management SDK exception.	Look under access management SDK log for more information.

TABLE C–3 Log Reference for the Access Manager 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 userserror 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 userserror 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 patternerror 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 patternerror 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 C–3 Log Reference for the Access Manager 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 containererror 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 containererror message*	Unable to create for people container due to access management SDK exception.	Look under access management SDK log for more information.

TABLE C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 userserror 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 userserror 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager 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 patternerror 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 patternerror 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 patternView role's members page.*	View organization's roles page.	
10743	SEVERE	Getting roles in organization failed.	DN of role*Search patternerror 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 C–3 Log Reference for the Access Manager Console *(Continued)*

Id	Log Level	Description	Data	Triggers	Actions
10744	SEVERE	Getting roles in organization failed.	DN of role*Search patternerror 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 patternView role's members page.*	View container's roles page.	
10753	SEVERE	Getting roles in container failed.	DN of role*Search patternerror 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 patternerror 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 C–3 Log Reference for the Access Manager 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 roleerror 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 roleerror 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 C–3 Log Reference for the Access Manager 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 serviceerror 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 C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
10794	SEVERE	Removal of service from role failed.	DN of role*Name of serviceerror 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 serviceerror 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 serviceerror 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 C–3 Log Reference for the Access Manager 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 serviceerror 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 roleerror 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 roleName 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 C–3 Log Reference for the Access Manager 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 roleerror 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 roleName 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 C–3 Log Reference for the Access Manager 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 serviceerror 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 serviceerror 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 patternerror 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 C–3 Log Reference for the Access Manager 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 C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
10973	SEVERE	Creation of user failed.	DN of people container*Name of usererror 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 usererror 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 C–3 Log Reference for the Access Manager 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 serviceerror 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 serviceerror 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 C–3 Log Reference for the Access Manager 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 grouperror 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 grouperror 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 grouperror 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 C–3 Log Reference for the Access Manager Console *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
11024	SEVERE	Addition of group to user failed.	DN of user*DN of grouperror message*	Unable to add group due to access management SDK exception.	Look under access management SDK log for more information.

TABLE C–4 Log Reference 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 Afliation	afliation id	Deleted Affiliation	
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 Afliation	afliation id	Modified Afliation	
11	INFO	Modify Provider	provider id	Modified Provider	
12	INFO	Create Entity	entity id	Created Entity	
13	INFO	Create Affiliation	afliation id	Created Affiliation	

TABLE C–4 Log Reference for Federation *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
14	INFO	Write Account Federation Info	user DN*federation info keyfederation info value*	Acccount Federation Info with key was added to user	
15	INFO	Remove Account Federation Info	user DN*provider idexisting 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.	
22	INFO	Wrong Authentication type	authentication type	Wrong Authentication type	

TABLE C–4 Log Reference for Federation *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 :	
36	INFO	Common Domain Service Information not found	message	Common Domain Service Information not found.	

TABLE C–4 Log Reference for Federation *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 SPProvided NameIdentifier.	message	Failed to create SPProvided NameIdentifier.	
48	INFO	Invalid Signature.	message	Invalid Signature.	
49	INFO	Federation Termination failed.	user name	Federation Termination failed. Cannot update account.	

TABLE C–4 Log Reference 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.	

TABLE C–5 Log Reference 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.	
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	

TABLE C–5 Log Reference for Liberty *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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	
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	

TABLE C–5 Log Reference for Liberty *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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 idcache 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.	

TABLE C–6 Log Reference for Policy

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
1	INFO	Evaluating policy succeeded	policy name*realm nameservice type name resource nameaction namespolicy decision*	Evaluating policy.	
2	INFO	Getting protected policy resources succeeded	principal name*resource nameprotecting policies*	Getting protected policy resources.	

TABLE C–6 Log Reference for Policy *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.
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 nameresource name policy decision*	Computing policy decision by an administrator.	

TABLE C–6 Log Reference for Policy *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
11	INFO	Computing policy decision by an administrator ignoring subjects succeeded	admin name*resource namepolicy decision*	Computing policy decision by an administrator ignoring subjects.	

TABLE C–7 Log Reference 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 ArtifactID 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 C–7 Log Reference 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 C–7 Log Reference 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 C–7 Log Reference 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 C–7 Log Reference 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 C–7 Log Reference 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 C–7 Log Reference for SAML *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
32	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.

TABLE C–8 Log Reference for Session

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
1	INFO	Session is Created	User ID	User is authenticated.	
2	INFO	Session has idle timedout	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	
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	

TABLE C–8 Log Reference for Session *(Continued)*

Id	*Log Level*	*Description*	*Data*	*Triggers*	*Actions*
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.	

APPENDIX D

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 399
- "Authentication Error Codes" on page 401
- "Policy Error Codes" on page 404
- "amadmin Error Codes" on page 406

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 D–1 Access Manager Console Errors

Error Message	Description/Probable Cause	Action
An error has occurred while deleting the following:	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 D–1 Access Manager Console Errors *(Continued)*

Error Message	Description/Probable Cause	Action
You have entered an invalid URL	This occurs if the URL for an Access Manager console window is entered incorrectly.	
There are no entries matching the search criteria.	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	
Search size limit exceeded. Please refine your search.	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.
Search time limit exceeded. Please refine your search.	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	In the User Profile page, change the value of the start DN to a valid DN.
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 D–2 Authentication Error Codes

Error Message	Description/Probable Cause	Action
authentication.already.login.	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.
uncaught_exception	An authentication Exception is thrown due to an incorrect handler	Check the Login URL for any invalid or special characters.
redirect.error	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	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.
auth.failed	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.)
nouser.profile	No user profile was found matching the 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.

TABLE D–2 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
notenough.characters	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).
useralready.exists	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.
uidpasswd.same	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.
nouser.name	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	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.confirm.passwd	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.
password.mismatch	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.	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.

TABLE D–2 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
orginactive	This organization is not active.	Activate the organization through the Access Manager console by changing the organization status from `inactive` to `active`.
internal.auth.error	Internal Authentication Error. This is a generic Authentication error which may be caused by different and multiple environmental and/or configuration issues.	
usernot.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.not.inrole	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.
session.timeout	The user session has timed out.	Login in again.
authmodule.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.
noconfig.found	No configuration found.	Check the Authentication Configuration service for the required authentication method.
cookie.notpersistent	Persistent Cookie Username does not exist in the Persistent Cookie Domain.	
nosuch.domain	The organization found.	Make sure that the requested organization is valid and correct.

TABLE D–2 Authentication Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
userhasnoprofile.org	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.
reqfield.missing	One of the required fields was not completed. Please make sure all required fields are entered.	Make sure that all required fields are entered.
session.max.limit	Maximum Sessions Limit 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 D–3 Policy Error Codes

Error Message	Description/Probable Cause	Action
illegal_character_/_in_name	Illegal character "/" in the policy name.	Make sure that the policy name does not contain the "/' character.
policy_already_exists_in_org	A rule with the same name already exists.	Use a different name for policy creation.
rule_name_already_present	Another rule with the given name already exists	Use a different rule name for policy creation.
rule_already_present	A rule with the same rule value already exists.	Use a different rule value.
no_referral_can_not_create_policy	No referral exists to the organization.	In order to create policies under a sub organization, you must create a referral policy at its parent organization to indicate what resources can be referred to this sub organization.
ldap_search_exceed_size_limit	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.The Search Size Limit is located in the Policy Configuration service.

TABLE D–3 Policy Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
ldap_search_exceed_time_limit	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.
ldap_invalid_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.
app_sso_token_invalid	Application SSO token is invalid.	The server could not validate the Application SSO token. Most likely the SSO token is expired.
user_sso_token_invalid	User SSO token is invalid.	The server could not validate the User SSO token. Most likely the SSO token is expired.
property_is_not_an_Integer	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_can_not_be_greater_than_end_ip	Start IP is larger than End IP	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_can_not_be_larger_than_end_date	Start Date is larger than End Date	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_organization	Policy not found in organization. An error occurred trying to locate a non-existing policy in an organization.	Make sure that the policy exists under the specified organization.
insufficient_access_rights	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.

TABLE D–3 Policy Error Codes *(Continued)*

Error Message	Description/Probable Cause	Action
invalid_ldap_server_host	Invalid LDAP Server host.	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 D–4 amadmin error codes

Error Message	Code	Description/Probable Cause	Action
nocomptype	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.
file	2	The input XML file was not found.	Check the syntax and make sure that the input XML is valid.
nodnforadmin	3	The user DN for the `--runasdn` value is missing.	Provide the user DN as the value for `--runasdn`.
noservicename	4	The service name for the `--deletservice` value is missing.	Provide the service name as the value for `--deleteservice`.
nopwdforadmin	5	The password for the `--password` value is missing.	Provide the password as the value for `--password`.
nolocalename	6	The locale name was not provided. The locale will default to en_US.	See the Online Help for a list of locales.
nofile	7	Missing XML input file.	Provide at least one input XML filename to process.
invopt	8	One or more arguments are incorrect.	Check that all arguments are valid. For a set of valid arguments, type `amadmin --help`.

TABLE D–4 amadmin error codes *(Continued)*

Error Message	Code	Description/Probable Cause	Action
oprfailed	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.
execfailed	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.
policycreatexception	12	Policy cannot be created.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
policydelexception	13	Policy cannot be deleted.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
smsdelexception	14	Service cannot be deleted.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
ldapauthfail	15	Cannot authenticate user.	Make sure the user DN and password are correct.
parserror	16	Cannot parse the input XML file.	Make sure that the XML is formatted correctly and adheres to the `amAdmin.dtd`.
parseiniterror	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`.
parsebuilterror	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.
ioexception	19	Cannot read the input XML file.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.

TABLE D–4 amadmin error codes *(Continued)*

Error Message	Code	Description/Probable Cause	Action
fatalvalidationerror	20	Cannot parse because the XML file is not a valid file.	Check the syntax and make sure that the input XML is valid.
nonfatalvalidationerror	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.
validwarn	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.
failedToProcessXML	23	Cannot process the XML file.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
nodataschemawarning	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`.
doctyperror	25	The XML file does not follow the correct DTD.	Check the XML file for the `DOCTYPE` element.
statusmsg9	26	LDAP Authentication failed due to invalid DN, password, hostname, or portnumber.	Make sure the user DN and password are correct.
statusmsg13	28	Service Manager exception (SSO exception).	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
statusmsg14	29	Service Manager exception.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
statusmsg15	30	Schema file inputstream exception.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
statusmsg30	31	Policy Manager exception (SSO exception).	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.

TABLE D–4 amadmin error codes *(Continued)*

Error Message	Code	Description/Probable Cause	Action
statusmsg31	32	Policy Manager exception.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
dbugerror	33	More than one debug option is specified.	Only one debug option should be specified.
loginFalied	34	Login failed.	`amadmin` produces exception messages to indicate the specific error. Refer to those messages to evaluate the problem.
levelerr	36	Invalid attribute value.	Check the level set for the LDAP search. It should be either `SCOPE_SUB` or `SCOPE_ONE`.
failToGetObjType	37	Error in getting object type.	Make sure that the DN in the XML file is value and contains the correct object type.
invalidOrgDN	38	Invalid organization DN.	Make sure that the DN in the XML file is valid and is an organization object.
invalidRoleDN	39	Invalid role DN.	Make sure that the DN in the XML file is valid and is a role object.
invalidStaticGroupDN	40	Invalid static group DN.	Make sure that the DN in the XML file is valid and is a static group object.
invalidPeopleContainerDN	41	Invalid people container DN.	Make sure the DN in the XML file is valid and is a people container object.
invalidOrgUnitDN	42	Invalid organizational unit DN.	Make sure that the DN in the XML file is valid and is a container object.
invalidServiceHostName	43	Invalid service host name.	Make sure that the hostname for retrieving valid sessions is correct.
subschemaexception	44	Subschema error.	Subcschema is only supported for global and organization attributes.

TABLE D–4 amadmin error codes *(Continued)*

Error Message	Code	Description/Probable Cause	Action
serviceschemaexception	45	Cannot locate service schema for service.	Make sure that the sub schema in the XML file is valid.
roletemplateexception	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.
cannotAddusersToFileredRole	47	Cannot add users to a filtered role.	Made sure that the role DN in the XML file is not a filtered role.
templateDoesNotExist	48	Template does not exist.	Make sure that the service template in the XML file is valid.
cannotAdduUersToDynamicGroup	49	Cannot add users to a dynamic group.	Made sure that the group DN in the XML file is not a dynamic group.
cannotCreatePolicyUnderContainer	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.
defaultGroupContainerNotFound	51	The group container was not found.	Create a group container for the parent organization or container.
cannotRemoveUserFromFilteredRole	52	Cannot remove a user from a filtered role.	Make sure that the role DN in the XML file is not filtered role.
cannotRemoveUsersFromDynamicGroup	53	Cannot remove users from a dynamic group.	Make sure that the group DN in the XML file is not a dynamic group.
subSchemStringDoesNotExist	54	The subschema string does not exist.	Make sure that the subschema string exists in the XML file.
defaultPeopleContainerNotFound	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.
nodefaulturlprefix	60	Default URL prefix is not found following --defaultURLPrefix argument	provide the default URL prefix accordingly.
nometaalias	61	Meta Alias is not found following --metaalias argument	provide the Meta Alias accordingly.
missingEntityName	62	Entity Name is not specified.	provide the entity name.

TABLE D–4 amadmin error codes *(Continued)*

Error Message	Code	Description/Probable Cause	Action
missingLibertyMetaInputFile	63	File name for importing meta data is missing.	provide the file name that contains meta data.
missingLibertyMetaOutputFile	64	File name for storing exported meta data is missing.	provide the file name for storing meta data.
cannotObtainMetaHandler	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.
missingResourceBundleName	66	Missing resource bundle name when adding, viewing or deleting resource bundle that is store in directory server.	provide the resource bundle name
missingResourceFileName	67	Missing file name of file that contains the resource strings when adding resource bundle to directory server.	Please provide a valid file name.
failLoadLibertyMeta	68	Failed to load liberty meta to Directory Server.	Please check the meta data again before loading it again

Index

A

access logs, 201
Access Manager SDK, deploying, 23
account locking
  memory, 121-122
  physical, 121-122
AM_ENC_PWD variable, 36
am.encryption.pwd property, 36
am2bak command line tool, 219-222
  Syntax, 219-222
amadmin command line tool, 207
  Syntax, 208-211
AMConfig.properties, 233-255
  overview, 234
AMConfig.properties file, 36
amconfig script
  deployment scenarios, 35
  operations for, 23
  syntax for, 34
ampassword command line tool, 215-216
amsamplesilent file, 22
amsecuridd helper, 34
amsecuridd Helper, Syntax, 228
amserver command line tool, 223
  Syntax, 223
amserver.instance script, 34
amserver script, 34
amunixd helper, 34
Application Server
  configuration variables, 30
  support for, 30
arg login URL parameter, 118
authentication
  account locking
    memory, 121-122
    physical, 121-122
Authentication, By Module, 112-113
authentication
  FQDN mapping, 123-124
  login URLs
    organization-based, 96, 99
    role-based, 102
    service-based, 104-105
    user-based, 107
  methods
    organization-based, 98-101
    policy-based, 154-155
    realm-based, 96-98
    role-based, 101-104
    service-based, 104-107
    user-based, 107-109
  multiple LDAP configurations, 124-127
  persistent cookies, 124
  redirection URLs
    authentication level-based, 110-111
    organization-based, 97-98, 99-100
    role-based, 102-104
    service-based, 105-107
    user-based, 107-109
  session upgrade, 127
  user interface
    login URL, 114-120
    login URL parameters, 114-120
  validation plug-in interface, 128

Authentication Configuration
  For Organizations, 98, 100-101
authentication level-based redirection URLs, 110-111
authlevel login URL parameter, 119

B

bak2am command line tool, 217-218
  Syntax, 217-218
BEA WebLogic Server, support for, 23

C

Command line tools
  am2bak, 219-222
    Syntax, 219-222
  amadmin, 207
    Syntax, 208-211
  ampassword, 215-216
  amsecuridd Helper
    Syntax, 228
  amserver, 223
    Syntax, 223
  bak2am, 217-218
    Syntax, 217-218
  VerifyArchive, 225-226, 227-229
    Syntax, 225-226
Conditions
  Authentication Level, 136
  Authentication Scheme, 137
  IP Address, 137
configuration variables
  Access Manager, 23
  Application Server, 30
  IBM WebSphere Server, 32
  Web Server, 29
Configure Later option, Java Enterprise System installer, 21
Configure Now option, Java Enterprise System installer, 21
console
  user interface
    login URL, 114-120
console, user interface *(Continued)*
    login URL parameters, 114-120
Containers, 170-171
  Creating, 170
  Deleting, 170-171
Current Sessions
  Interface, 187-188
  Session Management
    Terminating a Session, 188
  Session Management Window, 187

D

Data Stores, 71
  LDPAv3 repository plug-in attributes, 72
  To create a new Access Manager repository plug-in, 78
  To create a new LDAPv3 data store, 72
debug files, 202-204
DEPLOY_LEVEL variable, 24
deployment scenarios, Access Manager, 35
Directory Management, 167
domain login URL parameter, 119
DTD files
  policy.dtd, 139-143
  server-config.dtd, 258-261

E

error logs, 201

F

failover configuration, in serverconfig.xml, 261-262
Federation Management module, deploying, 23
FQDN mapping, and authentication, 123-124

G

goto login URL parameter, 115
gotoOnFail login URL parameter, 115

Group Containers, 171
  Creating, 171
  Deleting, 171
Groups, 172-175
  Adding to a Policy, 175
  Create a Managed Group, 173
  Membership by Filter, 172
  Membership by Subscription, 172

I

IBM WebSphere, support for, 23
Identity Management, 167-186
  Containers, 170-171
    Creating, 170
    Deleting, 170-171
  Group Containers, 171
    Creating, 171
    Deleting, 171
  Groups, 172-175
    Adding to a Policy, 175
    Create a Managed Group, 173
    Membership by Filter, 172
    Membership by Subscription, 172
  Organizations, 167-170
    Adding to a Policy, 170
    Creating, 168-169
    Deleting, 169-170
  People Containers, 175-176
    Creating, 175
    Deleting, 175-176
  Roles, 179-186
    Adding to a Policy, 186
    Adding Users to, 182-183
    Creating, 180-182
    Removing Users from, 185
  Users, 176-179
    Adding to a Policy, 179
    Adding to Services, Roles and Groups, 158, 179
    Creating, 176
Identity Server, installation overview, 21
IDTokenN login URL parameter, 119-120
installation directory, Access Manager, 22
installer, Java Enterprise System, 21
instance, new Access Manager, 35
iPSPCookie login URL parameter, 119

J

Java Enterprise System installer, 21, 35

L

LDAP authentication, multiple configurations, 124-127
Linux systems, base installation directory for, 22
locale login URL parameter, 117-118
logging
  access logs, 201
  component log filenames, 201
  error logs, 201
  flat file format, 201
login URLs
  organization-based, 96, 99
  role-based, 102
  service-based, 104-105
  user-based, 107

M

Managing Access Manager Objects, 167-186
methods
  authentication
    organization-based, 96-98, 98-101
    policy-based, 154-155
    role-based, 101-104
    service-based, 104-107
    user-based, 107-109
module login URL parameter, 118

N

naming service, and policy, 133
new installation, Access Manager, 21
Normal Policy, 134-139

Normal Policy *(Continued)*
  Modifying, 147-150

O

operations, using amconfig, 23
org login URL parameter, 115-116, 116
organization-based authentication, 96-98, 98-101
organization-based login URLs, 96, 99
organization-based redirection URLs, 97-98, 99-100
Organizations, 167-170
  Adding to a Policy, 170
  Creating, 168-169
  Deleting, 169-170
overview
  AMConfig.properties, 234
  authentication
    login URL, 114-120
  policy, 131-132
  policy agents, 132-133
  policy process, 133-134
  user interface
    login URL parameters, 114-120
overview, Access Manager installation, 21
owner and group, changing, 37

P

password encryption key, 36
People Containers, 175-176
  Creating, 175
  Deleting, 175-176
persistent cookies, and authentication, 124
Policies
  To add a condition to, 149
  To add a response provider to, 150, 152
  To add a rule to, 147, 150
  To add a subject to, 148
  To create a new referral policy, 145
Policy, 131-155
policy
  and naming service, 133
Policy
  Creating for Peer and Suborganizations, 146
policy
  DTD files
    policy.dtd, 139-143
Policy
  Normal Policy, 134-139
    Modifying, 147-150
policy
  overview, 131-132
  policy-based resource management (authentication), 154-155
  process overview, 133-134
Policy
  Referral Policy, 139
  To add referrals to, 151-152
policy agents, overview, 132-133
policy-based resource management (authentication), 154-155
policy configuration service, 153
policy.dtd, 139-143
Privileges, 70

R

Realms, 67
  Authentication, 68
  Data Stores, 71
  General Properties, 68
  Privileges, 70
  Services, 69
  Subjects, 157
  To add a service to, 69
  To create a new, 67
  To create a new authentication chain, 92
  To create a new authentication module, 92
reconfiguring Access Manager instance, 37
redirection URLs
  authentication level-based, 110-111
  organization-based, 97-98, 99-100
  role-based, 102-104
  service-based, 105-107
  user-based, 107-109
Referral Policy, 139

related JES product documentation, 15
role-based authentication, 101-104
role-based login URLs, 102
role-based redirection URLs, 102-104
role login URL parameter, 117
Roles, 179-186
  Adding to a Policy, 186
  Adding Users to, 182-183
  Creating, 180-182
  Removing Users from, 185

S

server-config.dtd, 258-261
serverconfig.xml, 257-262
  and failover, 261-262
service-based authentication, 104-107
service-based login URLs, 104-105
service-based redirection URLs, 105-107
service login URL parameter, 118
services, policy, 131-132
session upgrade, and authentication, 127
silent mode input file, amconfig script, 22
Solaris systems, base installation directory for, 22
SSL, Configuring Access Manager For, 47-58
state file, Java Enterprise System installer, 23
Subjects, 157
  Filtered Roles, 162
  Groups, 163
  User, 157

T

Terminating a Session, 188

U

un-install Access Manager instance, 38
unconfigure Access Manager instance, 38
user-based authentication, 107-109
user-based login URLs, 107
user-based redirection URLs, 107-109
user interface login URL, 114-120
user interface login URL parameters, 114-120
user login URL parameter, 116-117
Users, 176-179
  Adding to a Policy, 179
  Adding to Services, Roles, and Groups, 158, 179
  Creating, 176

V

validation plug-in interface, and authentication, 128
VerifyArchive command line tool, 225-226, 227-229
  Syntax, 225-226

W

WEB_CONTAINER variable, 28
Web Server
  configuration variables, 29
  support for, 29
WebLogic Server, support for, 23
WebSphere
  configuration variables, 32
  support for, 23

X

XML, serverconfig.xml, 257-262