

Sun Java System Federated Access Manager Integration Guide

Beta



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

Part No: 820-4729-06
August 2008

Copyright 2008 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

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

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

This distribution may include materials developed by third parties.

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

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

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

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

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

Copyright 2008 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

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

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

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

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

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

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

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

Contents

Preface	7
1 Integrating Sun Identity Manager	11
About the Deployment	11
About Sun Identity Manager	12
About Sun Directory Server	12
About Sun MySQL	13
Software Versions Used in the Deployment	13
Installing and Configuring MySQL	14
▼ To Install MySQL	14
▼ To Configure MySQL	17
Installing Identity Manager on Application Server	18
▼ To Install Application Server	18
▼ To Install Identity Manager on Application Server	18
▼ To Create Identity Manager Tables in MySQL	19
▼ To Configure the Application Server Data Source to Work with Identity Manager	20
▼ To Configure Identity Manager to Work with Application Server	21
▼ To Configure Application Server to Work with Identity Manager	24
Creating a Federated Access Manager Realm Administrator	27
▼ To Create a Federated Access Manager Realm Resource Object	27
Provisioning Identities from Identity Manager to Federated Access Manager	30
▼ To View Federated Access Manager Roles and Groups in Identity Manager	31
▼ To View Federated Access Manager User Accounts in Identity Manager	32
▼ To Provision a Test User From Identity Manager Into Federated Access Manager	33
▼ To Verify that Identities Were Successfully Provisioned	34
▼ To Provision a Test Role From Identity Manager Into Federated Access Manager	35
▼ To Verify the Test User Role Was Successfully Provisioned from Identity Manager Into Federated Access Manager	37

▼ To Provision an Admin-User From Identity Manager Into Federated Access Manager ...	37
▼ To Verify the Admin-User Was Successfully Provisioned from Identity Manager into Federated Access Manager	38
▼ To Provision an Admin-Role From Identity Manager Into Federated Access Manager	39
▼ To Verify the Test Admin Role Was Successfully Provisioned from Identity Manager Into Federated Access Manager	40
Installing And Configuring the Federated Access Manager Policy Agent on Identity Manager	41
▼ To Create the Federated Access Manager Agent Profile On The Federated Access Manager Server	41
▼ To Install the Federated Access Manager Policy Agent on the Identity Manager Server	42
▼ To Configure the Federated Access Manager Policy Agent on Federated Access Manager	43
▼ To Create Policies on Federated Access Manager	44
▼ To Disable Protection of Identity Manager Server by the Federated Access Manager Policy Agent	45
▼ To Configure The Federated Access Manager Policy Agent On Identity Manager Server .	46
Configuring Identity Manager for Single Sign-On	47
▼ To Configure Identity Manager Login Module Groups	48
▼ To Configure the Identity Manager User Login Interface	49
▼ To Configure the Identity Manager Admin Login Interface	49
Testing Single Sign-On from Federated Access Manager to Identity Manager	50
▼ To Re-Enable Protection Identity Manager Protection by the Federated Access Manager Policy Agent	52
▼ To Test End-User Single Sign-On Between Federated Access Manager and Identity Manager	53
▼ To Test Admin-User Single Sign-On Between Federated Access Manager and Identity Manager	54
Troubleshooting	54
▼ To Enable Trace in Identity Manager	54
To Inspect Log Files	55
To View or Change Identity Manager System Settings	55
▼ To Inspect an Identity Manager Object	56
To Update an Identity Manager Object	56
To Consult Forums and Mailing Lists	57
Sample Output	57

2	Integrating CA SiteMinder	87
	About CA SiteMinder	87
	Authentication and Authorization	88
	User Sessions	89
	Understanding the SiteMinder User Cases	89
	Simple Single Sign-On Use Case	90
	Federated Single Sign-On Use Cases	92
	Installing SiteMinder	99
	Configuring SiteMinder After Installation	100
	▼ To Log In to SiteMinder	100
	Creating a Sample User	100
	▼ To Create a SiteMinder Policy Agent Configuration	101
	▼ To Create and Configure the User Directory	103
	Creating and Configuring a Form-Based Authentication Scheme	106
	▼ To Create a Policy	107
	Using Federated Access Manager to Enable SiteMinder Federation in an Identity Provider Environment	109
	▼ To Install the Principal Components	109
	▼ To Configure the Identity Provider Federated Access Manager to Use SAMLv2 Identity Provider Protocols	112
	▼ To Configure the SiteMinder Agent to Protect Federated Access Manager URLs	115
	Installing the Federated Access Manager Policy Agent	116
	▼ To Verify that Single Sign-On is Working Properly	117
	Sample Identity Provider Interactions	117
	Using Federated Access Manager to Enable SiteMinder Federation in a Service Provider Environment	126
	▼ To Install Federated Access Manager Instances	126
	▼ To Install and Configure SiteMinder in the Service Provider Domain	127
	▼ To Configure the Federated Access Manager Identity Provider and Service Provider for SAML2 protocols	131
	Sample Service Provider Interactions	134
3	Integrating Oracle Access Manager	141
	About Oracle Access Manager	141
	Overview of a Typical Oracle Access Manager Session	142
	Understanding the Oracle Access Manager Use Cases	143

Simple Single Sign-On Use Case	143
Federated Single Sign-On Use Cases	145
Installing and Configuring Oracle Access Manager	152
▼ To Install Oracle Access Manager and Oracle Access Manager Web Policy Agent	153
▼ To Configure Oracle Access Manager	154
Using Federated Access Manager to Enable Oracle Federation in the Identity Provider Environment	161
Installing and Configuring Federated Access Manager in the Identity Provider Container	161
Installing and Configuring the Oracle WebGate	161
Installing the Custom Oracle Authentication Module	162
Installing and Configuring Federated Access Manager in the Service Provider Container	163
Setting Up SAML2	163
▼ To Configure the Identity Provider Federated Access Manager for SAMLv2 Identity Provider Protocols	163
To Configure Oracle Access Manager Agent to protect Federation Access Manager URLs	165
▼ To Configure the Service Provider	166
▼ To Test the Single Sign-On	166
Using Federated Access Manager to Enable Oracle Federation in a Service Provider Environment	167
Installing Federation Access Manager in the Identity Provider Environment	167
Installing Federation Access Manager in the Service Provider Environment	168
Installing Oracle Access Manager	169
Configuring Oracle Access Manager for Federation Access Manager Scheme	170
Configuring a Resource	171
Setting Up SAMLv2	171
▼ To Configure the Federated Access Manager Identity and Service Providers for SAML2 Protocols	172
Verifying that Single Sign-On Works Properly	174

Preface

The *Sun Federated Access Manager Integration Guide* provides high-level instructions for deploying Federated Access Manager 8.0 with CA SiteMinder, Sun Identity Manager, and Oracle Access Manager.

Who Should Use This Book

This book is designed to be used by deployment architects and installation engineers. Readers should already be proficient with installing Federated Access Manager. You will derive the most benefit from this book if you already have a working knowledge of Federated Access Manager, CA SiteMinder, Sun Identity Manager, and Oracle databases.

How This Book Is Organized

This book contains three chapters:

- Integrating Sun Identity Manager
- Integrating CA SiteMinder
- Integrating Oracle Access Manager

Related Books

- Sun Federated Access Manager Deployment Planning Guide
- Sun Federated Access Manager Installation Guide

Related Third-Party Web Site References

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

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

Documentation, Support, and Training

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

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

Typographic Conventions

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

TABLE P-1 Typographic Conventions

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

Shell Prompts in Command Examples

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

TABLE P-2 Shell Prompts

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

Integrating Sun Identity Manager

This chapter provides instructions for configuring Federated Access Manager to work with Identity Manager. The examples in this chapter demonstrate how to configure Access Manager to protect Identity Manager, and to allow single sign-on login to the Identity Manager user and administrator interface. The examples also demonstrate how to configure Identity Manager to provision users and roles to Access Manager.

It is possible to configure the deployment for only SSO or for only provisioning. If you do not require single sign-on between Federated Access Manager and Identity Manager, then the Federated Access Manager Policy Agent does not need to be installed or configured. You can disregard the steps that involve the Federated Access Manager Policy Agent.

About the Deployment

In this deployment, Federated Access Manager is installed in the Realm mode of operation. The Federated Access Manager data store is configured to store configuration data.

A sub-realm named `idm` is created on Federated Access Manager. The user data store for this sub-realm is a Sun Directory Server data store that has the Federated Access Manager schema loaded into it. This sub-realm is used later when configuring the policy agent. The policy agent is deployed on Identity Manager to regulate access to the Identity Manager server. Identity Manager uses the MySQL database as its data store. Identity Manager can be configured to use MySQL or Oracle databases as its configuration data store.

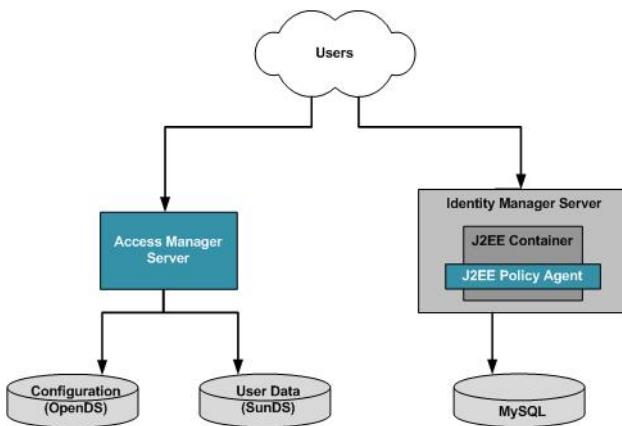


FIGURE 1-1 Deployment Architecture

About Sun Identity Manager

Sun Java System Identity Manager enables you to securely and efficiently manage and audit access to accounts and resources, and to distribute access management overhead. By mapping Identity Manager objects to the entities you manage such as users and resources, you significantly increase the efficiency of your operations.

The Identity Manager solution enables you to:

- Manage account access to a large variety of systems and resources.
- Securely manage dynamic account information for each user's array of accounts.
- Set up delegated rights to create and manage user account data.
- Handle large numbers of enterprise resources, as well as an increasingly large number of extranet customers and partners.
- Securely authorize user access to enterprise information systems. With Identity Manager, you have fully integrated functionality to grant, manage, and revoke access privileges across internal and external organizations.
- Keep data in sync by not keeping data.

About Sun Directory Server

Sun Java System Directory Server Enterprise Edition provides secure, highly available, scalable directory services for storing and managing identity data. Directory Server Enterprise Edition is the foundation of an enterprise identity infrastructure. It enables mission-critical enterprise applications and large-scale extranet applications to access consistent and reliable identity data. Directory Server Enterprise Edition provides a central repository for storing and managing

identity profiles, access privileges, application and network resource information. It also provides secure, on-demand synchronization of passwords, users, and groups with Microsoft Active Directory. See <http://docs.sun.com/app/docs/doc/820-2486/fxjbo?a=view>.

About Sun MySQL

MySQL is the world's most popular open source database software. MySQL has become the preferred choice for Web, Web 2.0, SaaS, ISV, Telecom companies and forward-thinking corporate IT Managers because it eliminates the major problems associated with downtime, maintenance and administration for modern, online applications. Powerful administration features enable users to fine-tune the server to optimize performance for the particular details of an embedded or bundled application. Plus, a pluggable storage engine architecture enables you to mix and match storage engines or just use what you need for an efficient optimized footprint.

Note – Identity Manager supports MySQL as a database resource in development or production deployments. MySQL is only supported as a repository database server in development deployment. See <http://docs.sun.com/source/820-2958/index.html#wp33051> for more details.

Software Versions Used in the Deployment

TABLE 1–1 Software Versions Used in the Deployment

Product	Download Location
Sun Solaris Operating System 10	http://www.sun.com/software/solaris/get.jsp
JDK 5.0 Update 16	http://java.sun.com/javase/downloads/index_jdk5.jsp
OpenSSO 1 (Build 4)	https://opensso.dev.java.net/public/use/index.html#stableopensso
Sun Java Identity Manager 8.0 (Build 10)	
Sun Java Web Server 7.0	Sun Java System Web Server 7.0 Update 2
Sun Java Application Server 9.1	Sun Java Application Server 9.1
Sun Java Directory Server 6.3	http://www.sun.com/software/products/directory_srver_ee/get1.jsp
	Choose Directory Server Enterprise Edition 6.x.

TABLE 1-1 Software Versions Used in the Deployment *(Continued)*

Product	Download Location
MySQL 5.0 Identity Manager supports MySQL as a database resource in development or production deployments. MySQL is only supported as a repository database server in development deployment. See http://docs.sun.com/source/820-2958/index.html#wp33051 for more details.	http://dev.mysql.com/downloads/mysql/5.0.html#solaris
MySQL Connector/J 5.0	http://dev.mysql.com/downloads/
Sun Java AM Policy Agent 3.0 (for Sun Application Server 9.1)	https://opensso.dev.java.net/public/use/index.html#stableagent
Netbeans IDE 6.0	http://download.netbeans.org/netbeans/6.0/final/
Sun Identity Manager IDE Plugin 8.0 Beta 1	https://identitymanageride.dev.java.net/

Installing and Configuring MySQL

To install and configure MySQL, follow these steps:

1. [Install MySQL](#)
2. [Configure MySQL](#)

▼ To Install MySQL

1 Follow the installation instructions provided at the MySQL website.

See <http://dev.mysql.com/doc/refman/5.0/en/installing-binary.html>.

The following is output from an installation session:

```
# groupadd mysql

# useradd -g mysql mysql

# pwd
/opt/MySQL

# ls -al
total 106
drwxr-xr-x 14 root      root          512 Jan  2 12:48 .
drwxr-xr-x  30 root      sys          1024 Jan  2 12:40 ..
```

```

drwxr-xr-x  2 root    root      2048 Jan  2 12:48 bin
-rw xr-xr-x  1 root    root      801 Jan  2 12:48 configure
-rw-r--r--  1 root    root     19071 Jan  2 12:48 COPYING
drwxr-xr-x  4 root    root      512 Jan  2 12:48 data
drwxr-xr-x  2 root    root      512 Jan  2 12:48 docs
-rw-r--r--  1 root    root      5139 Jan  2 12:48 EXCEPTIONS-CLIENT
drwxr-xr-x  3 root    root      1536 Jan  2 12:48 include
-rw-r--r--  1 root    root      8528 Jan  2 12:48 INSTALL-BINARY
drwxr-xr-x  2 root    root      512 Jan  2 12:48 lib
drwxr-xr-x  4 root    root      512 Jan  2 12:48 man
drwxr-xr-x  9 root    root      512 Jan  2 12:48 mysql-test
-rw-r--r--  1 root    root      1410 Jan  2 12:48 README
drwxr-xr-x  2 root    root      512 Jan  2 12:48 scripts
drwxr-xr-x  3 root    root      512 Jan  2 12:48 share
drwxr-xr-x  5 root    root      1024 Jan  2 12:48 sql-bench
drwxr-xr-x  2 root    root      512 Jan  2 12:48 support-files
drwxr-xr-x  2 root    root      512 Jan  2 12:48 tests

# chown -R mysql .

# chgrp -R mysql .

# ls -al
total 106
drwxr-xr-x 14 mysql    mysql      512 Jan  2 12:48 .
drwxr-xr-x 30 root     sys       1024 Jan  2 12:40 ..
drwxr-xr-x  2 mysql    mysql      2048 Jan  2 12:48 bin
-rw xr-xr-x  1 mysql    mysql      801 Jan  2 12:48 configure
-rw-r--r--  1 mysql    mysql     19071 Jan  2 12:48 COPYING
drwxr-xr-x  4 mysql    mysql      512 Jan  2 12:48 data
drwxr-xr-x  2 mysql    mysql      512 Jan  2 12:48 docs
-rw-r--r--  1 mysql    mysql      5139 Jan  2 12:48 EXCEPTIONS-CLIENT
drwxr-xr-x  3 mysql    mysql      1536 Jan  2 12:48 include
-rw-r--r--  1 mysql    mysql      8528 Jan  2 12:48 INSTALL-BINARY
drwxr-xr-x  2 mysql    mysql      512 Jan  2 12:48 lib
drwxr-xr-x  4 mysql    mysql      512 Jan  2 12:48 man
drwxr-xr-x  9 mysql    mysql      512 Jan  2 12:48 mysql-test
-rw-r--r--  1 mysql    mysql      1410 Jan  2 12:48 README
drwxr-xr-x  2 mysql    mysql      512 Jan  2 12:48 scripts
drwxr-xr-x  3 mysql    mysql      512 Jan  2 12:48 share
drwxr-xr-x  5 mysql    mysql      1024 Jan  2 12:48 sql-bench
drwxr-xr-x  2 mysql    mysql      512 Jan  2 12:48 support-files
drwxr-xr-x  2 mysql    mysql      512 Jan  2 12:48 tests

# scripts/mysql_install_db --user=mysql
Installing MySQL system tables...
OK
Filling help tables...

```

OK

To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:
.bin/mysqldadmin -u root password 'new-password'
.bin/mysqldadmin -u root -h am-v490-01 password 'new-password'
See the manual for more instructions.
You can start the MySQL daemon with:
cd . ; .bin/mysqld_safe &

You can test the MySQL daemon with mysql-test-run.pl
cd mysql-test ; perl mysql-test-run.pl

Please report any problems with the ./bin/mysqlbug script!

The latest information about MySQL is available on the web at
<http://www.mysql.com>
Support MySQL by buying support/licenses at <http://shop.mysql.com>

chown -R root .
chown -R mysql data
bin/mysqld_safe --user=mysql &
5994
Starting mysqld daemon with databases from /opt/MySQL/data

2 Stop the MySQL server.

```
# cd /opt/MySQL  
  
# ./bin/mysqldadmin -u root -p shutdown  
Enter password: <"password">  
STOPPING server from pid file /opt/MySQL/data/am-v490-01.pid  
080104 09:39:21 mysqld ended  
  
[1]+ Done .bin/mysqld_safe  
#
```

▼ To Configure MySQL

1 Set the password for the root user in MySQL.

```
# ./bin/mysql -u root -p  
Enter password:  
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 6  
Server version: 5.0.45-log MySQL Community Server (GPL)  
  
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.  
  
mysql> SET PASSWORD FOR 'root'@'localhost' = PASSWORD('password');  
Query OK, 0 rows affected (0.00 sec)  
  
mysql> SET PASSWORD FOR 'root'@'am-v490-01' = PASSWORD('password');  
Query OK, 0 rows affected (0.01 sec)  
  
mysql> exit  
Bye  
#
```

2 Set environment parameters for the MySQL script.

Change the file /opt/MySQL/support-files/mysql.server:

```
basedir=/opt/MySQL  
  
datadir=/opt/MySQL/data  
  
...  
  
basedir=/opt/MySQL  
  
bindir=/opt/MySQL/bin  
# cp /opt/MySQL/support-files/mysql.server /etc/sfw/mysql
```

3 Start the MySQL server.

```
# cd /opt/MySQL  
  
# ./bin/mysqld_safe --user=mysql --log&  
[1] 7764  
# Starting mysqld daemon with databases from /opt/MySQL/data  
  
#
```

Installing Identity Manager on Application Server

To install Identity Manager on Application Server, follow these steps:

1. [Install Application Server](#)
2. [Install Identity Manager on Application Server](#)
3. [Create Identity Manager Tables in MySQL](#)
4. [Configure the Application Server Data Source to Work with Identity Manager](#)
5. [Configure Identity Server to Work with Application Server](#)
6. [Configure Application Server to Work with Identity Manager](#)
7. [Create a Federated Access Manager Realm Administrator](#)
8. [Create a Federated Access Manager Realm Resource Object](#)

▼ To Install Application Server

- 1 **Follow the installations instructions in the Application Server product documentation.**

See <http://docs.sun.com/app/docs/doc/819-3670>.

- 2 **Start the Application Server.**

```
# /opt/SUNWappserver91/bin/asadmin start-domain domain1
```

▼ To Install Identity Manager on Application Server

The `idm.war` file is used because you will make manual changes to the deployed WAR in a subsequent procedure.

- 1 **Follow the installation instructions (with one exception) in the Identity Manager Installation Guide for deploying the `idm.war` file on the Application Server. This is the exception:**

Do not recreate the file suggested in the Identity Manager Installation Guide. Use the `idm.war` file that is available in the downloaded zip distribution.

See the Identity Manager Installation Guide at
<http://docs.sun.com/app/docs/doc/820-2956>

- 2 **Remove the following file:**

`/opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm/WEB-INF/lib/j2ee.jar`

This file causes conflicts with the `j2ee.jar` file that ships with Application Server.

- 3 **Set the Application Server classpath.**

- a. **Log in to the Application Server console.**

- b. In the left frame, click Application Server.
 - c. In the right frame, navigate to the "JVM Settings | Path Settings" tab.
 - d. Add the following entries to the Server Classpath in this exact order:


```
/opt/SUNWappserver91/lib/appserv-admin.jar
/opt/SUNWappserver91/lib/appserv-rt.jar
/opt/SUNWappserver91/imq/lib/imq.jar
/opt/SUNWappserver91/lib/j2ee.jar
/opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm/
WEB-INF/lib/mysql-connector-java-5.0.8-bin.jar
```
 - e. Click Save.
- 4 Set the Application Server JVM options.**
- In the right frame of the Application Server console, navigate to the "JVM Settings | JVM Options" tab.
- To add or modify the following JVM options, click the Add JVM Option button.
- a. Increase the JVM heap size to -Xmx1024M.
 - b. Set the Identity Manager home location to:
`-Dwaveset.home=/opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm`
 - c. Add the following option to ensure you can create resources in Identity Manager.
`-Dcom.sun.enterprise.server.ss.ASQuickStartup=false`
 - d. Click Save.

5 Stop the Application Server.

```
# /opt/SUNWappserver91/bin/asadmin stop-domain domain1
```

▼ To Create Identity Manager Tables in MySQL

1 Run the following commands:

```
# cd /opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm/sample
# /opt/mysql/bin/mysql -uroot -ppassword < create_waveset_tables.mysql
```

2 Verify that the Waveset database was successfully created.

```
-$ /opt/mysql/bin/mysqlshow -uroot -ppassword
+-----+
| Databases |
```

```
+-----+  
| information_schema |  
| mysql           |  
| test            |  
| waveset         |  
+-----+  
-$
```

You should see the waveset database name in the output above.

▼ To Configure the Application Server Data Source to Work with Identity Manager

- 1 Download the MySQL Connector/J 5.0.

- 2 Extract the archive mysql-connector-java-5.0.8.tar.gz.

- 3 Copy mysql-connector-java-5.0.8-bin.jar from the above download to /opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm/WEB_INF/lib/

- 4 Set the password for the waveset user in MySQL.

```
# cd /opt/mysql
```

```
# ./bin/mysql -u root -p  
Enter password:  
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 6  
Server version: 5.0.45-log MySQL Community Server (GPL)
```

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

```
mysql> SET PASSWORD FOR 'waveset'@'localhost' = PASSWORD('password');  
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> exit  
Bye  
#
```

- 5 Start the Application Server.

```
# /opt/SUNWappserver91/bin/asadmin start-domain domain1
```

- 6 Connect to the data source.

```
# cd /opt/SUNWappserver91/domains/domain1/applications/  
j2ee-modules/idm/bin
```

```
# chmod +x lh

# export WSHOME=/opt/SUNWappserver91/domains/domain1/applications/
j2ee-modules/idm

# export CLASSPATH=/opt/SUNWappserver91/lib/appserv-rt.jar:
/opt/SUNWappserver91/lib/javaee.jar:$CLASSPATH

# ./lh setRepo -v -tMySQL -ujdbc:mysql://localhost/waveset -Uwaveset -Ppassword
Defaulting administrator to 'configurator'.
Defaulting credentials to 'configurator'.
DB Server @ jdbc:hsqldb:hsq://127.0.0.1:53878/idm
Defaulting jdbcDriver to 'org.gjt.mm.mysql.Driver'.
Checking 'MysqlDataStore:jdbc:mysql://localhost/waveset'...
Switching to 'MysqlDataStore:jdbc:mysql://localhost/waveset'...
Getting current location....
Current Location is 'MysqlDataStore:jdbc:mysql://localhost/waveset'
userid is 'waveset'
password is '(set)'
jdbcDriver is 'org.gjt.mm.mysql.Driver'
#
#
```

▼ To Configure Identity Manager to Work with Application Server

- 1 Set the environment variables that will be required for the setup program:

```
# export WSHOME=/opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm

# export JAVA_HOME=/usr/java

# export PATH=/usr/java/bin:$PATH
```

- 2 Start an X server on your local machine, and set the DISPLAY variable on the Application Server host computer.

- 3 Run the following commands:

```
# cd /opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm/bin

# ./lh setup
```

- 4 Select MySQL (JDBC Driver) as the Repository Type.

- 5 Enter the same password for the waveset user that you set earlier in MySQL.

- 6 Click the Next button.**
- 7 Accept the default setting to setup a demo environment.**

- 8 Enter information about the demo user.**

In this case, enter following credentials:

User Name: demoapprover

Password: password

- 9 In the next screen, select the option for a Notification File for the Mail Settings.**

You may accept the default file or customize it.

- 10 In the next screen, click Execute.**

The `lh` program logs the details of the execution steps in the screen. See the Example in the “[Sample Output](#)” on page [57](#) at the end of this chapter.

Click Done.

- 11 Change permissions so that Identity Manager can perform certain actions.**

Add the following lines to

`/opt/SUNWappserver91/domains/domain1/config/server.policy:`

```
grant {  
    permission java.lang.RuntimePermission "accessClassInPackage.sun.io";  
    permission java.lang.RuntimePermission "getClassLoader";  
    permission java.lang.RuntimePermission "createClassLoader";  
    permission java.lang.RuntimePermission "accessDeclaredMembers";  
    permission com.waveset.repository.test.testConcurrentLocking "read";  
    permission java.net.SocketPermission "*", "connect,resolve";  
    permission java.io.FilePermission "*", "read";  
    permission java.util.PropertyPermission "*", "read,write";  
};  
grant codeBase "file:${waveset.home}/-"  
{  
    permission java.util.PropertyPermission "waveset.home", "read,write";  
    permission java.util.PropertyPermission "security.provider", "read,write";  
    permission java.io.FilePermission "${waveset.home}${{/}}*",  
        "read,write,execute";  
    permission java.io.FilePermission "${waveset.home}/help/index/-",  
        "read,write,execute,delete";  
    permission java.io.FilePermission "${(java.io.tmpdir)}$(/)*",  
        "read,write,delete";  
    permission java.util.PropertyPermission "*", "read,write";  
    permission java.lang.RuntimePermission "accessClassInPackage.sun.io";  
    permission java.net.SocketPermission "*", "connect,resolve";  
};
```

```
};
```

- 12 To enable Identity Manager to connect to Federated Access Manager with the SunAccessManagerRealmResourceAdapter, add the two following policies:**

```
grant {  
    permission java.lang.RuntimePermission "shutdownHooks";  
    permission java.io.FilePermission "${waveset.home}/WEB-INF/spe/config/spe.tld", "read";  
};
```

- 13 Restart the Application Server.**

```
# /opt/SUNWappserver91/bin/asadmin stop-domain domain1
```

```
# /opt/SUNWappserver91/bin/asadmin start-domain domain1
```

Watch for any errors in the Application Server server.log file.

- 14 Verify that you can successfully log in to Identity Manager.**

Go to the Identity Manager console at <http://host1.example.com:2080/idm/>

- a. Log in using the following credentials:**

Username: configurator

Password: configurator

To minimize security risk, it is a good practice to change the default password for this administrator.

- b. Log out.**

- c. Log in using the following credentials:**

Username: administrator

Password: administrator

- d. Log out.**

- e. Log in using the following credentials:**

Username: demoapprover

Password: password

- f. Log out.**

▼ To Configure Application Server to Work with Identity Manager

Before You Begin In the following steps, you configure the `AMConfig.properties` you generate in the first step. Use the credentials of the `amadmin` user to connect with the Federated Access Manager or OpenSSO server. You could use a user other than `amadmin` as long as the user has privileges to read the Federated Access Manager configuration data. This should not be a security concern because the `AMConfig.properties` file is required only to perform the initial configuration and to test the Access Manager Realm Resource adapter instance. The `AMConfig.properties` file is not needed after the Policy Agent has been installed on the Identity Manager server, and the file can be deleted afterward.

1 Generate the Federated Access Manager client configuration file.

Go to the directory, where you extracted the Federated Access Manager or OpenSSO zip distribution, and unzip the `opensso/samples/fam-client.zip` archive in a temporary directory. Then run the following commands:

```
# cd opensso/samples/tmp/sdk  
  
# chmod +x scripts/compile-samples.sh  
  
# scripts/compile-samples.sh  
  
# chmod +x scripts/setup.sh  
  
# scripts/setup.sh  
Debug directory (make sure this directory exists):  
/opt/SUNWappserver91/domains/domain1/logs/am_debug  
Password of the server application: password  
Protocol of the server: http  
Host name of the server: host1.example.com  
Port of the server: 48080  
Server's deployment URI: /opensso  
Naming URL (hit enter to accept default value,  
http://host1.example.com:48080//opensso/namingservice):  
#
```

You should now see a `AMConfig.properties` file created in the `sdk/resources` directory.

2 Install the Federated Access Manager or OpenSSO cmdline tools.

They are present in the Federated Access Manager or OpenSSO zip distribution, in the `opensso/tools/famAdminTools.zip` archive.

```
# mkdir /opt/fam80-idm80-tools  
  
# cd /opt/fam80-idm80-tools
```

```

# unzip /export/software/
FAM_80_IDM_80_Integration/fam_zip/fam/tools/famAdminTools.zip

# ./setup
Path to config files of server (example: /opt/OpenSSO/config):
/opt/fam80-idm80
The scripts are properly setup under directory:
/opt/fam80-idm80-tools/fam
The version of this tools.zip is: 8.0
The version of your server instance is: 8.0 (2008-February-13 01:40)
#

```

You will now see an opensso directory (or a directory with the name of the context-root of your Federated Access Manager or OpenSSO deployment), in the /opt/fam80-idm80-tools directory.

3 Encrypt the password for the amadmin user using the ampassword utility.

First, you need to create a text file containing the password of the amadmin user in plain text. In the following example, the password file /export/software/amadmin_pwd is created:

```

# cd /opt/fam80-idm80-tools/fam/bin

# ./ampassword --encrypt /export/software/amadmin_pwd
AQICSw+UrU2DJyY1KBeoC0iuZv3gQTGkbI39
#

```

4 Customize the AMConfig.properties file that was created in step

- In the Federated Access Manager console, navigate through these tabs: Configuration | Sites and Servers | <server-entry> | Security.**

- Copy the value from the property Password Encryption Key, and use the value to modify the following property:**

am.encryption.pwd=AQICrPmBjI5aThg1H6kKcJr0/Lu4D9LdTlqe

- Modify the following property as shown:**

com.sun.identity.agents.app.username=amadmin

- For security purposes, either comment out the following line, or leave the value empty:**

#com.iplanet.am.service.password=

- Modify the following property using the value from the encrypted password generated in step 3 above:**

com.iplanet.am.service.secret=AQICSw+UrU2DJyY1KBeoC0iuZv3gQTGkbI39

5 Copy the Federated Access Manager or OpenSSO Client files to the Identity Manager application directory. You will need the following files:

- The openssoclientsdk.jar library that is present in the /sdk/lib directory from the fam-client.zip archive in the Federated Access Manager or OpenSSO zip distribution.

```
# cp /export/software/
FAM_80_IDM_80_Integration/fam_zip/opensso/samples/
tmp/sdk/lib/openssoclientsdk.jar /opt/SUNWappserver91/domains/domain1/
applications/j2ee-modules/idm/WEB-INF/lib/
```

- The AMConfig.properties generated above.

```
# mkdir /opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/
idm/WEB-INF/classes
# cp /export/software/FAM_80_IDM_80_Integration/fam_zip/opensso/samples/
tmp/sdk/resources/AMConfig.properties /opt/SUNWappserver91/domains/domain1/
applications/j2ee-modules/
idm/WEB-INF/classes
```

6 Copy the customized AMConfig.properties from step (4) above, to the following directory:

/opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm/WEB-INF/classes/

7 Update the Application Server classpath.

- a. Login to the Application Server Console.

- b. Navigate to Application Server | JVM Settings | Path Settings

- c. Update the Classpath Suffix to contain the following entries:

```
/opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm/
WEB-INF/lib/openssoclientsdk.jar
```

```
/opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm/WEB-INF/classes
```

- d. Click Save to save your changes.

- e. Log out from the Application Server Console.

8 Restart the Application Server.

```
# /opt/SUNWappserver91/bin/asadmin stop-domain domain1
```

```
# /opt/SUNWappserver91/bin/asadmin start-domain domain1
```

Watch for any errors in the Application Server server.log log file.

Creating a Federated Access Manager Realm Administrator

If you plan to use Identity Manager to manage objects in the Federated Access Manager root realm, then create a user in the Federated Access Manager root realm. Give this user the same privileges as the Top-level Admin Role. The privileges should allow this user "Read and write access to all realm and policy properties." This user will be used to configure the Identity Manager Resource adapter.

If you plan to use Identity Manager to manage objects in the Federated Access Manager sub-realm, then create a user in the Federated Access Manager sub-realm. Give this user privileges to "Read and write access to all realm and policy properties." This user will have the privileges of a sub-realm administrator, and will be used to configure the Identity Manager Resource adapter. In this example, a realm administrator `sradmin` with the password `password` was created in the sub-realm `opensso > idm`.

▼ To Create a Federated Access Manager Realm Resource Object

1 Access the Identity Manager console.

In this example, go to `http://host1.example.com:2080/idm/`. The Identity Manager login page is displayed.

2 Log in using the following credentials:

User Name: configurator

Password: configurator

3 Add the Federated Access Manager realm adapter to the resource classpath.

a. Navigate to Resources | Configure Types.

b. At the bottom of the page, click "Add Custom Resource."

c. Add the following to the Resource Classpath:

```
com.waveset.adapter.SunAccessManagerRealmResourceAdapter
```

In earlier versions of Federated Access Manager, it was possible to install Access Manager in the legacy mode of operation. In legacy mode, a different Identity Manager resource adapter `com.waveset.adapter.SunAccessManagerResourceAdapter`, should be configured on Identity Manager. Both types of adapters have the same functionality. But

`com.waveset.adapter.SunAccessManagerResourceAdapter` uses the legacy Access Manager AMSDK api, while the `com.waveset.adapter.SunAccessManagerRealmResourceAdapter` uses the Federated Access Manager idRepo api.

- d. Click Save.

4 Configure the Federated Access Manager Realm adapter.

- a. **Navigate to Resources | List Resources**
- b. **Choose --Resource Type Actions-- | New Resource**
- c. **Choose Sun Access Manager Realm from the list of resources. Click New.**
- d. **In the Create Sun Access Manager Realm Resource Wizard screen, click Next.**

e. **In the Resource Parameters screen, provide the following information:**

Host: Fully-qualified hostname of the Federated Access Manager Server.
Example: host1.example.com

TCP Port: Port number of the Federated Access Manager server. In this example, 48080.

User: sradmin

You must use a Federated Access Manager realm administrator, and not a non-administrator user, because it requires special permissions. If you use a non-administrator user, this test will fail. Use the realm administrator configured in the previous section.

Password: password

This is the plain-text password of the user realm administrator.

Protocol : Protocol of the Federated Access Manager Server realm or Identity Manager. In this example, enter http.

Realm: This is the realm name of the Federated Access Manager server. In this example, enter /idm. If the user entered above were in the top-level realm, you would enter just a slash (/).

Encryption Key: This is the value of the `am.encryption.pwd` property in the `AMConfig.properties` file.

Example: `AQICrPmBjI5aThg1H6kKcJr0/Lu4D9LdTlqe`

JCE Encryptor Class :	This is the value of the <code>com.ipplanet.security.encryptor</code> property in the <code>AMConfig.properties</code> file.
	In this example, enter: <code>com.ipplanet.services.util.JCEEEncryption</code> .
Naming Service URL:	This is the value of the <code>com.ipplanet.am.naming.url</code> property in the <code>AMConfig.properties</code> file.
	In this example, enter <code>:http://host1.example.com:48080/openSSO/namingservice</code> .
Error Log Level:	message
Error Log Directory:	Directory into which the Identity Manager Access Manager Resource will write debug logs. This directory must already exist.
	In this example, enter: <code>/opt/SUNWappserver91/domains/domain1/logs/am_debug</code> .

5 Click Test Configuration.

The following message will be displayed: “Test connection succeeded for resource(s): SunAccessManagerRealm.” If you don't see this message, then you must troubleshoot by looking at the following logs:

- Application Server `server.log`
`/opt/SUNWappserver91/domains/domain1/logs/server.log`
- Access Manager client logs at `/opt/SUNWappserver91/domains/domain1/logs/am_debug` (specified in the form above)

Click Next.

6 In the Account Attributes page, set the following mapping:

Identity System Attribute: Full name

Resource User Attribute: cn

Click Next.

7 In the Identity Template page, make sure you have this entry:

`$accountId$`

Click Next.

8 In the Identity System Parameters page, select uid for the Display Name Attribute parameter.

Click Save to save the value.

9 In the Configure Identity Attributes? page, click No.

The Resource List page is displayed. You should see a resource of the type Sun Access Manager Realm. To expand this branch, click the arrow next to it.

a. Expand the Sun Access Manager Realm type by clicking the arrow next to it.

You should see an entry SunAccessManagerRealm.

b. Expand the SunAccessManagerRealm branch by clicking the arrow next to it.

You should see a listing of all Federated Access Manager roles and groups under this branch that exist in the Federated Access Manager sub-realm that the Identity Manager Resource was configured with in step 4e above.

Provisioning Identities from Identity Manager to Federated Access Manager

Before you can provision a user, role, or group into Federated Access Manager, the SunAccessManagerRealm adapter must be configured with the information required to successfully log in to Federated Access Manager and the target Federated Access Manager realm.

When you provision a user, role, or group from Identity Manager into Federated Access Manager, you must select the Resource that you want to provision into. In this example, you will select the SunAccessManagerRealm adapter as the Resource to provision into. This adapter uses Federated Access Manager APIs (OpenSSO package com.sun.identity.idm.*), to communicate with Federated Access Manager. Federated Access Manager receives the request to create or retrieve a user, role, or group. Federated Access Manager then performs the task on its configured data stores in the relevant Federated Access Manager realm. Similarly, for role or group retrieval from the Federated Access Manager data store, the SunAccessManagerRealm adapter uses Federated Access Manager APIs to communicate with Federated Access Manager and to retrieve these objects.

In Identity Manager, Resource Objects correspond to Federated Access Manager roles and groups. Resource Accounts correspond to Federated Access Manager users that have been provisioned from Identity Manager. Since Resource Objects and Resource Accounts are managed differently in Identity Manager, both types of resources are viewable on separate tabs in the Identity Manager console.

The following figure illustrates how objects are provisioned and retrieved in Identity Manager.

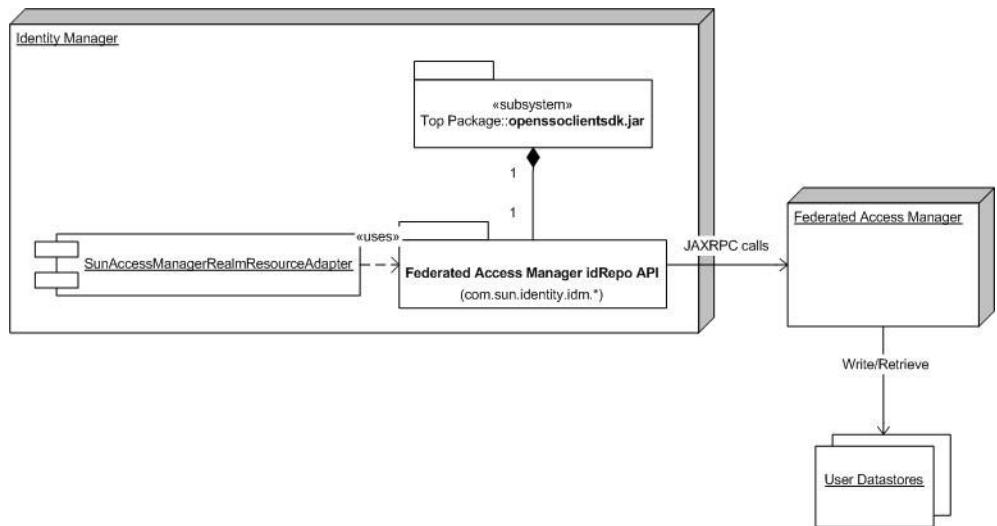


FIGURE 1–2 Overview of Provisioning and Retrieving Objects in Identity Manager

To provision identities from Identity Manager to Federated Access Manager, follow these steps:

1. [View Federated Access Manager Roles and Groups in Identity Manager](#)
2. [View Federated Access Manager User Accounts in Identity Manager](#)
3. [Provision a Test User From Identity Manager Into Federated Access Manager](#)
4. [Verify that Identities Were Successfully Provisioned](#)
5. [Provision a Test Role From Identity Manager Into Federated Access Manager](#)
6. [Verify the Test Role Was Successfully Provisioned from Identity Manager Into Federated Access Manager](#)
7. [Provision an Admin-User From Identity Manager Into Federated Access Manager](#)
8. [Verify the Admin-User Was Successfully Provisioned from Identity Manager into Federated Access Manager](#)
9. [Provision an Admin-Role From Identity Manager Into Federated Access Manager](#)

▼ To View Federated Access Manager Roles and Groups in Identity Manager

- 1 1) Login to the Identity Manager console using the following credentials:

User Name: configurator

Password: configurator

- 2 Navigate to the tab Resources | List Resources.
- 3 Expand the branch for the SunAccessManagerRealm adapter instance.

Name	Description
idmtestrole10	am-v490-01.red.ipplanet.com
idmtestrole11	am-v490-01.red.ipplanet.com
idmtestrole12	am-v490-01.red.ipplanet.com
idmtestrole2	am-v490-01.red.ipplanet.com
idmtestrole3	am-v490-01.red.ipplanet.com
manager	am-v490-01.red.ipplanet.com
srtestrole1	am-v490-01.red.ipplanet.com

▼ To View Federated Access Manager User Accounts in Identity Manager

- 1 Log in to the Identity Manager console using the following credentials:
User Name: configurator
Password: configurator
- 2 Navigate to the tab Resources | Examine Account Index.
- 3 Expand the branch for the SunAccessManagerRealm adapter instance.

No items were found.

Name	Situation	Owner
+ LDAP		
└ Sun Access Manager Realm		
└ SunAccessManagerRealm		
└ idmtestuser1	CONFIRMED	idmsrtestuser1
└ idmsrtestuser2	CONFIRMED	idmsrtestuser2
└ idmsrtestuser3	CONFIRMED	idmsrtestuser3
└ idmsrtestuser5	CONFIRMED	idmsrtestuser5
└ idmtestuser1	CONFIRMED	idmtestuser1

You can also view the provisioned Federated Access Manager user accounts in the Identity Manager console by navigating to the tab Accounts | List Accounts. However, that page will show you all Identity Manager accounts in the Identity Manager server, including those provisioned into Federated Access Manager and any other resource or system, that has been configured in Identity Manager. For example, if Identity Manager were configured for SAP and Federated Access Manager Resources, you would see a listing of users that have been provisioned into both systems. You can also use this page to create or provision users as described in sections below.

To view the accounts created per Resource Type, navigate to the tab Resources | Examine Account Index. This page is for viewing only, and you cannot use this page to create or provision a user.

▼ To Provision a Test User From Identity Manager Into Federated Access Manager

Follow these steps to test the Access Manager Realm Resource that was configured in Identity Manager.

- 1 Log in to the Identity Manager console using the following credentials:**

User Name: configurator

Password: configurator

- 2 Navigate to the tab Accounts | List Accounts.**

3 Select the option New Actions | New User.

4 In the Create User page, enter these values:

AccountID:	idmuser
First Name	Identity Manager
Last Name:	User
Password:	password
Confirm Password:	password

5 In the Create User page, click the Resources tab.

Select the SunAccessManagerRealmResourceAdapter resource as the Current Resource.

6 For the Individual Resource Assignment property, select the SunAccessManagerRealm as the Current Resource.

a. For the Capabilities property, select all capabilities as Assigned Capabilities.

Review the list of capabilities for the user being created to manage Identity Manager and Federated Access Manager users. Not all capabilities will be applicable. This will vary from site to site.

b. For the Controlled Organizations property, select Top as the Selected Organizations.

Also, please note that for 6a above,

7 Click Save at the bottom of the screen.

8 In the next screen, you should see a success message "Account idmuser created."

Click OK.

The User List page is displayed and contains a list with the newly-created user idmuser.

9 Logout from the Identity Manager console.

▼ To Verify that Identities Were Successfully Provisioned

1 In the Identity Manager console, return to the Accounts tab | List Accounts tab..

You should see the idmuser user entry in the listing

2 Log in to the Federated Access Manager console and verify that the user account is visible from the Subjects tab of your realm.

If the end-user entry is visible in both Identity Manager and Federated Access Manager, then the end-user has successfully been provisioned.

3 Log in to Identity Manager and verify that you are logged into the Identity Manager User Page.

In this example, go to the following URL:

`http://host1.example.com:2080/idm/user`

Log in using the following credentials:

User Name: idmuser

Password: password

4 Log in to Federated Access Manager.

In this example, go to the following URL:

`http://host1.example.com:48080/amserver/UI/Login?realm=idm`

Log in using the following credentials:

User Name: idmuser

Password: password

5 Verify that you are logged into Federated Access Manager and that you can see the user profile page.

6 Log out from the Identity Manager and Federated Access Manager consoles.

Next Steps If you are not able to log in as the user, do the following:

- Verify that you can see the user entry in the sub-realm in the Federated Access Manager console.
- Troubleshoot the issue using the Federated Access Manager debug logs and the debug logs written by the Identity Manager's Access Manager Resource

▼ To Provision a Test Role From Identity Manager Into Federated Access Manager

Before You Begin

In the Federated Access Manager console, in the data store configuration page for the realm or sub-realm into which you will be provisioning the role, for the property LDAP Roles Attributes, add cn to the list of values.

The cn attribute is not defined as an attribute for the IdType.ROLE in the Data Store configuration by default. This attribute is set, when the role is provisioned to Federated Access Manager. If the cn attribute is not already defined, Identity Manager shows the following error on the Identity Manager console:

```
com.waveset.util.WavesetException:  
Error creating object 'idmsrtestrole5'.  
com.waveset.util.WavesetException:  
Error setting attributes for 'idmsrtestrole5'  
com.sun.identity.idm.IdRepoException:  
Illegal arguments: One or more required arguments is null or empty
```

1 Log in to the Identity Manager console using the following credentials:

User Name: configurator

Password: password

2 Navigate to the tab Resources | List Resources.

3 Expand the branch for the Sun Access Manager Realm entry.

4 Mark the checkbox in front of the SunAccessManagerRealm entry.

5 Choose the option Resource Actions | Create Resource Object.

6 In the New Resource Object page, select Role from the dropdown box, and click New.

In the next page:

a. Enter the name of the role as `idm_users_role`.

b. Assign the user `idmuser` to this role.

7 Click Save.

8 In the Create Role Results page, click OK.

The Resource List page is displayed, and contains a list with the role `idm_users_role` created when you expand the SunAccessManagerRealm branch.

9 Log out from the Identity Manager console.

▼ To Verify the Test User Role Was Successfully Provisioned from Identity Manager Into Federated Access Manager

1 Log in to Federated Access Manager.

In this example, go to the following URL:

`http://host1.example.com:48080/opensso`

Log in using the following credentials:

User Name: amadmin

Password: password

2 Navigate to the sub-realm `idm` and tab Subjects | User.

The user Identity Manager User should be listed as one of the users.

3 Navigate to the tab Subjects | Role.

The role `idm_users_role` should be listed as one of the roles.

4 In the role profile page, click the `idm_users_role` role entry.

5 Click on the User tab.

The user Identity Manager User should be selected into the role.

6 Log out of the Federated Access Manager console.

Next Steps If you are not able to see the role entry or the user assigned to the role troubleshoot the issue using the Federated Access Manager debug logs and the debug logs written by the Identity Manager's Access Manager Resource.

▼ To Provision an Admin-User From Identity Manager Into Federated Access Manager

At this point, the Identity Manager is not yet protected by the policy agent. Follow these steps to create a user that will have administrative privileges on Identity Manager.

1 Login to the Identity Manager console using the following credentials:

User Name: configurator

Password: configurator

2 Navigate to the tab Accounts | List Accounts.

3 Choose the option New Actions | New User.

4 In the Create User page, enter these values:

 AccountID: idmadmin

 First Name Identity Manager

 Last Name: Admin

 Password: password

 Confirm Password : password

5 In the Create User page, click on the Resources tab.

a. For the Capabilities property, select all capabilities as Assigned Capabilities.

b. For the Controlled Organizations property, select Top as the Selected Organizations.

Click Save button.

In the next screen, you should see a success message "Account idmadmin created". Click OK.

The User List screen is displayed and contains a list with the the newly-created user idmadmin.

6 Log out of the Identity Manager console.

▼ **To Verify the Admin-User Was Successfully Provisioned from Identity Manager into Federated Access Manager**

1 In the Identity Manager Console, return to the Accounts tab | List Accounts tab

You should see the admin-user entry in the listing.

2 Log in to the Federated Access Manager console.

Verify that the admin—user account is visible from the Subjects tab of your realm. If the admin-user entry is visible in both Identity Manager and Federated Access Manager, then the admin-user has successfully been provisioned.

3 Log in to Identity Manager.

In this example, go to the following URL:

`http://host1.example.com:2080/idm`

Log in using the following credentials:

User Name: idmadmin

Password: password

Verify that you are logged into the Identity Manager console.

4 Log in to Federated Access Manager.

In this example, go to the following URL:

`http://host1.example.com:48080/opensso/UI/Login?realm=idm`

Log in using the following credentials:

User Name: idmadmin

Password: password

Verify that you are logged into Federated Access Manager and can see the user profile page.

▼ To Provision an Admin-Role From Identity Manager Into Federated Access Manager

At this point, the Identity Manager is not yet protected by the policy agent. The role that will be created here will not have any special privileges assigned to it. It will only be used to group the administrative users, and this role will be used later in a policy in Federated Access Manager.

1 Log in to the Identity Manager console as using the following credentials:

User Name: configurator

Password: configurator

2 Navigate to tab Resources | List Resources.**3 Expand the branch for the Sun Access Manager Realm entry.****4 Mark the checkbox in front of the SunAccessManagerRealm entry.****5 Choose the option Resource Actions | Create Resource Object.****6 In the New Resource Object page, select Role from the dropdown box, and click New.**

- 7 In the next page, enter the name of the role as `idm_admins`, and assign the user `idmadmin` to this role.
Click Save.
- 8 In the Create Role Results screen, click OK.
When you expand the `SunAccessManagerRealm` branch, the Resource List page is displayed and contains a list with the newly-created role `idmadmin`.
- 9 Log out of the Identity Manager console.

▼ To Verify the Test Admin Role Was Successfully Provisioned from Identity Manager Into Federated Access Manager

- 1 Log in to Federated Access Manager.
In this example, go to the following URL:
`http://host1.example.com:48080/opensso`
Log in using the following credentials:
User Name: `idm_admins`
Password: `password`
- 2 Navigate to the sub-realm `idm` and tab Subjects | User.
The user Identity Manager Admin should be listed as one of the users.
- 3 Navigate to the tab Subjects | Role.
The role `idm_admins` should be listed as one of the roles.
- 4 In the role profile page, click the `idm_admins` role entry.
- 5 Click on the User tab.
The user Identity Manager Admin should be selected into the role.
- 6 Log out of the Federated Access Manager console.

Next Steps If you are not able to see the role entry or the user assigned to the role, troubleshoot the issue using the Federated Access Manager debug logs and the debug logs written by the Identity Manager Access Manager Resource.

Installing And Configuring the Federated Access Manager Policy Agent on Identity Manager

Although this document describes an example where Identity Manager and Federated Access Manager are configured for both single sign-on and provisioning, it is possible to configure a deployment for single sign-on without provisioning, or for provisioning without single sign-on. If single sign-on between Federated Access Manager and Identity Manager is not required, then the Federated Access Manager Policy Agent does not need to be installed or configured. In that case, you can ignore the steps that involve the Federated Access Manager Policy Agent.

To install and configure the Federated Access Manager policy agent on Identity Manager, follow these steps:

1. Create the Federated Access Manager Agent Profile On The Federated Access Manager Server.
2. Install the Federated Access Manager Policy Agent on the Identity Manager Server.
3. Configure the Federated Access Manager Policy Agent on Federated Access Manager .
4. Create Policies on Federated Access Manager.
5. Disable Protection of Identity Manager Server by the Federated Access Manager Policy Agent .
6. Configure The Federated Access Manager Policy Agent On Identity Manager Server.

▼ To Create the Federated Access Manager Agent Profile On The Federated Access Manager Server

- 1 Download Policy Agent 3.0 for Sun Application Server 9.1.
- 2 Log in to the Federated Access Manager console.
- 3 Navigate to Configuration > Agents > J2EE.
- 4 In the Agent section, New and create a new agent profile with these values:

Name:	idmagent
Password:	password
Re-Enter Password:	password
Server URL:	http://host1.example.com:48080/opensso
Agent URL:	http://host1.example.com:2080/agentapp

Click Create.

The console displays the J2EE Policy Agent page again with a hyperlink for the agent profile `idmagent`.

5 Click on the `idmagent` hyperlink.

The “Edit `idmagent`” page is displayed. The agent profile is now created.

6 If Federated Access Manager is deployed on a web server, In the Agent profile page, navigate to the tab SSO.

Select the property SSO Decode (`com.sun.identity.agents.config.sso.decode`).

It is necessary to select this property only when Federated Access Manager is deployed on a web server. If you leave this property unselected, then you will find that, after you login to Federated Access Manager, the browser appears to be stuck and hanging on the Federated Access Manager login screen.

Click Save.

7 Log out of the Federated Access Manager console.

8 Verify that you can login to the Federated Access Manager console as this user.

9 Create an policy agent password file named `/export/software/agent_pwd`.

This file should contain only the password for the Agent profile, in plain text

▼ **To Install the Federated Access Manager Policy Agent on the Identity Manager Server**

The Policy Agent provides these capabilities:

- Retrieve and map an Federated Access Manager user session attribute (`UserToken`), to an Identity Manager attribute (`sois_user`), so that Identity Manager can perform the single sign-on from Federated Access Manager.
- Access protection for the Identity Manager pages in addition to the protection offered by the specific capabilities that can be explicitly assigned to a user from the Identity Manager console.

The `sois_user` is the authentication property in Identity Manager that is used during single sign-on between Federated Access Manager and Identity Manager. The name `sois_user` given to the property was an abbreviation for Sun ONE Identity Server User. The Sun ONE Identity Server product was a predecessor to Federated Access Manager.

- 1 Follow instructions in the policy agent documentation for installing the Policy Agent on Application Server.
- 2 Deploy the `agentapp.war` on the Sun Application Server.
- 3 When the policy agent installation is complete, verify that the agent is installed and functioning properly.

Install the sample application agent sample that is ships with the agent and test the application. Instructions to install and test the sample application are available on the OpenSSO website.

▼ To Configure the Federated Access Manager Policy Agent on Federated Access Manager

- 1 Configure the Federated Access Manager Agent Profile
 - a. Log in to the Federated Access Manager console as `amadmin`.
 - b. Navigate to Configuration > Agents > J2EE.
 - c. Click the policy agent profile that was created earlier and was associated with the agent installation.
 - d. Navigate to the tab Global.
 - e. For the property **Federated Access Manager Login URL** (`com.sun.identity.agents.config.login.url`), remove the existing entry, and add this entry:
`[0]=http://host1.example.com:48080/openssso/UI/Login?realm=idm`
The value must be the login URL that the AM users should use to login to AM
Click Save.
- 2 Navigate to the tab Application.
 - a. For the property **Session Attribute Fetch Mode** (`com.sun.identity.agents.config.session.attribute.fetch.mode`), choose the option `HTTP_HEADER`.

- b. For the property **Session Attribute Mapping** (`com.sun.identity.agents.config.session.attribute.mapping`), remove the existing entry, and add this entry:

```
[UserToken]=sois_user
```

- c. For the property **Not Enforced URLs**

```
(com.sun.identity.agents.config.notenforced.uri), add these entries:
```

```
[0]=/idm/styles/*
```

```
[1]=/idm/includes/*
```

```
[2]=/idm/images/*
```

Click Save.

- 3 Log out from the Federated Access Manager console.

▼ To Create Policies on Federated Access Manager

Create the following roles in the realm where the users will be provisioned. If the policy is to be created in a sub-realm, then you must first create a Referral Policy in the top-level realm for the same URLs.

1 Identity Manager User Policy

This policy restricts access to the Identity Manager user pages, only to the users in the `idm_users_role` role. So regular Identity Manager users will not be allowed to access the Identity Manager console URIs.

a. URL Policy

For `http://server:port/idm/user`, allow GET and POST actions .

b. URL Policy

For `http://server:port/idm/user/*`, allow GET and POST actions .

Subject Type: Access Manager Identity Subject | Role | `idm_users_role`

2 Identity Manager Admin Policy

This policy restricts access to the Identity Manager pages, to only the users in the `idm_admins` role. The users in this role will be able to access all Identity Manager pages, both administrator and user pages.

a. URL Policy

For `http://server:port/idm`, allow GET and POST actions

b. URL Policy

For `http://server:port/idm/*`, allow GET and POST actions

Subject Type: Access Manager Identity Subject | Role | `idm_admins`

▼ To Disable Protection of Identity Manager Server by the Federated Access Manager Policy Agent

This task enables you to perform the tasks described in the sections below without the policy agent getting in the way. At this point, the policies haven't been set up on Federated Access Manager. You would be denied access to all Identity Manager URLs until policies are set up. The protection by the policy agent will be re-enabled in a subsequent procedure. See "[To Re-Enable Protection Identity Manager Protection by the Federated Access Manager Policy Agent](#)" on page 52.

1 Log in to the Federated Access Manager console using the following credentials:

User Name: amadmin

Password: password

2 Navigate to Configuration > Agents > J2EE > *agent-name* > Application.

3 For the property Not Enforced URI (`com.sun.identity.agents.config.notenforced.uri`), add this entry:

[3] = /idm/*

4 Click Save.

5 Log out of the Federated Access Manager console.

▼ To Configure The Federated Access Manager Policy Agent On Identity Manager Server

1 Modify the Identity Manager application descriptor.

a. Go to the directory where the application descriptor is present.

```
# cd /opt/SUNWappserver91/domains/  
domain1/applications/j2ee-modules/idm/WEB-INF
```

b. Back up the file web.xml.

c. Edit web.xml.

- Change DOCTYPE as follows:

```
<web-app version="2.4"  
xmlns="http://java.sun.com/xml/ns/j2ee"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee  
http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd">
```

- Delete the single instance of <web-app> in the next line.
- Add the following just before the first <filter> definition:

```
<filter>  
  <filter-name>Agent</filter-name>  
  <filter-class>com.sun.identity.agents.filter.AmAgentFilter</filter-class>  
</filter>  
  
<filter-mapping>  
  <filter-name>Agent</filter-name>  
  <url-pattern>/*</url-pattern>  
  <dispatcher>REQUEST</dispatcher>  
  <dispatcher>INCLUDE</dispatcher>  
  <dispatcher>FORWARD</dispatcher>  
  <dispatcher>ERROR</dispatcher>  
</filter-mapping>
```

2 Log in to the Application Server console.

3 Navigate to Application Server > JVM Settings > Path Settings.

4 Update the classpath suffix.

Remove the following entries that you had added earlier:

```
/opt/SUNWappserver91/domains/domain1/applications/  
j2ee-modules/idm/WEB-INF/lib/openssoclientsdk.jar
```

```
/opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/  
idm/WEB-INF/classes
```

At this time, you can also physically delete the `openssoclientsdk.jar` file and the `classes` directory. They are no longer needed.

5 Click Save.

In the following steps, the recommended approach is to update the `web.xml` file (above), recreate the `idm.war`, and then redeploy the new `idm.war` file on the Application Server.

6 Stop the Application Server.

```
# /opt/SUNWappserver91/bin/asadmin stop-domain domain1
```

7 Delete the generated Identity Manager application files.

They will be re-generated when you access the Identity Manager application. If you don't do this step, the changes that you made in the `web.xml` file may not go into effect.

```
# cd /opt/SUNWappserver91/domains/domain1/generated/xml/j2ee-modules  
  
# rm -rf idm
```

8 Start the Application Server.

```
# /opt/SUNWappserver91/bin/asadmin start-domain domain1
```

Watch for any errors in the Application Server `server.log` file.

Configuring Identity Manager for Single Sign-On

To configure Identity Manager for Single Sign-On, follow these steps:

1. [Configure Identity Manager Login Module Groups](#)
2. [Configure the Identity Manager User Login Interface](#)
3. [Configure the Identity Manager Admin Login Interface](#)

▼ To Configure Identity Manager Login Module Groups

At this point, Identity Manager is not yet protected by the policy agent.

- 1 **Log in to the Identity Manager console using the following credentials:**

User Name: configurator

Password: configurator

- 2 **Navigate to the Security > Login tab**

- 3 **Click "Manage Login Module Groups."**

- 4 **In The Login Module Groups page, click New.**

- 5 **In the Create Login Module Group page, complete the following:**

Login Module Group Name: Sun Access Manager Realm

Assign Login Module: Sun Access Manager Realm Login Module

In the second dropdown: SunAccessManagerRealm

The Modify Login Module screen is displayed.

- 6 **In the Modify Login Module screen, choose the following values:**

Login success requirement: Sufficient

Login correlation rule: Leave this field blank. Don't make a selection; leave it at entry "Select..."

Click Save.

The Create Login Module Group page is displayed. Here you will see a new row added to the table that will describe the selections you had made. You should now see one login module listed in the table.

- 7 **In the Assign Login Module dropdown, choose "Identity System UserID/Password Login Module".**

You will now be redirected to the Modify Login Module screen.

- 8 **In the Modify Login Module page, enter the following values:**

Login display name: PassThrough

Login success requirement: sufficient

Click Save.

You will be taken back to the Create Login Module Group. Here you will see a new row added to the table that will describe the selections you had made. You should now see two login modules listed in the table.

9 Click Save.

You will be redirected to the Login Module Groups screen. Here you will see the custom group you added Sun Access Manager Realm.

10 Click “Return To Login Applications.”

▼ **To Configure the Identity Manager User Login Interface**

You are logged into the Identity Manager console, and are on the Security > Login tab.

1 Click on the User Interface hyperlink.

2 Remove the “Default Identity System ID/Password Login Module Group.”

Select the checkbox beside the entry and click Delete.

3 In the “Assign Login Module Groups” dropdown, select the Sun Access Manager Realm login module.

The Modify Login Module page is displayed. You should see just one login module group listed in the table, Sun Access Manager Realm.

Click Save.

4 The Login Applications page is displayed.

For the User Interface application, the Sun Access Manager Realm login module group has been assigned to it.

5 Log out of Identity Manager console.

▼ **To Configure the Identity Manager Admin Login Interface**

At this point, Identity Manager is not yet protected by the policy agent.

1 Log in to the Identity Manager console using these credentials:

User Name: configurator

Password: configurator

- 2 Navigate to the Security > Login tab.**
- 3 Click the Administrator Interface hyperlink.**
- 4 Remove the “Default Identity System ID/Password Login Module Group.”**
Mark the checkbox beside the entry and click Delete.
- 5 In the Assign Login Module Groups dropdown, select the Sun Access Manager Realm login module.**
The Modify Login Module page is displayed. You should now see just one login module group listed in the table, Sun Access Manager Realm.
Click Save.
- 6 Log out of Identity Manager console.**

Testing Single Sign-On from Federated Access Manager to Identity Manager

The following figure illustrates the process flow of single sign-on from Federated Access Manager to Identity Manager.

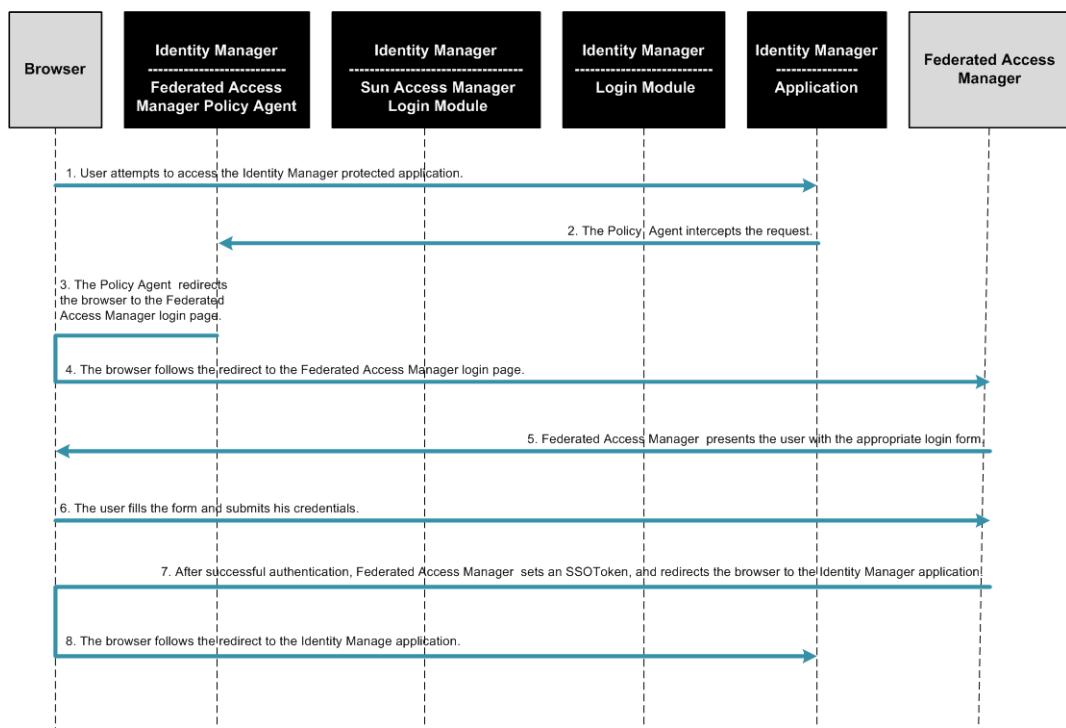


FIGURE 1–3 Single Sign-On Protocol Flow

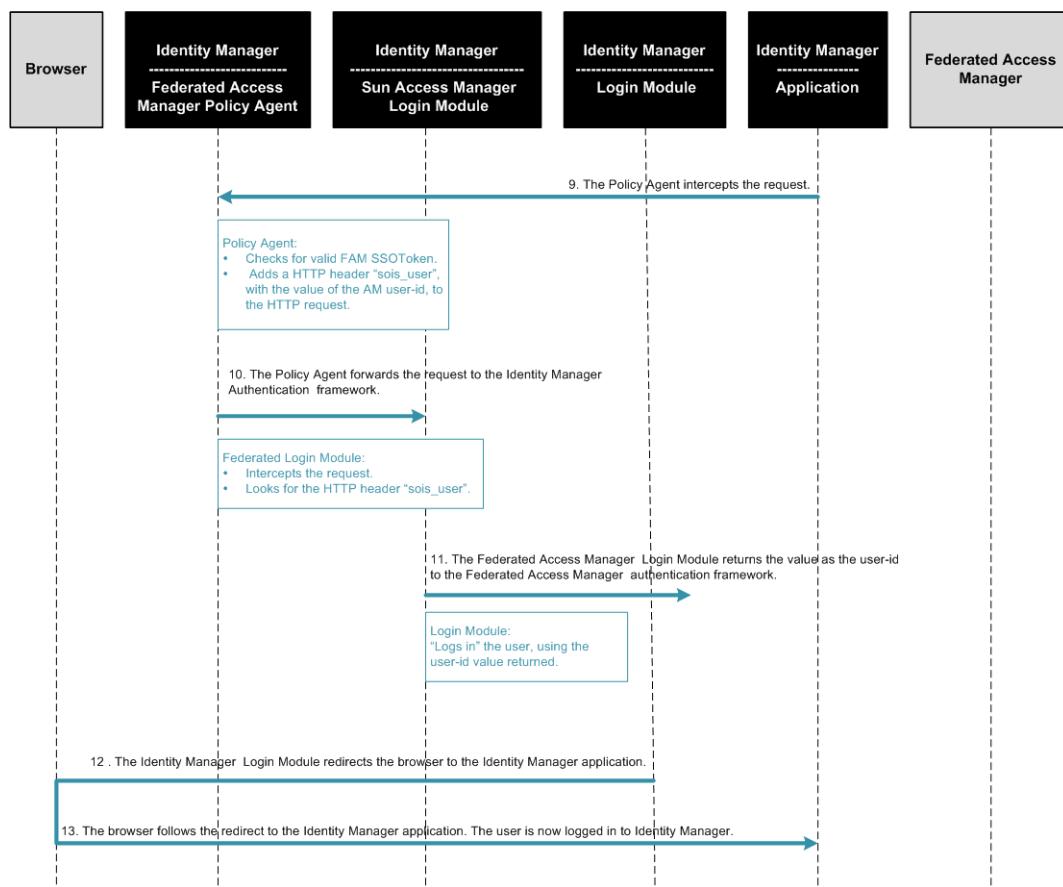


FIGURE 1-4 Single Sign-On Process Flow (continued)

To test single sign-on from Federated Access Manager to Identity Manager, follow these steps:

1. [Re-Enable Protection Identity Manager Protection by the Federated Access Manager Policy Agent](#)
2. [Test Admin-User Single Sign-On Between Federated Access Manager and Identity Manager](#)

▼ To Re-Enable Protection Identity Manager Protection by the Federated Access Manager Policy Agent

1. Log in to the Federated Access Manager Console using the following credentials:

User Name: amadmin

Password: password

- 2 Navigate to Configuration > Agents > J2EE > *agent-name* > Application .**
- 3 For the property Not Enforced URI (com.sun.identity.agents.config.notenforced.uri), remove the following entry that you had earlier added:**
[9]=/idm/*
- 4 Make sure these lines are present:**
[6]=/idm/styles/*

[7]=/idm/includes/*

[8]=/idm/images/*
- 5 Click Save.**
- 6 Log out of the Federated Access Manager Console.**

▼ To Test End-User Single Sign-On Between Federated Access Manager and Identity Manager

- 1 Go to the Federated Access Manager console..**

In this example, go to <http://host1.example.com:2080/idm/user> The Federated Access Manager login page is displayed.

- 2 Log in using the following credentials:**

User Name: idmuser

Password: password

The Identity Manager user page is displayed.

You should be single signed-on to Identity Manager, and should not be prompted for login by Identity Manager.

- 3 Log out of the Identity Manager user page.**

▼ To Test Admin-User Single Sign-On Between Federated Access Manager and Identity Manager

- 1 Go to following Identity Manager URL:

`http://host1.example.com:2080/idm`

The Federated Access Manager login page is displayed.

- 2 Log in using the following credentials:

User Name: idmadmin

Password: password

The Identity Manager console is displayed. You should be single-signed onto Identity Manager, and should not be prompted for login by Identity Manager

- 3 Log out of Identity Manager.

Troubleshooting

To troubleshoot problems with any procedure in this chapter, try the following:

- Inspect Log Files
- View or Change Identity Manager System Settings
- Inspect an Identity Manager Object
- Update an Identity Manager Object
- Consult Forums and Mailing Lists

▼ To Enable Trace in Identity Manager

- 1 Login to the Identity Manager debug interface:

Go to the following URL:

`http://host1.example.com:2080/idm/debug`

Provide the following credentials:

UserName: configurator

Password: configurator

- 2 Click the Show Trace button.

- 3 In the Edit Trace Configuration window, mark Trace Enabled checkbox.**
- 4 Add the following classes, each with a trace level of 4:**
 - com.waveset.adapter.ResourceAdapterBase
 - com.waveset.adapter.SunAccessManagerRealmResourceAdapter
- 5 Click Save.**
- 6 Log out of the Identity Manager debug interface.**

To Inspect Log Files

For the installation described in this chapter, these are the log locations:

- Application Server logs
`/opt/SUNWappserver91/domains/domain1/logs`
In the file:
`/opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm/config/Waveset.properties`
enable this property:
`exception.trace=true`
- Federated Access Manager Client SDK debug logs
`/opt/SUNWappserver91/domains/domain1/logs/am_debug`
- Federated Access Manager Server debug logs
`/opt/fam80-idm80/opensso/debug`
- Federated Access Manager Policy Agent debug logs
`/opt/j2ee_agents/appserver_v9_agent/Agent_001/logs/debug`

To View or Change Identity Manager System Settings

Using Identity Manager Debug Console

URL: <http://host1.example.com:2080/idm/debug>
User Name: configurator
Password: configurator

The following Identity Manager objects were created/modified in this document:

Resource	SunAccessManagerRealm
LoginModGroup	Sun Access Manager Realm
LoginApp	UI_LOGIN_CONFIG_DISPLAY_NAME_USER_INTERFACE UI_LOGIN_CONFIG_DISPLAY_NAME_ADMIN_INTERFACE

You can view, edit, or export Identity Manager objects in `xml` format, or through the Get Object and List Objects buttons.

Using the Identity Manager IDE Interface

Before you begin, disable the Policy Agent on the Identity Manager server. This enables Netbeans to connect to the Identity Manager server.

1. Download Netbeans IDE 6.0. Web & Java EE edition).
 2. Download the Identity Manager IDE plug-in .
 3. Follow the instructions for installing the IDE Plug-in in Netbeans. Go to the following URL:
<https://identitymanageride.dev.java.net/netbeans-setup.html>
- A new IDM menu item appears in the Netbeans menubar.

▼ To Inspect an Identity Manager Object

- 1 Choose the "Custom Identity Manager Objects" in the Project window.
- 2 In the Netbeans menu, choose IDM / Open Object.
- 3 In the Open Object page, do this:

```
Object Name: *
Object Type: <select an object, ex:Resource>
```

You will see that the list of Matching Objects gets populated with the objects of the selected type. In this example, if you select SunAccessManagerRealm, and OK, the object-definition will be downloaded to the project.

To Update an Identity Manager Object

To modify the object, and upload the changed object, right-click on the object in the Project window and select Identity Manager / Upload Object. The following Identity Manager objects were created or modified in this chapter:

Resource	SunAccessManagerRealm
LoginModGroup	Sun Access Manager Realm
LoginApp	User Interface
	Administrator Interface

To Consult Forums and Mailing Lists

- Sun Identity Manager Forum questions
identityManager-technical-questions-ext@sun.com
- Sun Identity Manager IDE Plug-in related questions
<https://identitymanageride.dev.java.net/servlets/ProjectMailingListList>
<https://identitymanageride.dev.java.net/servlets/ProjectForumView>
- Sun Federated Access Manager / Policy Agent questions
amfm-technical-ext@sun.com
- OpenSSO questions
<https://opensso.dev.java.net/servlets/ProjectForumView>

Sample Output

EXAMPLE 1-1 Sample Output from lh Log Program

```
Import init.xml Identity Manager configuration
Getting new session...

*****
Importing file '/opt/SUNWappserver91/domains/domain1/applications/
j2ee-modules/idm/sample/init.xml':

Including file 'sample/sysconfig.xml'.
PKCS#5 encryption set. Server encryption keys re-encrypted.
Restored Configuration:System Configuration
Including file 'sample/certdata.xml'.
Restored UserForm:CertificateDataMainForm
Restored UserForm:CertificateDataAddCertForm
Restored UserForm:CertificateDataForm
Including file 'sample/changelogconfig.xml'.
Restored Configuration:ChangeLog Configuration
Including file 'sample/admingroups.xml'.
Added Configuration:AuthorizationTypes
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored AdminGroup:Admin
Restored AdminGroup>List Admin Roles
Restored AdminGroup:Connect Admin Roles
Restored AdminGroup:Admin Role Administrator
Restored AdminGroup:Approver Administrator
Restored AdminGroup:Organization Approver
Restored AdminGroup:Role Approver
Restored AdminGroup:Resource Approver
Restored AdminGroup>List Capabilities
Restored AdminGroup:Connect Capabilities
Restored AdminGroup:Capability Administrator
Restored AdminGroup:EndUser
Restored AdminGroup:End User Administrator
Restored AdminGroup:Import/Export Administrator
Restored AdminGroup:License Administrator
Restored AdminGroup>Login Administrator
Restored AdminGroup>List Organizations
Restored AdminGroup:Connect Organizations
Restored AdminGroup:Organization Administrator
Restored AdminGroup>List Policies
Restored AdminGroup:Connect Policies
Restored AdminGroup:Policy Administrator
Restored AdminGroup:Reconcile Administrator
Restored AdminGroup:Reconcile Request Administrator
Restored AdminGroup:View Meta View
Restored AdminGroup:Meta View Administrator
Restored AdminGroup:Configure Audit
Restored AdminGroup:Configure Certificates
Restored AdminGroup:Run Report Refs
Restored AdminGroup:Run Admin Report
Restored AdminGroup:Admin Report Administrator
Restored AdminGroup:Run Audit Report
Restored AdminGroup:Audit Report Administrator
Restored AdminGroup:Run Reconcile Report
Restored AdminGroup:Reconcile Report Administrator
Restored AdminGroup:Run Resource Report
Restored AdminGroup:Resource Report Administrator
Restored AdminGroup:Run Risk Analysis
Restored AdminGroup:Risk Analysis Administrator
Restored AdminGroup:Run Role Report
Restored AdminGroup:Role Report Administrator
Restored AdminGroup:Run User Report
Restored AdminGroup:User Report Administrator
Restored AdminGroup:Run Task Report
Restored AdminGroup:Task Report Administrator
Restored AdminGroup:Report Administrator
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored AdminGroup>List Resources
Restored AdminGroup>Connect Resources
Restored AdminGroup>Access Resource UI
Restored AdminGroup>Resource Administrator
Restored AdminGroup>Bulk Resource Administrator
Restored AdminGroup>Resource Object Administrator
Restored AdminGroup>Change Resource Password Administrator
Restored AdminGroup>Bulk Change Resource Password Administrator
Restored AdminGroup>Reset Resource Password Administrator
Restored AdminGroup>Bulk Reset Resource Password Administrator
Restored AdminGroup>Resource Password Administrator
Restored AdminGroup>Bulk Resource Password Administrator
Restored AdminGroup>Change Active Sync Resource Administrator
Restored AdminGroup>Control Active Sync Resource Administrator
Restored AdminGroup>List Resource Groups
Restored AdminGroup>Connect Resource Groups
Restored AdminGroup>Resource Group Administrator
Restored AdminGroup>List Roles
Restored AdminGroup>Connect Roles
Restored AdminGroup>Role Administrator
Restored AdminGroup>List Rules
Restored AdminGroup>Connect Rules
Restored AdminGroup>Connect Capabilities Rules
Restored AdminGroup>Connect Login Constraint Rules
Restored AdminGroup>Connect Controlled Organizations Rules
Restored AdminGroup>Connect Login Correlation Rules
Restored AdminGroup>Connect New User Name Rules
Restored AdminGroup>List User Members Rules
Restored AdminGroup>Connect User Members Rules
Restored AdminGroup>Connect Excluded Accounts Rules
Restored AdminGroup>Connect User Is Assigned Admin Role Rules
Restored AdminGroup>Connect SPE User Is Assigned Admin Role Rules
Restored AdminGroup>Connect SPE Users Search Context Rules
Restored AdminGroup>Connect SPE Users Search Filter Rules
Restored AdminGroup>Connect SPE Users After Search Filter Rules
Restored AdminGroup>Connect Capabilities On SPE User Rules
Restored AdminGroup>View UserUIConfig
Restored AdminGroup>Access User UI
Restored AdminGroup>List User Refs
Restored AdminGroup>User Refs
Restored AdminGroup>List Users
Restored AdminGroup>View User
Restored AdminGroup>Connect Users
Restored AdminGroup>Create User
Restored AdminGroup>Bulk Create User
Restored AdminGroup>Update User
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored AdminGroup:Bulk Update User
Restored AdminGroup:Delete IDM User
Restored AdminGroup:Deprovision User
Restored AdminGroup:Unlink User
Restored AdminGroup:Unassign User
Restored AdminGroup:Delete User
Restored AdminGroup:Bulk Delete IDM User
Restored AdminGroup:Bulk Unassign User
Restored AdminGroup:Bulk Unlink User
Restored AdminGroup:Bulk Deprovision User
Restored AdminGroup:Bulk Delete User
Restored AdminGroup:Enable User
Restored AdminGroup:Bulk Enable User
Restored AdminGroup:Disable User
Restored AdminGroup:Bulk Disable User
Restored AdminGroup:Unlock User
Restored AdminGroup:Rename User
Restored AdminGroup:Change Password Administrator
Restored AdminGroup:Reset Password Administrator
Restored AdminGroup:Password Administrator
Restored AdminGroup:Change Password Administrator (Verification Required)
Restored AdminGroup:Reset Password Administrator (Verification Required)
Restored AdminGroup:Password Administrator (Verification Required)
Restored AdminGroup:Import User
Restored AdminGroup:User Account Administrator
Restored AdminGroup:Bulk User Account Administrator
Restored AdminGroup:Change User Account Administrator
Restored AdminGroup:Bulk Change User Account Administrator
Restored AdminGroup:Assign User Capabilities
Restored AdminGroup:SPML Access
Restored AdminGroup:Account Administrator
Restored AdminGroup:Bulk Account Administrator
Restored AdminGroup:Change Account Administrator
Restored AdminGroup:Bulk Change Account Administrator
Restored AdminGroup>List UserForms
Restored AdminGroup:Connect UserForms
Restored AdminGroup:Security Administrator
Restored AdminGroup:Waveset Administrator
Restored AdminGroup:Remedy Integration Administrator
Restored AdminGroup:Auditor View User
Restored AdminGroup>List Audit Policies
Restored AdminGroup:Connect Audit Policies
Restored AdminGroup:Assign User Audit Policies
Restored AdminGroup:Assign Organization Audit Policies
Restored AdminGroup:Assign Audit Policies
Restored AdminGroup:Audit Policy Administrator
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored AdminGroup:Run Audited Attribute Report
Restored AdminGroup:Audited Attribute Report Administrator
Restored AdminGroup:Run User Access Report
Restored AdminGroup:User Access Report Administrator
Restored AdminGroup:Run AuditLog Report
Restored AdminGroup:AuditLog Report Administrator
Restored AdminGroup:Run Policy Summary Report
Restored AdminGroup:Policy Summary Report Report Administrator
Restored AdminGroup:Run Audit Policy Scan Report
Restored AdminGroup:Audit Policy Scan Report Administrator
Restored AdminGroup:Run AuditPolicy Violation History
Restored AdminGroup:AuditPolicy Violation History Administrator
Restored AdminGroup:Run Organization Violation History
Restored AdminGroup:Organization Violation History Administrator
Restored AdminGroup:Run Resource Violation History
Restored AdminGroup:Resource Violation History Administrator
Restored AdminGroup:Run Violation Summary Report
Restored AdminGroup:Violation Summary Report Administrator
Restored AdminGroup:Run Separation of Duties Report
Restored AdminGroup:Separation of Duties Report Administrator
Restored AdminGroup:Run Access Review Summary Report
Restored AdminGroup:Access Review Summary Report Administrator
Restored AdminGroup:Run Access Review Detail Report
Restored AdminGroup:Access Review Detail Report Administrator
Restored AdminGroup:Run Auditor Report
Restored AdminGroup:Auditor Report Administrator
Restored AdminGroup:Auditor Remediator
Restored AdminGroup:Auditor Attestor
Restored AdminGroup:Auditor Access Scan Administrator
Restored AdminGroup:Auditor Periodic Access Review Administrator
Restored AdminGroup:Auditor Administrator
Including file 'sample/adminroles.xml'.
Restored AdminRole:User
Including file 'sample/admins.xml'.
Restored User:Configurator
Restored User:Administrator
Restored User:Reset
Including file 'sample/enduserobjects.xml'.
Restored ObjectGroup:End User
Restored Rule:End User Controlled Organizations
Including file 'sample/loginconfig.xml'.
Restored LoginConfig:Waveset Login Configuration
Added LoginModGroup:Default Lighthouse Id/Pwd Login Module Group
Added LoginModGroup:Default Lighthouse Id/Questions Login Module Group
Added LoginModGroup:Default Lighthouse X509 Cert Login Module Group
Added LoginApp:Administrator Interface
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Added LoginApp:BPE
Added LoginApp:User Interface
Added LoginApp:Secondary Authentication Interface
Added LoginApp:Command Line Interface
Added LoginApp:DefaultUser
Added LoginApp:IVR Interface
Including file 'sample/auditconfig.xml'.
Preserving object Configuration #ID#Configuration:AuditConfiguration
Restored Configuration:Audit Configuration
Restored Configuration:WorkflowDetailsRecordForm
Restored Configuration:LogRecordForm
Restored UserForm:AuditMainForm
Restored UserForm:AuditGroupEditForm
Restored UserForm:AuditPublisherForm
Restored Configuration:AuditConfigForm
Including file 'sample/remedyconfig.xml'.
Added Configuration:Remedy Workflow Process
Added TaskDefinition:Test Remedy Template Workflow
Restored Configuration:RemedyTemplateForm
Including file 'sample/serverkeys.xml'.
Restored TaskDefinition:Server Encryption
Including file 'sample/metaView.xml'.
Restored MetaView:User Meta View
Including file 'sample/auditorforms.xml'.
Preserving object Rule #ID#Rule:ViolationPriority
Preserving object Rule #ID#Rule:ViolationSeverity
Restored UserForm:AuditPolicyLibrary
Restored UserForm:AuditorFormLibrary
Added UserForm:Audit Policy List
Added UserForm:Audit Policy Delete Confirmation Form
Restored UserForm:Audit Policy Form
Restored UserForm:Update Audit Policy Form
Added UserForm:Remediation Library
Restored UserForm:Bulk Remediation
Restored UserForm:Sign Bulk Remediation
Restored Rule:ViolationPriority
Restored Rule:ViolationSeverity
Restored UserForm:Remediation List
Restored Configuration:AuditorOrgForm
Restored UserForm:Violation Detail Form
Restored UserForm:Compliance Violation Summary Form
Restored UserForm:Conflict Violation Details Form
Restored UserForm:Auditor Tab
Restored UserForm:Remediation Form
Restored Configuration:User Extended Attributes
Restored AttributeDefinition:accountId
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored AttributeDefinition:password
Restored AttributeDefinition:fullname
Restored AttributeDefinition:email
Restored AttributeDefinition:lastname
Restored AttributeDefinition:firstname
Restored UserForm:Example Form
Restored TaskDefinition:Password Expiration
Restored Configuration:SoapConfig
Restored ResourceAction:Example Login Action
Restored ResourceAction:Example Logoff Action
Restored TaskDefinition:LoadTask
Restored TaskDefinition:ImportTask
Restored Configuration:Reconcile Configuration
Including file 'sample/userSearchDefaults.xml'.
Added UserForm:User Search Defaults
Including file 'sample/userActionsConfig.xml'.
Restored Configuration:User Actions Configuration
Including file 'sample/findObjectsDefaults.xml'.
Restored Configuration:Find Objects Defaults
Including file 'sample/approvalforms.xml'.
Including file 'sample/AdminDashboard.xml'.
Restored UserForm:Admin Dashboard
Including file 'sample/otherWorkItems.xml'.
Restored UserForm:Other Work Item List
Including file 'sample/emailTemplates.xml'.
Restored EmailTemplate:Password Reset
Restored EmailTemplate:Temporary Password Reset
Restored EmailTemplate:Request Resource
Restored EmailTemplate:Retry Notification
Restored EmailTemplate:Risk Analysis
Restored EmailTemplate:Report
Restored EmailTemplate:User ID Recovery
Including file 'sample/policy.xml'.
Preserving object Policy #ID#PasswordPolicy
Preserving object Policy #ID#AccountIdPolicy
Preserving object Policy #ID#Windows2000PasswordPolicy
Preserving object Policy #ID#Policy.DefaultLighthouseAccount
Preserving object Policy #ID#Policy.LdapDnAccount
Restored Policy:Password Policy
Restored Policy:AccountId Policy
Restored Policy:Windows 2000 Password Policy
Restored Policy:Default Identity Manager Account Policy
Restored Policy:LDAP DN Account Policy
Including file 'sample/deferredtasks.xml'.
Added TaskDefinition:Deferred Task Scanner
Added TaskDefinition:Start Date
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Added TaskDefinition:Sunset Date
Including file 'sample/formlib.xml'.
Added UserForm:Default User Library
Added UserForm:Password Library
Added UserForm:Questions Library
Added UserForm:Account Summary Library
Added UserForm:Account Link Library
Added UserForm:Administrator Library
Added UserForm:User Library
Added UserForm:Organization Library
Added UserForm:Locale Selection Library
Added UserForm:Approval Library
Added UserForm:Scalable Selection Library
Added Rule:Role Names
Added Rule:Organization Names
Added Rule:Resource Names
Including file 'sample/treetableLibrary.xml'.
Added Configuration:Tree Table Library
Including file 'sample/forms.xml'.
Not saving object UserForm #ID#UserForm:DefaultUserForm: not found
Not saving object UserForm #ID#UserForm:RenameUserForm: not found
Not saving object UserForm #ID#UserForm:ChangeUserPasswordForm: not found
Not saving object UserForm #ID#UserForm:ReprovisionForm: not found
Not saving object UserForm #ID#UserForm:DeprovisionForm: not found
Not saving object UserForm #ID#UserForm:DisableForm: not found
Not saving object UserForm #ID#UserForm:EnableForm: not found
Not saving object UserForm #ID#UserForm:UnlockForm: not found
Not saving object UserForm #ID#UserForm:ResetUserPasswordForm: not found
Not saving object UserForm #ID#UserForm:UserFormLibrary: not found
Not saving object Configuration #ID#Configuration:UserFormLibrary: not found
Restored UserForm:Default User Form
Added UserForm:Default View User Form
Restored UserForm:Select Accounts Form
Added UserForm:Tabbed User Form
Added UserForm:Tabbed View User Form
Added UserForm:Wizard User Form
Added UserForm:Wizard View User Form
Restored UserForm:Reprovision Form
Restored UserForm:Deprovision Form
Restored UserForm:Disable Form
Restored UserForm:Enable Form
Restored UserForm:Unlock Form
Restored UserForm:Change My Password Form
Restored UserForm:Change User Password Form
Restored UserForm:Reset User Password Form
Restored UserForm:Rename User Form
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored UserForm:User Form Library
Restored Configuration:User Form Library
Restored Configuration:Role Rename Form
Restored Configuration:Role Form
Restored Configuration:Resource Group Rename Form
Restored Configuration:Application Form
Added UserForm>List Resource Groups
Restored Configuration:Lighthouse Policy Rename Form
Restored Configuration:Lighthouse Policy Form
Restored UserForm>Change User Capabilities Form
Restored UserForm>Change User Audit Policies Form
Restored UserForm>Change Organization Audit Policies Form
Restored Configuration>Organization Rename Form
Restored Configuration>Organization Form
Restored Configuration>Directory Junction Form
Restored Configuration>Virtual Organization Form
Restored Configuration>Virtual Organization Refresh Form
Restored Configuration>Capability Form
Restored Configuration>Admin Role Form
Restored UserForm>Managed Resources Form
Restored UserForm>Form and Process Mappings Form
Restored UserForm>Empty Form
Restored Configuration>Find Objects Form
Restored Configuration>Find Objects Results Form
Restored UserForm>User Interface Configuration Form
Restored UserForm>Delegate WorkItems
Restored UserForm>Lookup UserId
Including file 'sample/configforms.xml'.
Added UserForm>Confirm Deletes
Added UserForm>List Rules
Added UserForm>Expression Editor
Added UserForm>Edit Rule
Added UserForm>Edit Argument
Added UserForm>List Forms
Added UserForm>Edit Form
Added UserForm>Display Component Fields
Added UserForm>Edit Field
Including file 'sample/sysforms.xml'.
Not saving object UserForm #ID#UserForm:TaskScheduleForm: not found
Restored UserForm>Work Item Confirmation
Restored UserForm>Work Item List
Restored UserForm>Task Schedule Form
Restored Configuration>SyslogRecordForm
Including file 'sample/userFind.xml'.
Not saving object UserForm #ID#UserForm:UserSearchLibrary: not found
Not saving object UserForm #ID#UserForm:AdvancedFindUserForm: not found
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Not saving object UserForm #ID#UserForm:FindUserForm: not found
Not saving object UserForm #ID#UserForm:FindUserResultsForm: not found
Not saving object UserForm #ID#UserForm:UserSelectionForm: not found
Not saving object UserForm #ID#UserForm:FindAccountOwnerForm: not found
Not saving object UserForm #ID#UserForm:AccountOwnerSelectionForm: not found
Restored UserForm:User Search Library
Restored UserForm:Advanced Find User Form
Restored UserForm:Find User Form
Restored UserForm:Find User Results Form
Restored UserForm:User Selection Form
Restored UserForm:Find Account Owner Form
Restored UserForm:Account Owner Selection Form
Including file 'sample/userListForm.xml'.
Restored UserForm:User List Library
Restored UserForm:User List Form
Including file 'sample/accountFind.xml'.
Not saving object UserForm #ID#UserForm:AccountSearchLibrary: not found
Not saving object UserForm #ID#UserForm:FindAccountForm: not found
Not saving object UserForm #ID#UserForm:FindAccountResultsForm: not found
Restored UserForm:Account Search Library
Restored UserForm:Find Account Form
Restored UserForm:Find Account Results Form
Including file 'sample/loginForms.xml'.
Added UserForm:Login App List
Restored Configuration>Login App Rename Form
Restored Configuration>Login App View Form
Added UserForm:Login Mod Group List
Restored Configuration>Login Mod Group Rename Form
Restored Configuration>Login Mod Group View Form
Restored Configuration>Login Module Edit Form
Added Rule:Sample On Local Network
Including file 'sample/metaViewForms.xml'.
Restored UserForm>Edit Meta View
Restored UserForm>Edit Meta Events
Restored UserForm:Meta View Library
Restored UserForm>List Builder Library
Restored UserForm>Edit Meta View Attribute
Restored UserForm>Edit Meta View Attribute Target
Restored UserForm>Edit Meta Event
Restored UserForm>Edit Meta Event Response
Restored UserForm>Confirm Meta View Attribute Deletes
Restored UserForm>Import Meta View
Restored UserForm>Configure MetaView from Resource Changes
Restored UserForm>Continue To Meta View From Resource
Restored UserForm>Meta View Password Generation
Including file 'sample/changelogconfigForms.xml'.
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored UserForm>Edit ChangeLog Configuration
Restored UserForm>Edit ChangeLog Policy
Restored UserForm>Edit ChangeLog
Including file 'sample/workflow.xml'.
Not saving object ProvisioningTask Create User: not found
Not saving object TaskDefinition Update User: not found
Not saving object TaskDefinition Delete User: not found
Not saving object TaskDefinition Disable User: not found
Not saving object TaskDefinition Enable User: not found
Not saving object TaskDefinition Rename User: not found
Not saving object TaskDefinition Change User Password: not found
Not saving object TaskDefinition Reset User Password: not found
Not saving object TaskDefinition Delete Resource Account: not found
Not saving object TaskDefinition Password Login: not found
Not saving object TaskDefinition Question Login: not found
Not saving object TaskDefinition Create Resource Object: not found
Not saving object TaskDefinition Update Resource Object: not found
Not saving object TaskDefinition Delete Resource Object: not found
Not saving object UserForm #ID#UserForm:ApprovalForm: not found
Including file 'sample/wfutil.xml'.
Added Configuration:Rename Task
Added Configuration:Parse Result
Added Configuration:Update View
Added Configuration:Update User View
Added Configuration:Set Password
Added Configuration:Update User Object
Added Configuration:Move User
Added Configuration:Sunrise Via Work Item
Added Configuration:Sunset
Added Configuration:Derive Date
Added Configuration:Data Transformation
Including file 'sample/wfapproval.xml'.
Preserving object EmailTemplate #ID#EmailTemplate:ProvisioningApproval
Preserving object EmailTemplate #ID#EmailTemplate:DeprovisioningApproval
Preserving object EmailTemplate #ID#EmailTemplate:ProvisioningNotification
Preserving object EmailTemplate #ID#EmailTemplate:DeprovisioningNotification
Preserving object EmailTemplate #ID#EmailTemplate:AccountUpdateNotification
Added Configuration:Approval
Restored UserForm:Approval Form
Added Rule:Approval Transaction Message
Added Rule:Approval Transaction Message Helper
Restored EmailTemplate:Account Creation Approval
Restored EmailTemplate:Account Deletion Approval
Restored EmailTemplate:Account Creation Notification
Restored EmailTemplate:Account Deletion Notification
Restored EmailTemplate:Account Update Notification
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Added Configuration:Multi Approval
Added Configuration:Approval Evaluator
Added Configuration:Notify
Added Configuration:Approval Notification Evaluator
Added Configuration:Notification Evaluator
Added Configuration:Lighthouse Approvals
Added Configuration:Provisioning Notification
Restored UserForm:Sunrise Form
Restored TaskDefinition:Approver Report
Including file 'sample/wfprovisioning.xml'.
Added Configuration:Provision With Retries
Updated EmailTemplate:Retry Notification
Added Configuration:Provision
Added Configuration:DeProvision
Added Configuration:Bulk Provision
Including file 'sample/wfrecon.xml'.
Added TaskDefinition:Audit Native Change To Account Attributes
Added TaskDefinition:Notify Reconcile Start
Added TaskDefinition:Notify Reconcile Response
Added TaskDefinition:Notify Reconcile Finish
Including file 'sample/wfresource.xml'.
Added Configuration:Resource Object Retries
Restored Configuration:Resource Policy
Added TaskDefinition:Create Resource Object
Added TaskDefinition:Update Resource Object
Added TaskDefinition:Delete Resource Object
Added TaskDefinition:Create Resource Group
Added TaskDefinition:Update Resource Group
Added TaskDefinition:Delete Resource Group
Added TaskDefinition:Create Resource Organization
Added TaskDefinition:Update Resource Organization
Added TaskDefinition:Delete Resource Organization
Added TaskDefinition:Create Resource Organizational Unit
Added TaskDefinition:Update Resource Organizational Unit
Added TaskDefinition:Delete Resource Organizational Unit
Added TaskDefinition:Create Resource Person
Added TaskDefinition:Update Resource Person
Added TaskDefinition:Delete Resource Person
Added TaskDefinition:Create Resource User
Added TaskDefinition:Update Resource User
Added TaskDefinition:Delete Resource User
Added Rule:Unix Excluded Resource Accounts
Added Rule:Windows Excluded Resource Accounts
Added Rule:Microsoft SQL Server Excluded Resource Accounts
Added Rule:Sun Access Manager Excluded Resource Accounts
Including file 'sample/wfuser.xml'.
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Added ProvisioningTask>Create User
Added TaskDefinition>Update User
Added TaskDefinition>Delete User
Added TaskDefinition>Disable User
Added TaskDefinition>Move User
Added TaskDefinition>Enable User
Added TaskDefinition>Unlock User
Added TaskDefinition>Rename User
Added TaskDefinition>Change User Password
Added TaskDefinition>Reset User Password
Added TaskDefinition>Password Login
Added TaskDefinition>Question Login
Added TaskDefinition>Change Resource Account Password
Added TaskDefinition>Handle LDAP Modify DN
Added TaskDefinition>Complete Sunrise Account Deferred
Including file 'sample/wfsystem.xml'.
Added TaskDefinition>Manage Role
Added TaskDefinition>Manage Resource
Including file 'sample/taskconfig.xml'.
Preserving object UserForm #ID#TaskTemplate>CreateUser
Preserving object UserForm #ID#TaskTemplate>UpdateUser
Preserving object UserForm #ID#TaskTemplate>DeleteUser
Including file 'sample/forms/TemplateFormLibrary.xml'.
Restored UserForm:Template Form Library
Including file 'sample/forms/CreateUserTaskTemplateForm.xml'.
Restored UserForm>Create User Template Form
Restored TaskTemplate>Create User Template
Including file 'sample/forms/DeleteUserTaskTemplateForm.xml'.
Restored UserForm>Delete User Template Form
Restored TaskTemplate>Delete User Template
Including file 'sample/forms/UpdateUserTaskTemplateForm.xml'.
Added UserForm>Update User Template Form
Restored TaskTemplate>Update User Template
Including file 'sample/enduser.xml'.
Not saving object UserForm #ID#UserForm>EndUserMenu: not found
Not saving object UserForm #ID#UserForm>AnonymousUserMenu: not found
Not saving object UserForm #ID#UserForm>End User Form: not found
Not saving object UserForm #ID#UserForm>AnonymousUserLogin: not found
Not saving object UserForm #ID#UserForm>ChangePasswordForm: not found
Not saving object UserForm #ID#UserForm>ResetPasswordForm: not found
Not saving object UserForm #ID#UserForm>ExpiredLoginForm: not found
Not saving object UserForm #ID#UserForm>QuestionLoginForm: not found
Not saving object Configuration EndUserRuleLibrary: not found
Preserving object Configuration #ID#Configuration>EndUserResources
Preserving object Configuration #ID#Configuration>EndUserTasks
Including file 'sample/enduserlib.xml'.
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Added Configuration:EndUserRuleLibrary
Including file 'sample/rules/ResourceFormRules.xml'.
Added Configuration:ResourceFormRuleLibrary
Including file 'sample/rules/RegionalConstants.xml'.
Added Configuration:Regional Constants
Including file 'sample/forms/ADUserForm.xml'.
Added UserForm:AD User Form
Including file 'sample/forms/AIXUserForm.xml'.
Added UserForm:AIX User Form
Including file 'sample/forms/HP-UXUserForm.xml'.
Added UserForm:HP-UX User Form
Including file 'sample/forms/LDAPUserForm.xml'.
Added UserForm:LDAP User Form
Including file 'sample/forms/NDSUserForm.xml'.
Added UserForm:NDS User Form
Including file 'sample/forms/SolarisUserForm.xml'.
Added UserForm:Solaris User Form
Including file 'sample/forms/SUSELinuxUserForm.xml'.
Added UserForm:SUSE Linux User Form
Including file 'sample/forms/RedHatLinuxUserForm.xml'.
Added UserForm:Red Hat Linux User Form
Restored Configuration:End User Resources
Restored Configuration:End User Tasks
Restored Configuration:Anonymous User Tasks
Restored UserForm:End User Empty Form
Restored UserForm:End User Menu
Restored UserForm:Anonymous User Menu
Restored UserForm:Anonymous User Login
Restored UserForm:End User Form
Restored UserForm:Basic Change Password Form
Restored UserForm:Change Password Form
Restored UserForm:Expired Login Form
Restored UserForm:Login Change User Answers Form
Restored UserForm:Question Login Form
Restored UserForm:Change User Answers Form
Added UserForm:End User Field Library
Added UserForm:End User Dynamic Resource Forms
Added UserForm:Self Discovery
Added UserForm:End User Launch List
Added UserForm:End User Work Item List
Added UserForm:End User Other Work Item List
Added UserForm:End User Work Item Edit
Added UserForm:End User Work Item List Ext
Added UserForm:End User Work Item Confirmation Ext
Restored UserForm:End User Approvals List
Restored UserForm:End User Approvals Confirmation
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Added UserForm:End User Task List
Added UserForm:End User Task Results
Restored UserForm:End User View WorkItem Delegations
Restored UserForm:End User Past WorkItem Delegations
Restored UserForm:End User Delegate WorkItems
Restored UserForm:End User Access Privileges
Restored UserForm:End User Dashboard
Restored UserForm:End User Navigation
Restored UserForm:End User Request Menu
Added Configuration:End User Update View
Added TaskDefinition:End User Update My Resources
Added TaskDefinition:End User Update My Roles
Added TaskDefinition:End User Update Resources
Added TaskDefinition:End User Update Roles
Restored UserForm:End User Anonymous Enrollment Completed Form
Restored UserForm:End User Anonymous Enrollment Validation Form
Restored UserForm:End User Anonymous Enrollment Completion Form
Restored UserForm:End User Anonymous Enrollment Form
Added TaskDefinition:End User Anonymous Enrollment
Restored EmailTemplate:End User Anonymous Enrollment Template
Including file 'sample/UserUIConfig.xml'.
Restored Configuration:UserUIConfig
Including file 'sample/reporttasks.xml'.
Added UserForm:Report Form Library
Added UserForm:Syslog Form Library
Restored TaskDefinition:AuditLog Report
Restored TaskDefinition:Historical User Changes Report
Restored TaskDefinition:Syslog Report
Restored TaskDefinition:Usage Report
Restored TaskDefinition:Role Report
Restored TaskDefinition:Admin Role Report
Restored TaskDefinition:User Report
Restored TaskDefinition:User Question Report
Restored TaskDefinition:Administrator Report
Restored TaskDefinition:Task Report
Restored TaskDefinition:LogTamperingReport
Restored TaskDefinition:Resource User Report
Restored TaskDefinition:Resource Group Report
Restored TaskDefinition:Default User Audit Report
Restored TaskDefinition:Account Index Summary
Restored TaskDefinition:Workflow Summary Report
Restored TaskDefinition:AuditLog Maintenance Task
Restored TaskDefinition:System Log Maintenance Task
Restored TaskDefinition:Resource Status Report
Including file 'sample/synchronization.xml'.
Added TaskDefinition:Resource Role Synchronizer
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored TaskDefinition:SourceAdapterTask
Restored TaskDefinition:IDM Synchronization
Restored TaskDefinition:IDMXUser Synchronization
Added Rule:supportedSyncObjectTypesForResource
Added Rule:getAvailableServerOptions
Restored UserForm:Synchronization Policy Edit
Including file 'sample/defaultreports.xml'.
Preserving object TaskTemplate #ID#TaskTemplate:PasswordChangeUsage
Preserving object TaskTemplate #ID#TaskTemplate:PasswordResetUsage
Preserving object TaskTemplate #ID#TaskTemplate:AccountsDeletedAudit
Preserving object TaskTemplate #ID#TaskTemplate:AccountsCreatedUsage
Preserving object TaskTemplate #ID#TaskTemplate:AccountsDeletedUsage
Preserving object TaskTemplate #ID#TaskTemplate:AllRoles
Preserving object TaskTemplate #ID#TaskTemplate:AllAdminRoles
Preserving object TaskTemplate #ID#TaskTemplate:AllAdministrators
Preserving object TaskTemplate #ID#TaskTemplate:AllUsers
Preserving object TaskTemplate #ID#TaskTemplate:WeeklyActivityAudit
Preserving object TaskTemplate #ID#TaskTemplate:DailyActivityAudit
Preserving object TaskTemplate #ID#TaskTemplate:ResPasswordResetAudit
Preserving object TaskTemplate #ID#TaskTemplate:ResAcctCreateAudit
Preserving object TaskTemplate #ID#TaskTemplate:ResPasswordChangeAudit
Preserving object TaskTemplate #ID#TaskTemplate:WeeklySystemMessages
Preserving object TaskTemplate #ID#TaskTemplate:MyDirectEmployeeSummary
Preserving object TaskTemplate #ID#TaskTemplate:MyDirectIndirectEmployeeSummary
Preserving object TaskTemplate #ID#TaskTemplate:MyDirectEmployeeDetail
Preserving object TaskTemplate #ID#TaskTemplate:MyDirectIndirectEmployeeDetail
Preserving object TaskTemplate #ID#TaskTemplate:HistoricalUserChangesTemplate
Restored TaskTemplate:Resource Accounts Deleted List
Restored TaskTemplate:All Administrators
Restored TaskTemplate:All Roles
Restored TaskTemplate:All Admin Roles
Restored TaskTemplate:All Users
Restored TaskTemplate:Today's Activity
Restored TaskTemplate:Resource Accounts Created List
Restored TaskTemplate:Resource Password Change List
Restored TaskTemplate:Resource Password Resets List
Restored TaskTemplate:Historical User Changes Report
Restored TaskTemplate:Weekly Activity
Restored TaskTemplate:Password Change Chart
Restored TaskTemplate:Password Reset Chart
Restored TaskTemplate:Created Resource Accounts Chart
Restored TaskTemplate:Deleted Resource Accounts Chart
Restored TaskTemplate:Recent System Messages
Restored TaskTemplate:My Direct and Indirect Employee Detail
Restored TaskTemplate:My Direct Employee Detail
Restored TaskTemplate:My Direct Employee Summary
```

EXAMPLE 1-1 Sample Output from `lh Log` Program *(Continued)*

```
Restored TaskTemplate:My Direct and Indirect Employee Summary
Including file 'sample/tickerconfig.xml'.
Restored Configuration:TickerConfig
Including file 'sample/redirectFilterConfig.xml'.
Restored Configuration:Redirect Filter Configuration
Including file 'sample/resourceforms.xml'.
Including file 'sample/forms/AccessManagergroupcreate.xml'.
Added ResourceForm:Access Manager Create Group Form
Including file 'sample/forms/AccessManagergroupupdate.xml'.
Added ResourceForm:Access Manager Update Group Form
Including file 'sample/forms/ADgroupcreate.xml'.
Added ResourceForm:Windows Active Directory Create Group Form
Including file 'sample/forms/ADgroupupdate.xml'.
Added ResourceForm:Windows Active Directory Update Group Form
Including file 'sample/forms/ADorganizationalunitupdate.xml'.
Added ResourceForm:Windows Active Directory Update Organizational Unit Form
Including file 'sample/forms/ADorganizationalunitcreate.xml'.
Added ResourceForm:Windows Active Directory Create Organizational Unit Form
Including file 'sample/forms/ADcontainercreate.xml'.
Added ResourceForm:Windows Active Directory Create Container Form
Including file 'sample/forms/ADcontainerupdate.xml'.
Added ResourceForm:Windows Active Directory Update Container Form
Including file 'sample/forms/ADpersoncreate.xml'.
Added ResourceForm:Windows Active Directory Create User Form
Including file 'sample/forms/ADpersonupdate.xml'.
Added ResourceForm:Windows Active Directory Update User Form
Including file 'sample/forms/AIXgroupcreate.xml'.
Added ResourceForm:AIX Create Group Form
Including file 'sample/forms/AIXgroupupdate.xml'.
Added ResourceForm:AIX Update Group Form
Including file 'sample/forms/SP2groupcreate.xml'.
Added ResourceForm:SP2 Create Group Form
Including file 'sample/forms/SP2groupupdate.xml'.
Added ResourceForm:SP2 Update Group Form
Including file 'sample/forms/HP-UXgroupcreate.xml'.
Added ResourceForm:HP-UX Create Group Form
Including file 'sample/forms/HP-UXgroupupdate.xml'.
Added ResourceForm:HP-UX Update Group Form
Including file 'sample/forms/LDAPgroupcreate.xml'.
Added ResourceForm:LDAP Create Group Form
Including file 'sample/forms/LDAPgroupupdate.xml'.
Added ResourceForm:LDAP Update Group Form
Including file 'sample/forms/LDAPOrganizationcreate.xml'.
Added ResourceForm:LDAP Create Organization Form
Including file 'sample/forms/LDAPOrganizationupdate.xml'.
Added ResourceForm:LDAP Update Organization Form
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Including file 'sample/forms/LDAPorganizationalunitcreate.xml'.
Added ResourceForm:LDAP Create Organizational Unit Form
Including file 'sample/forms/LDAPorganizationalunitupdate.xml'.
Added ResourceForm:LDAP Update Organizational Unit Form
Including file 'sample/forms/LDAPPersoncreate.xml'.
Added ResourceForm:LDAP Create Person Form
Including file 'sample/forms/LDAPPersonupdate.xml'.
Added ResourceForm:LDAP Update Person Form
Including file 'sample/forms/LDAPPosixGroupCreate.xml'.
Added ResourceForm:LDAP Create Posix Group Form
Including file 'sample/forms/LDAPPosixGroupUpdate.xml'.
Added ResourceForm:LDAP Update Posix Group Form
Including file 'sample/forms/SAPPortalgroupcreate.xml'.
Added ResourceForm:SAP Enterprise Portal Create Group Form
Including file 'sample/forms/SAPPortalgroupupdate.xml'.
Added ResourceForm:SAP Enterprise Portal Update Group Form
Including file 'sample/forms/SAPPortalroleupdate.xml'.
Added ResourceForm:SAP Enterprise Portal Update Role Form
Including file 'sample/forms/SunAMCreateFilteredGroupForm.xml'.
Added ResourceForm:Sun Access Manager Create Filtered Group Form
Including file 'sample/forms/SunAMUpdateFilteredGroupForm.xml'.
Added ResourceForm:Sun Access Manager Update Filtered Group Form
Including file 'sample/forms/SunAMCreateDynamicGroupForm.xml'.
Added ResourceForm:Sun Access Manager Create Dynamic Subscription Group Form
Including file 'sample/forms/SunAMUpdateDynamicGroupForm.xml'.
Added ResourceForm:Sun ONE Identity Server Update Dynamic Subscription Group Form
Including file 'sample/forms/SunAMCreateStaticGroupForm.xml'.
Added ResourceForm:Sun Access Manager Create Static Subscription Group Form
Including file 'sample/forms/SunAMUpdateStaticGroupForm.xml'.
Added ResourceForm:Sun Access Manager Update Static Subscription Group Form
Including file 'sample/forms/SunAMCreateRoleForm.xml'.
Added ResourceForm:Sun Access Manager Create Role Form
Including file 'sample/forms/SunAMUpdateRoleForm.xml'.
Added ResourceForm:Sun Access Manager Update Role Form
Including file 'sample/forms/SunAMCreateOrganizationForm.xml'.
Added ResourceForm:Sun Access Manager Create Organization Form
Including file 'sample/forms/SunAMUpdateOrganizationForm.xml'.
Added ResourceForm:Sun Access Manager Update Organization Form
Including file 'sample/forms/SunAMRealmCreateGroupForm.xml'.
Added ResourceForm:Sun Access Manager Realm Create Group Form
Including file 'sample/forms/SunAMRealmUpdateGroupForm.xml'.
Added ResourceForm:Sun Access Manager Realm Update Group Form
Including file 'sample/forms/SunAMRealmCreateRoleForm.xml'.
Added ResourceForm:Sun Access Manager Realm Create Role Form
Including file 'sample/forms/SunAMRealmUpdateRoleForm.xml'.
Added ResourceForm:Sun Access Manager Realm Update Role Form
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Including file 'sample/forms/SunAMRealmCreateFilteredRoleForm.xml'.
Added ResourceForm:Sun Access Manager Realm Create Filtered Role Form
Including file 'sample/forms/SunAMRealmUpdateFilteredRoleForm.xml'.
Added ResourceForm:Sun Access Manager Realm Update Filtered Role Form
Including file 'sample/forms/NDSgroupcreate.xml'.
Added ResourceForm:Netware NDS Create Group Form
Including file 'sample/forms/NDSgroupupdate.xml'.
Added ResourceForm:NetWare NDS Update Group Form
Including file 'sample/forms/NDSorganizationcreate.xml'.
Added ResourceForm:NetWare NDS Create Organization Form
Including file 'sample/forms/NDSorganizationupdate.xml'.
Added ResourceForm:NetWare NDS Update Organization Form
Including file 'sample/forms/NDSorganizationalunitcreate.xml'.
Added ResourceForm:NetWare NDS Create Organizational Unit Form
Including file 'sample/forms/NDSorganizationalunitupdate.xml'.
Added ResourceForm:NetWare NDS Update Organizational Unit Form
Including file 'sample/forms/NISgroupcreate.xml'.
Added ResourceForm:NIS Create Group Form
Including file 'sample/forms/NISgroupupdate.xml'.
Added ResourceForm:NIS Update Group Form
Including file 'sample/forms/NTgroupcreate.xml'.
Added ResourceForm:Windows NT Create Group Form
Including file 'sample/forms/NTgroupupdate.xml'.
Added ResourceForm:Windows NT Update Group Form
Including file 'sample/forms/RedHatLinuxgroupcreate.xml'.
Added ResourceForm:Red Hat Linux Create Group Form
Including file 'sample/forms/RedHatLinuxgroupupdate.xml'.
Added ResourceForm:Red Hat Linux Update Group Form
Including file 'sample/forms/Siebelpositioncreate.xml'.
Added ResourceForm:Siebel Create Position Form
Including file 'sample/forms/Siebelpositionupdate.xml'.
Added ResourceForm:Siebel Update Position Form
Including file 'sample/forms/SiteMinderLDAPgroupcreate.xml'.
Added ResourceForm:SiteMinderLDAP Create Group Form
Including file 'sample/forms/SiteMinderLDAPgroupupdate.xml'.
Added ResourceForm:SiteMinderLDAP Update Group Form
Including file 'sample/forms/SiteMinderLDAPorganizationcreate.xml'.
Added ResourceForm:SiteMinderLDAP Create Organization Form
Including file 'sample/forms/SiteMinderLDAPorganizationupdate.xml'.
Added ResourceForm:SiteMinderLDAP Update Organization Form
Including file 'sample/forms/SiteMinderLDAPorganizationalunitcreate.xml'.
Added ResourceForm:SiteMinderLDAP Create Organizational Unit Form
Including file 'sample/forms/SiteMinderLDAPorganizationalunitupdate.xml'.
Added ResourceForm:SiteMinderLDAP Update Organizational Unit Form
Including file 'sample/forms/Solarisgroupcreate.xml'.
Added ResourceForm:Solaris Create Group Form
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Including file 'sample/forms/Solarisgroupupdate.xml'.
Added ResourceForm:Solaris Update Group Form
Including file 'sample/forms/SUSELinuxgroupcreate.xml'.
Added ResourceForm:SUSE Linux Create Group Form
Including file 'sample/forms/SUSELinuxgroupupdate.xml'.
Added ResourceForm:SUSE Linux Update Group Form
Including file 'sample/forms/SunJSCSActiveSyncForm.xml'.
Added UserForm:Sun Java System Communications Services ActiveSync Form
Including file 'sample/forms/SunJSCSGroupCreate.xml'.
Added ResourceForm:Sun Java System Communications Services Create Group Form
Including file 'sample/forms/SunJSCSGroupUpdate.xml'.
Added ResourceForm:Sun Java System Communications Services Update Group Form
Including file 'sample/forms/SunJSCSOrganizationalUnitCreate.xml'.
Added ResourceForm:Sun Java System Communications Services Create
    Organizational Unit Form
Including file 'sample/forms/SunJSCSOrganizationalUnitUpdate.xml'.
Added ResourceForm:Sun Java System Communications Services Update
    Organizational Unit Form
Including file 'sample/forms/SunJSCSOrganizationCreate.xml'.
Added ResourceForm:Sun Java System Communications Services Create Organization Form
Including file 'sample/forms/SunJSCSOrganizationUpdate.xml'.
Updated ResourceForm:Sun Java System Communications Services Update Group Form
Including file 'sample/resourceAccountChangePassword.xml'.
Added ResourceForm:Change Resource Account Password Form
Including file 'sample/resourceAccountResetPassword.xml'.
Added ResourceForm:Reset Resource Account Password Form
Including file 'sample/resourcePolicyModify.xml'.
Added ResourceForm>Edit Resource Policy Form
Including file 'sample/resourceGroupDelete.xml'.
Added UserForm:Delete Group Form
Including file 'sample/resourceObjectFind.xml'.
Added ResourceForm:Find Resource Object Form
Including file 'sample/resourceObjectFindResults.xml'.
Added ResourceForm:Find Resource Object Results Form
Including file 'sample/resourceObjectRename.xml'.
Added ResourceForm:Rename Resource Object Form
Including file 'sample/resourceWizardForms.xml'.
Restored UserForm:Resource Wizard Library
Restored UserForm:Resource Wizard
Restored UserForm:Resource Rename Form
Restored UserForm:Database Resource Wizard Library
Restored UserForm:Resource Wizard Database Table
Restored UserForm:Resource Wizard ScriptedJDBC
Restored UserForm:Resource Wizard Microsoft Identity Integration Server
Restored UserForm:Resource Wizard PeopleSoft Component Interface
Restored UserForm:Resource Wizard JMS Listener
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored UserForm:Resource Wizard Sun Access Manager
Restored UserForm:Resource Wizard FlatFileActiveSync
Including file 'sample/resourceActiveSyncWizardLibrary.xml'.
Restored UserForm:Resource Active Sync Wizard Library
Including file 'sample/resourceActiveSyncWizardForms.xml'.
Including file 'sample/resourceActiveSyncWizardLibrary.xml'.
Updated UserForm:Resource Active Sync Wizard Library
Including file 'sample/conditionDialog.xml'.
Restored UserForm:Condition Dialog
Restored UserForm:Resource Active Sync Wizard
Including file 'sample/resourceList.xml'.
Restored UserForm:Resource List Library
Restored UserForm:Resource List Form
Including file 'sample/resourceTableTasks.xml'.
Added UserForm:Resource Create Form
Added UserForm:Resource Delete Form
Added UserForm:Default Resource Rename Form
Added UserForm:Resource Saveas Form
Added UserForm:Resource Object Create Form
Added UserForm:Resource Object Rename Form
Added UserForm:Resource Object Saveas Form
Added UserForm:Resource Object Delete Form
Including file 'sample/raforms.xml'.
Restored RiskReportTask:Windows NT Risk Analysis
Restored RiskReportTask:Windows Active Directory Risk Analysis
Restored RiskReportTask:NetWare NDS Risk Analysis
Restored RiskReportTask:AIX Risk Analysis
Restored RiskReportTask:Solaris Risk Analysis
Restored RiskReportTask:hPUX Risk Analysis
Restored RiskReportTask:Red Hat Linux Risk Analysis
Added RiskReportTask:Windows Active Directory Inactive Account Scan
Added RiskReportTask:Windows NT Inactive Account Scan
Added RiskReportTask:OS/400 Inactive Account Scan
Added RiskReportTask:ACF2 Inactive Account Scan
Including file 'sample/reconconfig.xml'.
Restored TaskDefinition:Reconcile
Restored TaskDefinition:Reconcile Requestor
Preserving object EmailTemplate #ID#EmailTemplate:ReconcileResourceEvent
Preserving object EmailTemplate #ID#EmailTemplate:ReconcileAccountEvent
Preserving object EmailTemplate #ID#EmailTemplate:ReconcileSummary
Restored EmailTemplate:Reconcile Resource Event
Restored EmailTemplate:Reconcile Account Event
Restored EmailTemplate:Reconcile Summary
Added Configuration:ReconConfigProxy
Including file 'sample/reconRules.xml'.
Added Rule:USER_NAME_MATCHES_ACCOUNT_ID
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Added Rule:USER_OWNS_MATCHING_ACCOUNT_ID
Added Rule:USER_EMAIL_MATCHES_ACCOUNT_EMAIL_CORR
Added Rule:USER_EMAIL_MATCHES_ACCOUNT_EMAIL_CONF
Added Rule:USER_FIRST_AND_LAST_NAMES_MATCH_ACCOUNT
Added Rule:SCHEDULING_RULE_ACCEPT_ALL_DATES
Including file 'sample/components.xml'.
Added Configuration:Component Properties
Including file 'sample/messages.xml'.
Added Configuration:defaultTestCustomCatalog
Including file 'sample/bulkoptask.xml'.
Preserving object TaskDefinition #ID#TaskDefinition:BulkOpTask
Restored TaskDefinition:Bulk Actions Task
Including file 'sample/dictionaryconfig.xml'.
Added Rule:TestDictionary
Added Rule:InsertDictionaryWord
Added Rule:CheckDictionaryWord
Preserving object Configuration #ID#Configuration:DictionaryConfig
Restored Configuration:Dictionary Configuration
Restored TaskDefinition:DictionaryLoader
Restored Configuration:DictionaryConfigForm
Including file 'sample/attrparse.xml'.
Added AttrParse:Default ACF2 AttrParse
Added AttrParse:Default VMS AttrParse
Added AttrParse:Default TopSecret ListUser CICS AttrParse
Added AttrParse:Default TopSecret ListUser TSO AttrParse
Added AttrParse:Default TopSecret TSO Segment AttrParse
Added AttrParse:Default TopSecret OMVS Segment AttrParse
Added AttrParse:Default CICS Segment AttrParse
Added AttrParse:Default TopSecret ListAllObjects AttrParse
Added AttrParse:Default RACF ListUser AttrParse
Added AttrParse:Default LDAP RACF ListUser AttrParse
Added AttrParse:Default RACF TSO Segment AttrParse
Added AttrParse:Default RACF OMVS Segment AttrParse
Added AttrParse:Default RACF CICS Segment AttrParse
Added AttrParse:Default RACF NETVIEW AttrParse
Added AttrParse:Default Natural ListUser AttrParse
Added AttrParse:Default Natural ListUser Groups AttrParse
Added AttrParse:Default Natural ListAllObjects AttrParse
Including file 'sample/serverForms.xml'.
Not saving object Configuration #ID#Form>EmailTemplateSettingsForm: not found
Not saving object Configuration #ID#Form>ReconcilerSettingsForm: not found
Not saving object Configuration #ID#Form>SchedulerSettingsForm: not found
Not saving object Configuration #ID#Form>ServerSettingsForm: not found
Not saving object Configuration #ID#Form>JMXSettingsForm: not found
Restored Configuration:Reconciler Settings Form
Restored Configuration:Scheduler Settings Form
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored Configuration:Email Template Settings Form
Restored Configuration:JMX Settings Form
Restored Configuration:Server Settings Form
Including file 'sample/scripttasks.xml'.
Added TaskDefinition:Script Interpreter
Including file 'sample/workItemTypes.xml'.
Restored Configuration:WorkItemTypes
Including file 'sample/rules/AlphaNumeric.xml'.
Added Configuration:Alpha Numeric Rules
Including file 'sample/rules/DateLibrary.xml'.
Added Configuration:Date Library
Including file 'sample/rules/NamingRules.xml'.
Added Rule:Fullname - Last comma First
Added Rule:Fullname - First space Last
Added Rule:Fullname - First space MI space Last
Added Rule:AccountName - First dot Last
Added Rule:AccountName - First initial Last
Added Rule:AccountName - First underscore Last
Added Rule:Email
Including file 'sample/rules/RegionalConstants.xml'.
Updated Configuration:Regional Constants
Including file 'sample/rules/LoginCorrelationRules.xml'.
Added Rule:Correlate via X509 Certificate SubjectDN
Added Rule:Correlate via LDAP Uid
Including file 'sample/rules/NewUserNameRules.xml'.
Added Rule:Use SubjectDN Common Name
Including file 'sample/rules/ActiveSyncRules.xml'.
Added Rule:ActiveSync has isDeleted set
Including file 'sample/PeopleSoftComponentInterfaces.xml'.
Restored Configuration:PeopleSoft Component Interfaces
Including file 'sample/wfpwsync.xml'.
Preserving object EmailTemplate #ID#EmailTemplate:PasswordSyncNotice
Preserving object EmailTemplate #ID#EmailTemplate:PasswordSyncFailureNotice
Added TaskDefinition:Synchronize User Password
Restored EmailTemplate:PasswordSyncFailureNotification
Restored EmailTemplate:PasswordSyncNotification
Including file 'sample/adsyncfailover.xml'.
Added TaskDefinition:Active Directory Synchronization Recovery Collector
Added TaskDefinition:Active Directory Synchronization Failover
Including file 'sample/reportConfig.xml'.
Restored Configuration:Reports Configuration
Restored Configuration:Tracked Events Configuration
Added UserForm:Reports Config Library
Added UserForm:Tracked Events Config Library
Restored UserForm:Reports Configuration Form
Including file 'sample/auditor.xml'.
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Including file 'sample/auditorrules.xml'.
Added Rule:Review Everyone
Added Rule:Review Changed Users
Added Rule:Reject Changed Users
Added Rule:Default Remediator
Added Rule:Default Attestor
Added Rule:Default Escalation Attestor
Added Rule:All Non-Administrators
Added Rule:All Administrators
Added Rule:Users Without a Manager
Added Rule:Compare Accounts to Roles
Added Rule:Compare Roles to actual Resource values
Added AuditPolicy:IdM Role Comparison
Added AuditPolicy:IdM Account Accumulation
Including file 'sample/auditorforms.xml'.
Preserving object Rule #ID#Rule:ViolationPriority
Preserving object Rule #ID#Rule:ViolationSeverity
Updated UserForm:AuditPolicyLibrary
Updated UserForm:AuditorFormLibrary
Updated UserForm:Audit Policy List
Updated UserForm:Audit Policy Delete Confirmation Form
Updated UserForm:Audit Policy Form
Updated UserForm:Update Audit Policy Form
Updated UserForm:Remediation Library
Updated UserForm:Bulk Remediation
Updated UserForm:Sign Bulk Remediation
Ignoring changes to preserved object 'Rule:ViolationPriority'
Ignoring changes to preserved object 'Rule:ViolationSeverity'
Updated UserForm:Remediation List
Updated Configuration:AuditorOrgForm
Updated UserForm:Violation Detail Form
Updated UserForm:Compliance Violation Summary Form
Updated UserForm:Conflict Violation Details Form
Updated UserForm:Auditor Tab
Updated UserForm:Remediation Form
Including file 'sample/accessreviewforms.xml'.
Restored UserForm:Access Review Library
Restored UserForm:Bulk Attestation
Restored UserForm:Sign Bulk Attestation
Restored UserForm:Access Approval List
Restored UserForm:Access Review Dashboard
Restored UserForm:Access Review Delete Confirmation Form
Restored UserForm:Access Review Abort Confirmation Form
Restored UserForm:Attestation Form
Restored UserForm:Access Review Summary
Restored UserForm:Access Review Detail
```

EXAMPLE 1-1 Sample Output from lh Log Program (Continued)

```
Restored UserForm:Access Scan Form
Added UserForm:Access Scan List
Added UserForm:Access Scan Delete Confirmation Form
Restored UserForm:UserEntitlementForm
Restored UserForm:UserEntitlement Summary Form
Restored UserForm:Access Review Remediation Form
Restored UserForm:Access Scan Rename Form
Including file 'sample/auditortasks.xml'.
Restored TaskDefinition:Detailed User Report
Restored TaskDefinition:Audited Attribute Report
Restored TaskDefinition:Violation Summary Report
Restored TaskDefinition:Audit Policy Summary Report
Restored TaskDefinition:Audit Policy Scan
Restored TaskDefinition:Audit Policy Rescan
Added TaskDefinition:Applet Audit Policy Scan
Added UserForm:Policy Violation Report Library
Restored TaskDefinition:Organization Violation History
Restored TaskDefinition:Resource Violation History
Restored TaskDefinition:AuditPolicy Violation History
Restored TaskDefinition:Default Compliance Audit Report
Restored TaskDefinition:Audit Policy System Scan
Restored TaskDefinition:Separation of Duties
Restored TaskDefinition:Access Scan
Restored TaskDefinition:Access Review Rescan
Restored TaskDefinition:Access Review Detail Report
Restored TaskDefinition:Access Scan User Scope Report
Restored TaskDefinition:Access Review Coverage Report
Restored TaskDefinition:Access Review Summary Report
Restored TaskDefinition:Abort Access Review
Restored TaskDefinition:Recover Access Review
Restored TaskDefinition:Delete Access Review
Including file 'sample/auditorwfs.xml'.
Preserving object EmailTemplate #ID#EmailTemplate:PolicyViolationNotice
Preserving object EmailTemplate #ID#EmailTemplate:AttestationNotice
Preserving object EmailTemplate #ID#EmailTemplate:BulkAttestationNotice
Preserving object EmailTemplate #ID#EmailTemplate:AccessScanBeginNotice
Preserving object EmailTemplate #ID#EmailTemplate:AccessScanEndNotice
Added Configuration:Remediation
Added Configuration:Access Review Remediation
Added Configuration:Attestation
Added Rule:Remediation Transaction Message
Added Rule:Remediation Transaction Message Helper
Added Rule:Attestation Transaction Message
Added Rule:Attestation Transaction Message Helper
Added Rule:Attestation Remediation Transaction Message
Added Rule:Attestation Remediation Transaction Message Helper
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored EmailTemplate:Policy Violation Notice
Added Configuration:Multi Remediation
Added TaskDefinition:Standard Remediation
Restored TaskDefinition:Remediation Report
Added Configuration:Update Compliance Violation
Restored EmailTemplate:Attestation Notice
Restored EmailTemplate:Access Review Remediation Notice
Restored EmailTemplate:Bulk Attestation Notice
Restored EmailTemplate:Access Scan Begin Notice
Restored EmailTemplate:Access Scan End Notice
Added TaskDefinition:Standard Attestation
Added TaskDefinition:Access Review
Added Configuration:Launch Access Scan
Added Configuration:Launch Entitlement Rescan
Added Configuration:Launch Violation Rescan
Added TaskDefinition:ScanNotification
Including file 'sample/auditorDefaultReports.xml'.
Preserving object TaskTemplate #ID#TaskTemplate:DefOrgViolationHistory
Preserving object TaskTemplate #ID#TaskTemplate:DefAuditPolicyViolationHistory
Preserving object TaskTemplate #ID#TaskTemplate:DefResourceViolationHistory
Preserving object TaskTemplate #ID#TaskTemplate:AllComplianceViolations
Preserving object TaskTemplate #ID##TaskTemplate:AllAuditPolicies
Preserving object TaskTemplate #ID#AllSeparationofDutiesViolations
Preserving object TaskTemplate #ID#AllAccessReviewSummary
Restored TaskTemplate:Default Organization Violation History
Restored TaskTemplate:Default AuditPolicy Violation History
Restored TaskTemplate:Default Resource Violation History
Restored TaskTemplate:All Compliance Violations
Restored TaskTemplate:All Audit Policies
Restored TaskTemplate:All Separation of Duties Violations
Restored TaskTemplate:All Access Review Summary
Including file 'sample/speInit.xml'.
Preserving object Configuration #ID#IDMXConfiguration
Preserving object Configuration #ID#IDMXTrackedEventsConfig
Preserving object Configuration #ID#IDMXTransactionManagerConfig
Preserving object Resource #ID#Resource:SPEEndUserDirectory
Preserving object Policy #ID#Policy:SPE
Restored Configuration:SPE
Restored UserForm:SPE Browse
Restored UserForm:SPE User Form
Restored UserForm:SPE Example End User Form
Restored Configuration:SPE SPML
Restored TaskDefinition:SPE Migration
Including file 'sample/speRules.xml'.
Restored Rule:SPE Example Is Account Locked Rule
Restored Rule:SPE Example Lock Account Rule
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Restored Rule:SPE Example Unlock Account Rule
Restored Rule:SPE Example Correlation Rule Returning Single Identity
Restored Rule:SPE Example Correlation Rule Returning List of Identities
Restored Rule:SPE Example Correlation Rule for LDAP Returning Option Map
Restored Rule:SPE Example Correlation Rule for Simulated Returning Option Map
Restored Rule:SPE Example Confirmation Rule Returning First Candidate
Restored Rule:SPE Example Confirmation Rule Rejecting All Candidates
Restored Rule:SPE Example Confirmation Rule Selecting Candidates Using AccountId
Including file 'sample/speConfigForm.xml'.
Restored UserForm:SPE Configuration
Including file 'sample/speSearchForms.xml'.
Restored UserForm:SPE Search Confirmation
Restored UserForm:SPE Bulk User Results
Restored UserForm:SPE Search
Restored UserForm:SPE Search Config
Restored UserForm:SPE User Delete
Including file 'sample/speTrackedEventConfig.xml'.
Restored Configuration:SPE Tracked Events Configuration
Including file 'sample/speTransactionManagerConfig.xml'.
Restored Configuration:SPE Transaction Manager Configuration
Including file 'sample/dashboardGraphConfig.xml'.
Restored UserForm:Dashboard Graph Configuration
Including file 'sample/dashboardConfig.xml'.
Restored UserForm:Dashboard Configuration
Including file 'sample/speDashboardExamples.xml'.
Added Configuration:Today's Completed Transactions by Type
Added Configuration:Recent Directory Search Duration
Added Configuration:Recent Per Server Total Locked Transactions
Added Configuration:Today's Concurrent Administrators (Sample Data)
Added Configuration:Today's Resource Operations (Sample Data)
Added Configuration:Recent Directory Searches
Added Configuration:Recent Transaction Searches
Added Configuration:Today's Concurrent Users (Sample Data)
Added Configuration:Recent Resource Operation Failures (Sample Data)
Added Configuration:Recent Administrator Operations by Type
Added Configuration:Recent Resource Operations (Sample Data)
Added Configuration:Recent Per Server Pending Retry Transactions
Added Configuration:Today's Active Sync Poll Durations
Added Configuration:Recent Concurrent Users (Sample Data)
Added Configuration:Recent Per Server Runnable Transactions
Added Configuration:Today's Resource Operations by Resource
Added Configuration:Recent Max Memory Usage by Server
Added Configuration:Today's Active Sync Errors by Resource and Type
Added Configuration:Recent Transaction Search Duration
Added Configuration:Today's Transaction Failures by Type
Added Configuration:Monthly Self-Service Operations (Sample Data)
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Added Configuration:Today's Active Sync Operations by Resource
Added Configuration:Recent Completed Transactions by Server
Added Configuration:Today's Resource Operations by Resource and Result
Added Configuration:Recent Provisioning Operation Duration (Sample Data)
Added Configuration:Monthly Resource Operations (Sample Data)
Added Configuration:Recent Thread Count by Server
Added Configuration:Today's In Process Transactions
Added Configuration:Today's Resource Operations by Type (Sample Data)
Added Configuration:Today's Registration Requests (Sample Data)
Added Configuration:Recent Concurrent Administrators (Sample Data)
Added Configuration:Today's Active Sync Activity
Added Configuration:Recent Administrator Activity
Added Configuration:Today's Provisioning Activity
Added Configuration:Recent Server Activity
Added Configuration:Resource Operations (Sample Data)
Added Configuration:Today's Activity (Sample Data)
Added Configuration:Recent Activity (Sample Data)
Including file 'sample/speAdminGroups.xml'.
Restored AdminGroup:Service Provider View User
Restored AdminGroup:Service Provider Update User
Restored AdminGroup:Service Provider Create User
Restored AdminGroup:Service Provider Delete User
Restored AdminGroup:Service Provider User Administrator
Restored AdminGroup:Service Provider Administrator
Restored AdminGroup:Service Provider Admin Role Administrator
Including file 'sample/speTransactionSearch.xml'.
Restored UserForm:SPE Transaction Search
Including file 'sample/speTransactionConfigForm.xml'.
Restored UserForm:SPE Transaction Configuration Form
Including file 'sample/speEndUserForms.xml'.
Restored Configuration:SPEUserPages
Restored UserForm:SPE End-User Login
Restored UserForm:SPE End-User Question Login Form
Restored UserForm:SPE End-User Forms Library
Restored UserForm:SPE End-User Forgot Username
Restored UserForm:SPE End-User Forgot Password
Restored UserForm:SPE End-User Change UserId
Restored UserForm:SPE End-User Change Notifications
Restored UserForm:SPE End-User Change Password
Restored UserForm:SPE End-User Reset Password
Restored UserForm:SPE End-User Change Challenge Answers
Restored UserForm:SPE Enrollment Main Form
Restored UserForm:SPE Enrollment Validation Form
Restored UserForm:SPE Enrollment Form
Restored Configuration:SPE End-User Pages Library
Restored Configuration:SPE Sample Users
```

EXAMPLE 1-1 Sample Output from lh Log Program *(Continued)*

```
Including file 'sample/speEmailTemplates.xml'.
Restored EmailTemplate:SPE End-User Username Recovery
Restored EmailTemplate:SPE End-User Profile Locked
Restored EmailTemplate:SPE End-User Reset Password
Restored EmailTemplate:SPE End-User Update Authentication Answers
Restored EmailTemplate:SPE End-User Change Notifications
Restored EmailTemplate:SPE End-User Change Notifications Old Address
Restored EmailTemplate:SPE End-User Change Password
Restored EmailTemplate:SPE End-User Change User Id
Restored EmailTemplate:SPE End-User Registration Template
Restored EmailTemplate:SPE Update Template
Restored EmailTemplate:SPE Cancellation Template
Including file 'sample/speEndUserResource.xml'.
Restored Resource:SPE End-User Directory
Including file 'sample/spePolicy.xml'.
Restored Policy:SPE Policy
Including file 'sample/speLoginConfig.xml'.
Restored LoginModGroup:Default SPE Id/Pwd Login Module Group
Restored LoginApp:SPE User Interface
Including file 'sample/speLinkingPolicyForm.xml'.
Restored UserForm:SPE Linking Policy Form

Successfully imported file '/opt/SUNWappserver91/domains/domain1/applications/
j2ee-modules/idm/sample/init.xml'.

* * * * *

Configure demo forms, tasks, and policies
Create demo users
Configure email preferences

Successfully configured Sun Java[tm] System Identity Manager. You can now start
your application server and login to Identity Manager.
More information:
Log File: /opt/SUNWappserver91/domains/domain1/applications/j2ee-modules/idm/
patches/logs/SaveConfigurationLog5229log
```


Integrating CA SiteMinder

Computer Associates (CA) SiteMinder, formerly Netegrity SiteMinder, is an enterprise infrastructure product that enables centralized, secure Web access management. Its features include user authentication and single sign-on, policy-based authorization, and identity federation. One of the first single sign-on products to arrive on the market, legacy SiteMinder installations still exist to protect enterprise applications in many company networks.

This chapter describes options for integrating CA SiteMinder with Sun Federation Access Manager. The chapter also provides instructions for Using Sun Federation Access Manager to configure end-to-end CA SiteMinder single sign-on.

The following topics are included in this chapter:

- “About CA SiteMinder” on page 87
- “Understanding the SiteMinder User Cases” on page 89
- “Installing SiteMinder” on page 99
- “Configuring SiteMinder After Installation” on page 100
- “Using Federated Access Manager to Enable SiteMinder Federation in an Identity Provider Environment” on page 109
- “Using Federated Access Manager to Enable SiteMinder Federation in a Service Provider Environment” on page 126

About CA SiteMinder

CA SiteMinder consists of two core components that are used for access control and single sign-on:

- Policy Server
- Policy Agents

The SiteMinder Policy Server provides policy management, authentication, authorization and accounting. The Policy Server core engine was developed in C/C++ and the core components run like process daemons with predefined TCP/IP ports. The policy user interface is a Java

applet-based console. A supported web server configured with a SiteMinder NSAPI plug-in provides the front-end HTTP interface. The policy user interface enables the user to create policies, domains, and realms, as well as to configure authentication schemes. The policy user interface also provides centralized agent configuration. SiteMinder also has a local Java applet-based console utility for managing system configuration such as authentication and authorization settings, port numbers, and so forth.

The SiteMinder policy agent acts as a filter for protecting enterprise applications. SiteMinder provides various policy agents to access Web applications and content according to predefined security policies:

- Web policy agents
- SAML affiliated policy agents
- Application server policy agents
- RADIUS database policy agents
- TransactionMinder XML policy agents
- Custom policy agents (Any policy agent that is written using the SiteMinder Agent API)

The SAML Affiliated agent is part of CA Federated Security Services. The Security Services provide single sign-on from a producer site, such as a portal, to a SAML consumer acting as an affiliate in a federated network. The communication between the SAML Affiliated policy agent and SiteMinder at the producer site results in the generation of a SAML Assertion. The TransactionMinder XML Agent is an XML-enabled version of the SiteMinder policy agent that authenticates and authorizes web services-bound URLs.

Authentication and Authorization

SiteMinder supports several authentication schemes as part of its authentication framework. Authentication schemes provide a way to collect credentials and determine the identity of a user. SiteMinder Credential Collector is an application within the web policy agent that gathers specific information about a user's credentials, and then sends the information to the Policy Server. For form-based authentication, credentials are acquired by the Forms Credential Collector (FCC) process. The default extension for FCC files is .fcc. FCC process files are composed in a simple mark-up language that includes HTML and some custom notation. The following describes a simple authentication scheme flow using a form-based authentication scheme:

1. A user requests a resource that is protected by a policy agent and contained in a realm. The realm is protected by an HTML form-based authentication scheme.
2. SiteMinder contacts the Policy Server and determines that the user request must be redirected to the credential collector.
3. The policy agent redirects to the URL of the Credential Collector file.
4. The Credential Collector displays the form described in the .fcc file of the user's browser.

5. The user fills out the custom form and submits it. The Credential Collector processes the credentials by submitting the form to the Policy Server.
6. If the user is authenticated, Credential Collector creates a session cookie and sends it to the browser. The browser redirects the user to the resource that the user originally requested.
7. The web policy agent handles user authorization by using the user's session.

User Sessions

SiteMinder supports persistent and non-persistent sessions. The standard SiteMinder sessions are non-persistent and contain user session data but no other user-specific data. For example, a session does not contain attributes unless configured to do so. The SiteMinder user session is created by the SiteMinder server upon successful authentication.

The servers send the user session SiteMinder policy agent to set in the browser. The policy agent is responsible for validating the cookie and enforcing session timeouts. The cookie named SMSESSION contains the following parameters by default:

- Device name or host name
- User's full DN
- User Name
- Session idle timeout
- Session maximum timeout
- Session creation time

Understanding the SiteMinder User Cases

This chapter describes three use cases, all built upon legacy SiteMinder deployments. In each use case, SiteMinder continues to provide authentication service for legacy applications even after Federated Access Manager is installed to protect the same enterprise applications. SiteMinder and Federated Access Manager typically co-exist in the following use cases:

- Simple Single Sign-On
- Federated Single Sign-On in a Service Provider Environment
- Federated Single Sign-On in an Identity Provider Environment

Single logout for any of these use cases can be implemented in many ways. The logout for federation use cases must have a link in the partner portal for the following URL:

```
http:<sphost>:<spport>/opensso/saml2/jsp/spSingleLogoutInit.jsp?metaAlias=<metaalias>&idpEntityID=<idp entityid>&RelayState=<integrated product logout url>
```

Single logout can also be achieved using Identity Provider-initiated single logout.

Simple Single Sign-On Use Case

In this use case, a SiteMinder instance is already deployed and configured to protect some of the enterprise applications in a company intranet. In the architecture figure below, the legacy application is contained in the Protected Resource . The company wants to continue leveraging SiteMinder for authentication purposes, while adding Federated Access Manager to the environment to protect the same application. Federated Access Manager is also used to protect all applications subsequently added to the enterprise.

A Federated Access Manager policy agent protects the Protected Resource, while Federated Access Manager itself is protected by a SiteMinder policy agent. In this use case, an access request goes to Federated Access Manager for policy evaluation or for single sign-on purposes. But the SiteMinder policy agent, installed on the same container as Federated Access Manager, redirects the user to the SiteMinder login page for authentication. The Federated Access Manager custom authentication module validates the SiteMinder session depending upon whether or not the user has previously logged in to Federated Access Manager. After successful login, the Federated Access Manager custom authentication module uses the SiteMinder session to generate a Federated Access Manager session. Federated Access Manager then honors the user session obtained by the SiteMinder Policy Server.

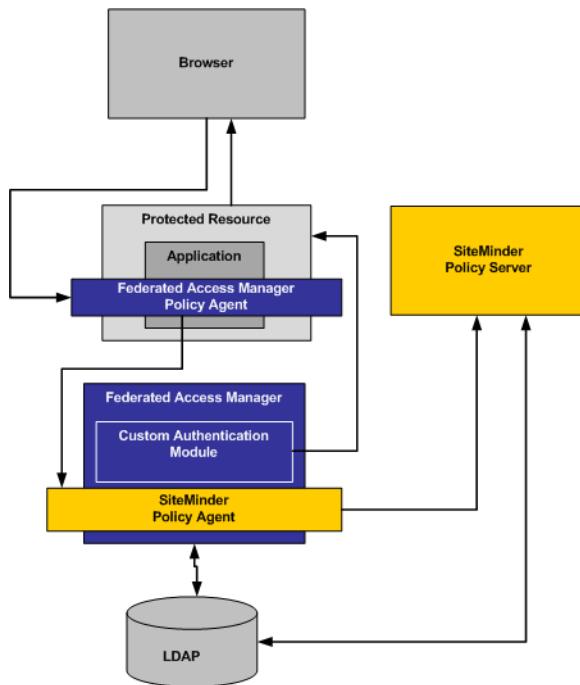


FIGURE 2–1 Single Sign-On Architecture

In this use case, both Federated Access Manager server and SiteMinder policy server share the same user repository for user profile verification. Federated Access Manager could also be configured to ignore the profile option if it relies on SiteMinder session for attributes.

The following figure illustrates the process flow for single sign-on using both SiteMinder and Federated Access Manager.

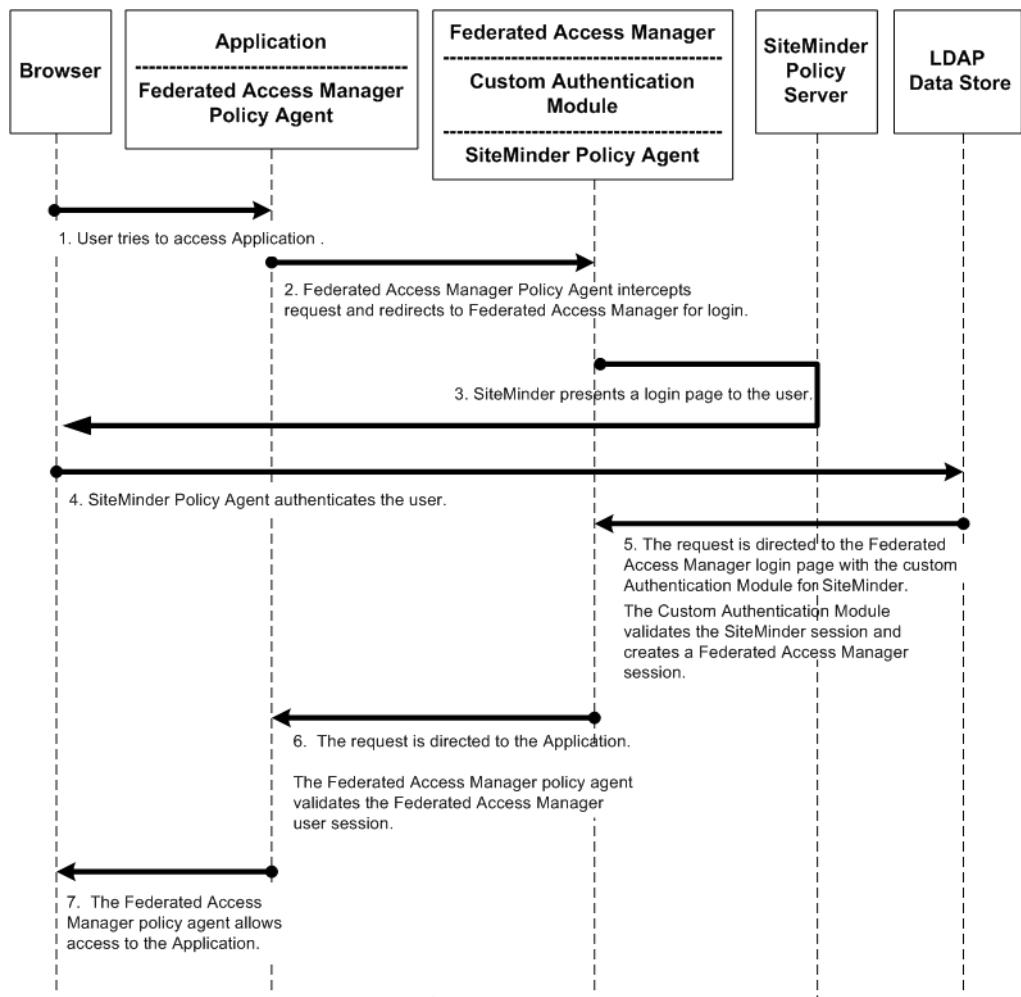


FIGURE 2-2 Single Sign-On Process Flow

Federated Single Sign-On Use Cases

The SAML, ID-FF, and WS-Federation protocols provide cross-domain single sign-on among multiple trusted business entities. These protocols are also used in Identity Federation. Identity Federation involves an Identity Provider, also known as an authentication provider, and a Service Provider where the user authentication session at the Identity provider is consumed. The following are common use cases in which SiteMinder is enabled for federation protocols:

- Enabling SiteMinder for federation protocols in a Service Provider environment
- Enabling SiteMinder for federation protocols in an Identity Provider environment

The deployment examples in this chapter are built upon simple single sign-on integration. You must set up single sign-on before enabling federation. For more information about setting up simple single sign-on, see the *Sun Federated Access Manager Installation and Configuration Guide*. After setting up simple single sign-on, you can enable SiteMinder for Federation in either the Identity Provider environment or in the Service Provider environment.

The federated single sign-on use cases are configured for transient federation. Transient federation assumes that the users exist only in the Identity Provider environment. The Service Provider honors user authentication at Identity Provider. The Service Provider then creates an anonymous session so that Service Provider applications, protected by single sign-on, can be accessed. During SAML interactions, user attribute information can be exchanged back to the Service Provider for authorization and other purposes.

Usually, bulk federation exists between Identity Provider and Service Provider. For more information about transient and bulk federation, see the Federated Access Manager product documentation.

Federated Single Sign-On in an Identity Provider Environment

In this use case, the company uses SiteMinder in the Identity Provider environment to protect applications within the company intranet. As the company partners with external companies, the company deploys Federated Access Manager in the Service Provider environment to leverage the SAMLv2 Federation protocols.

The following figure illustrates how SiteMinder can be enabled in an Identity Provider environment using Federated Access Manager for federation protocols.

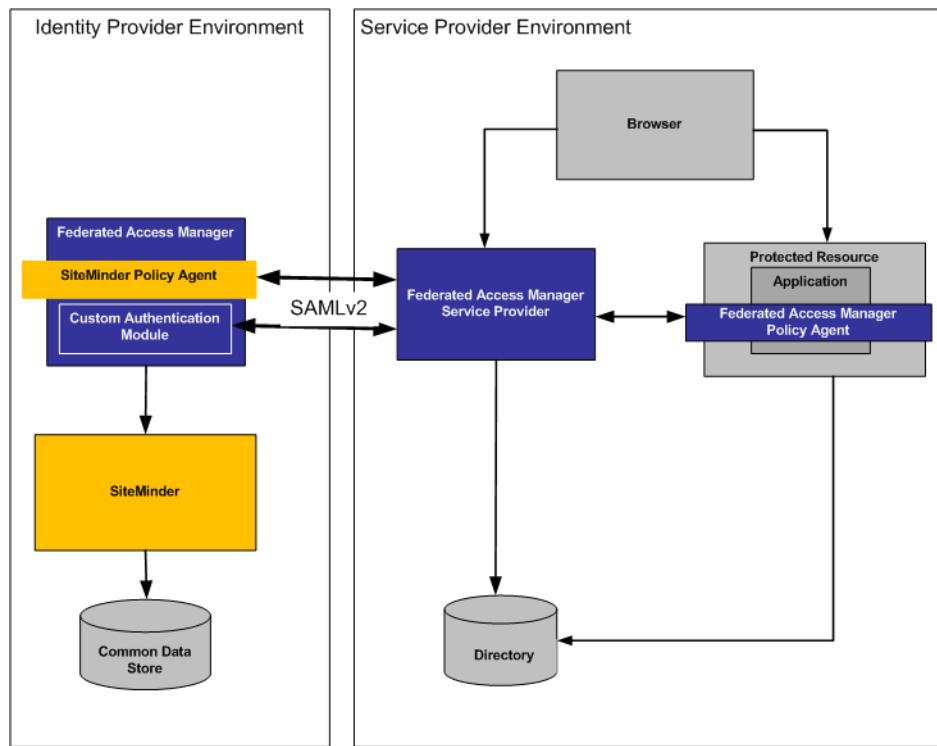


FIGURE 2–3 SiteMinder Federation in an Identity Provider Environment

In this deployment, Federated Access Manager provides federated single sign-on among enterprise applications in partner environments, while SiteMinder continues to provide authentication. The following two figures illustrates a typical transaction flow.

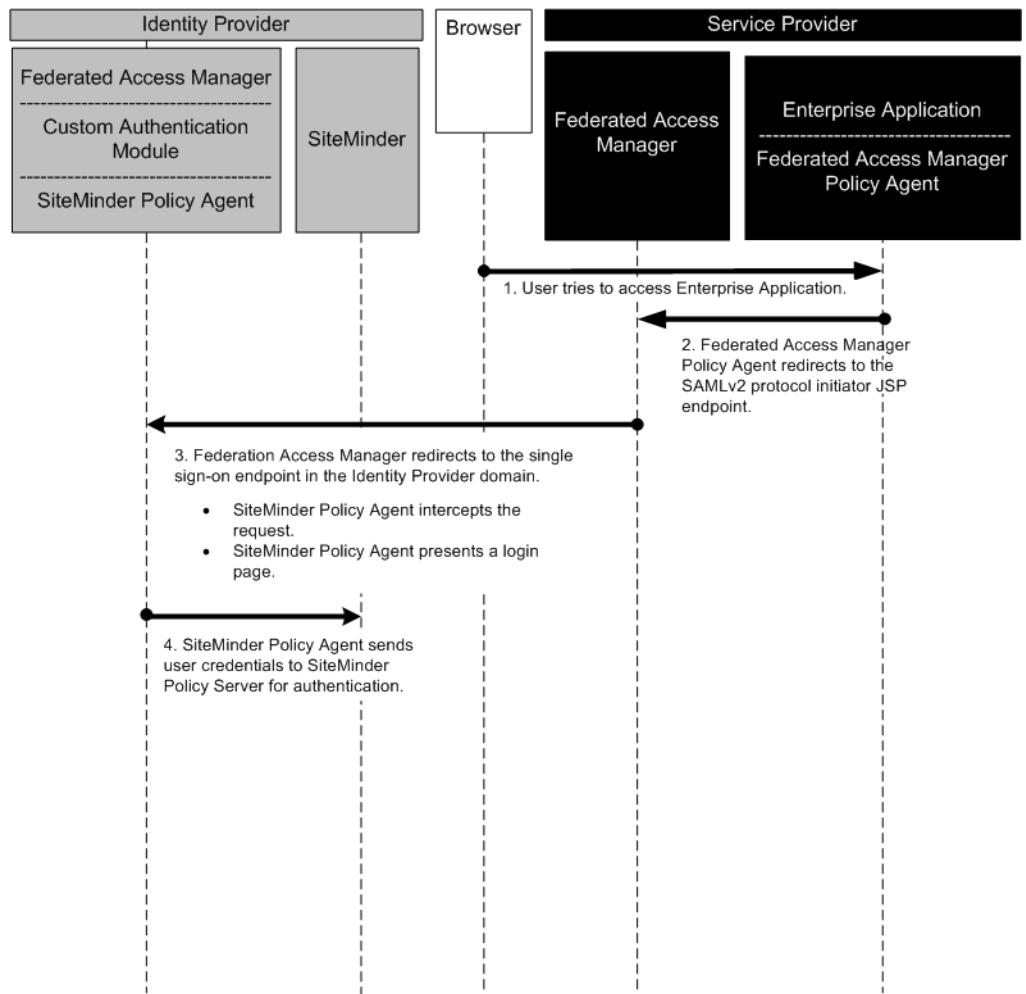


FIGURE 2–4 Process Flow for SiteMinder Federation in the Identity Provider Environment

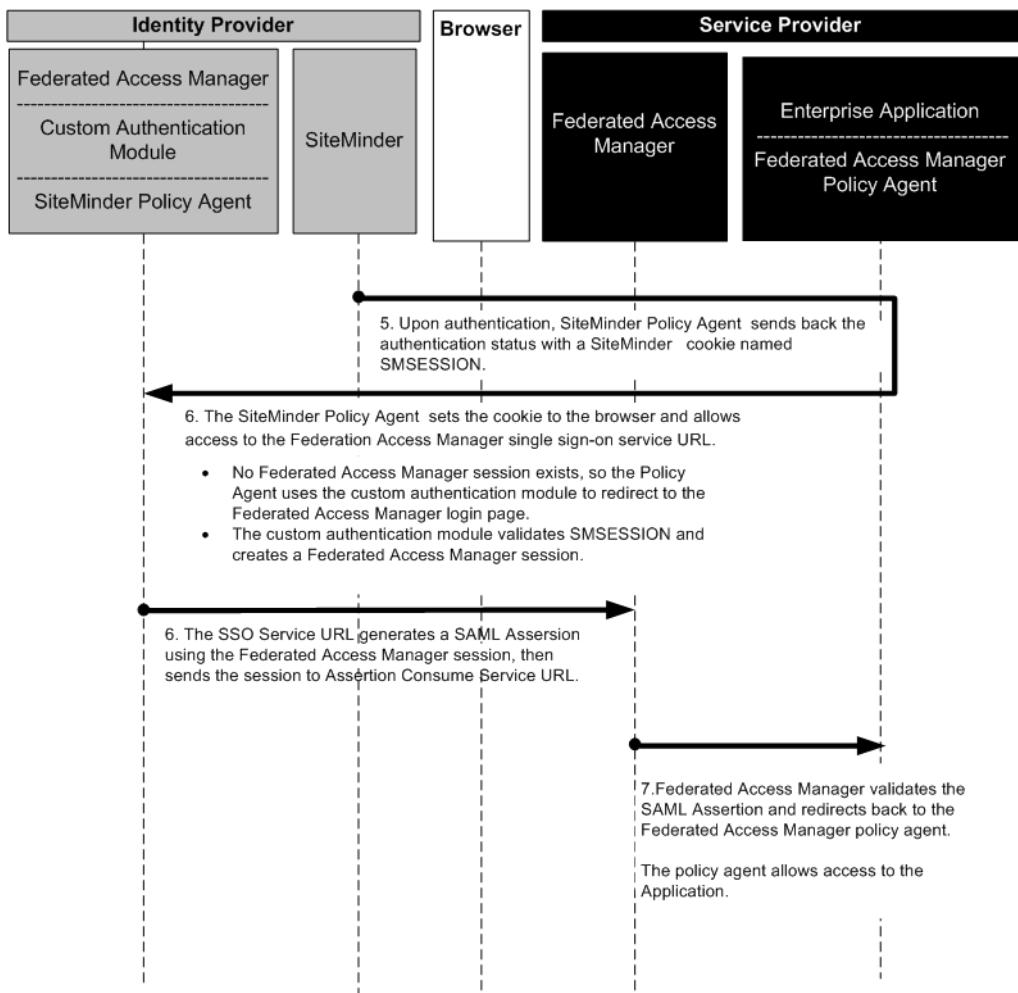


FIGURE 2-5 Process Flow for SiteMinder Federation in the Identity Provider Environment (continued)

Federated Single Sign-On Use Case in the Service Provider Environment

In this use case, the company uses SiteMinder in the Service Provider environment to protect legacy applications. Federated Access Manager is installed to invoke Federation protocols. The Federated Access Manager server includes a customized authentication module for handling SiteMinder sessions. A SiteMinder policy agent is installed on the same Federated Access Manager instance to protect Federated Access Manager.

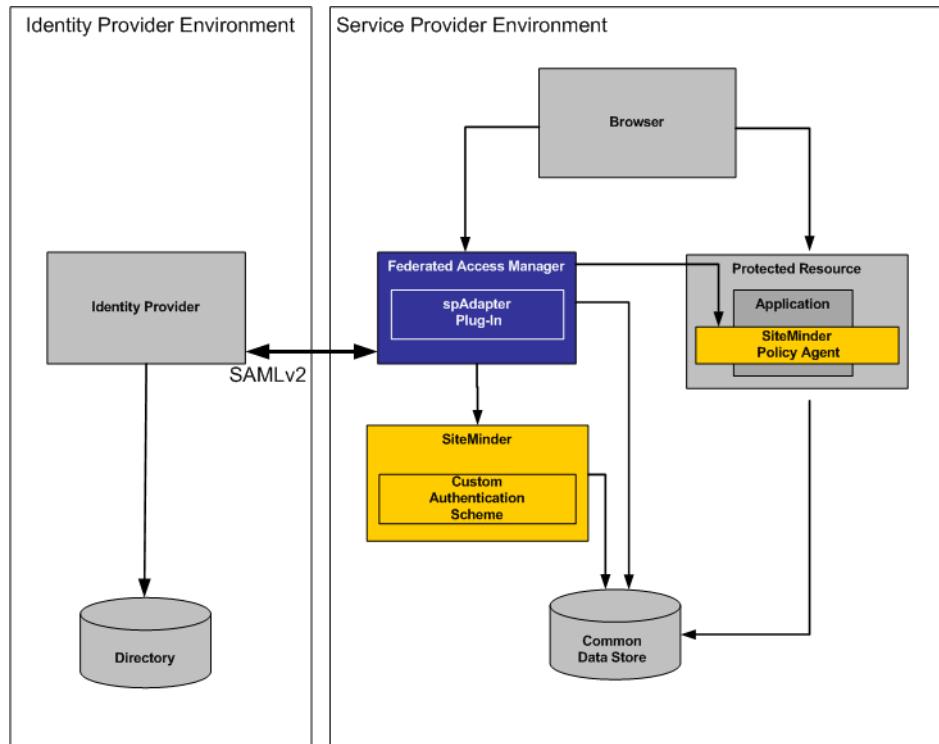


FIGURE 2–6 SiteMinder Federation in a Service Provider Environment

This use case includes two additional, lightweight components:

Custom Authentication Module (**spAdapter**)

This is a Federated Access Manager SAMLv2 plug-in that processes operations after federated single sign-on login is completed and before the target URL is displayed. After the Federated Access Manager session is established, the **spAdapter** plug-in uses the Federated Access Manager session to communicate with the SiteMinder Custom Authentication Scheme.

Custom Authentication Scheme

This is a SiteMinder SAMLv2 plug-in. It uses the Federated Access Manager configuration defined in the SAMLv2 metadata and the SAMLv2 session to generate a SiteMinder session.

When an access request comes from a partner application, the SiteMinder login page is displayed. If the user has already been authenticated, the Federated Access Manager custom authentication module creates a session for the user. The custom authentication module consumes the SiteMinder session, and then generates a SAML assertion. The following two figures illustrate the steps in the single sign-on flow:

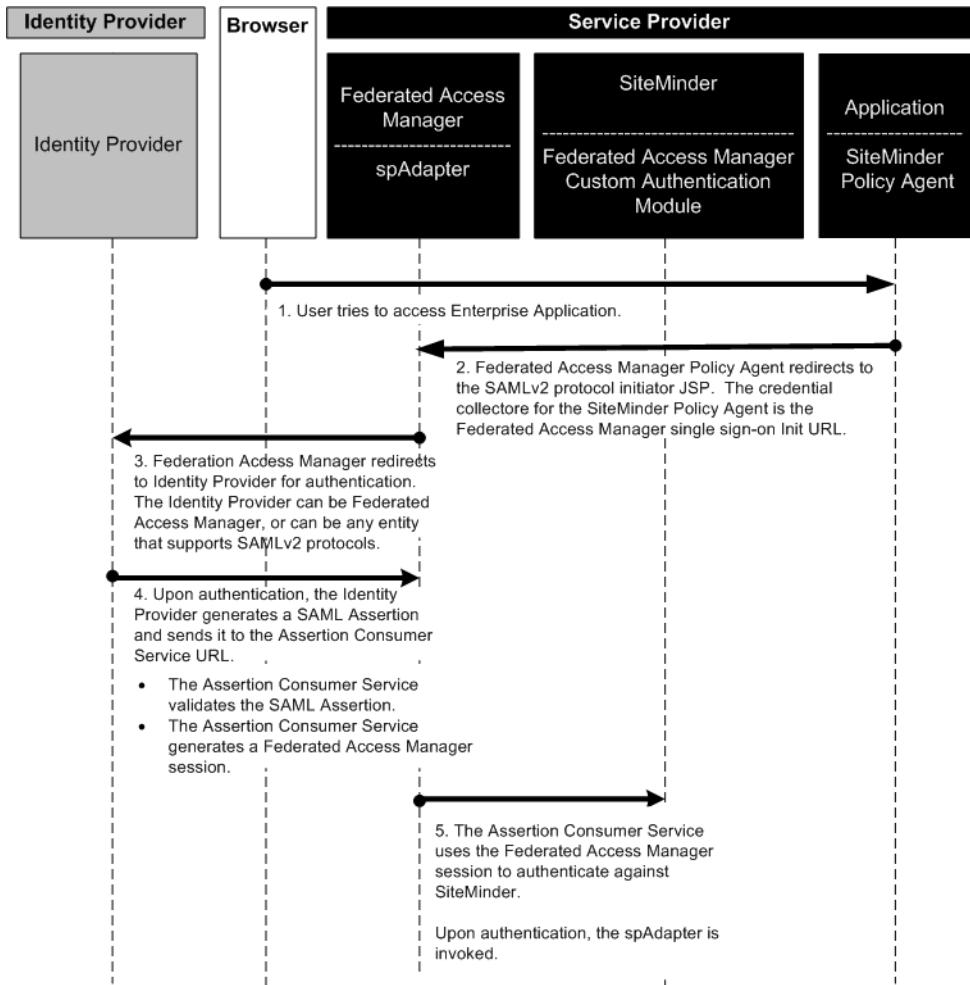


FIGURE 2-7 Process Flow for SiteMinder Federation in the Service Provider Environment

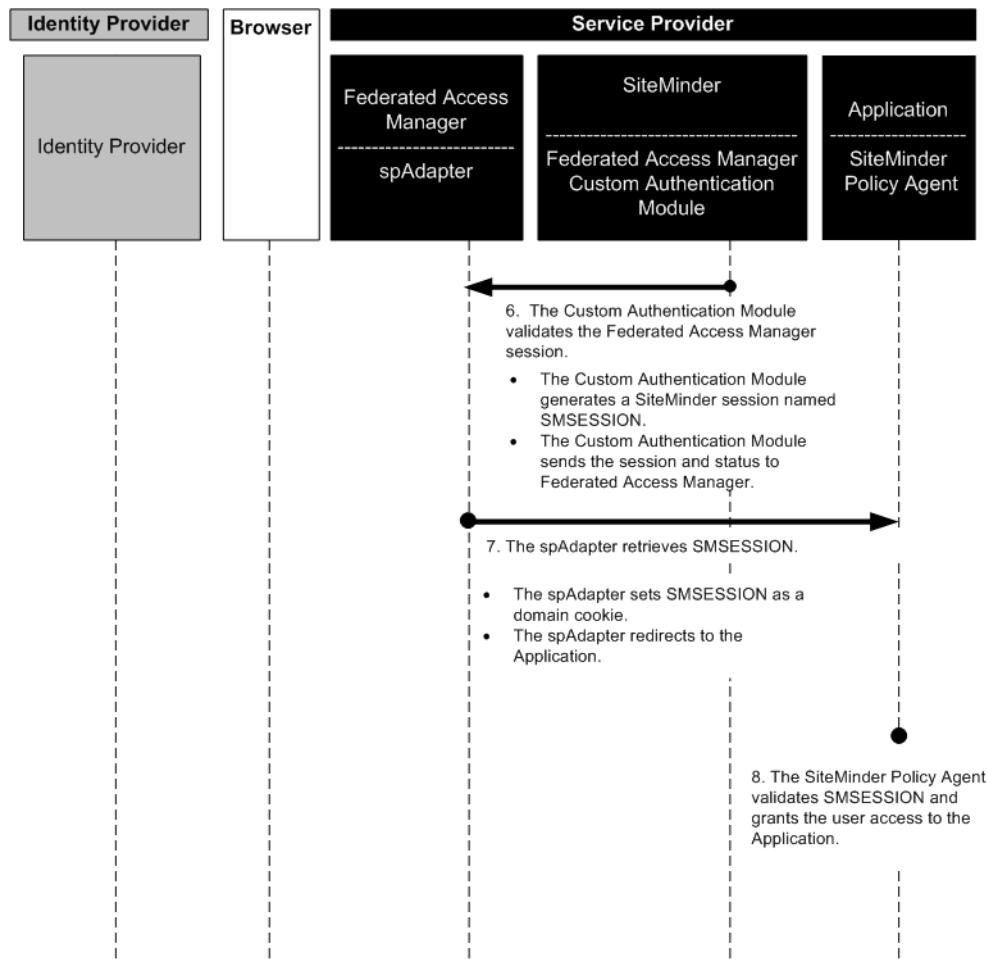


FIGURE 2-8 Process Flow for SiteMinder Federation in the Service Provider Environment (continued)

Installing SiteMinder

The use cases in this chapter describe Sun Java System Federated Access Manager 8.0 integrated with CA SiteMinder Server 6.0 Service Provider 5. Both products are installed on the Solaris operating system. Sun Web Server 6.1 SP5 is installed to serve the SiteMinder HTTP administrative interface. Sun Directory Server 6.3 is installed for its user data store and its configuration data store. Use these general instructions to install SiteMinder in any of the use cases discussed later in the chapter.

- ## 1. Install CA SiteMinder Access Manager.

You must have a licensed copy of CA SiteMinder to access its product documentation. See the product web page at <http://www.ca.com/us/products/product.aspx?id=5262>.

2. Install Sun Web Server 6.1 SP5.

See the product documentation at <http://docs.sun.com/source/819-0131/index.html>.

3. Install Directory Server 6.3.

See the product documentation at <http://docs.sun.com/source/817-7613/>.

Configuring SiteMinder After Installation

Use these general instructions after installing SiteMinder in any of the use cases discussed later in the chapter. To configure SiteMinder, follow these steps:

1. [Log inn to SiteMinder](#).
2. [Create a Sample User](#).
3. [Create a SiteMinder Policy Agent Configuration](#).
4. [Create and Configure the User Directory](#).
5. [Create and Configure a Form-Based Authentication Scheme](#).
6. [Create a Policy](#).

▼ To Log In to SiteMinder

- 1 **Go to the following URL:**

`http://hostname:portnumber/SiteMinder`

- 2 **On the SiteMinder Policy Server administration console, click "Administer Policy Server."**

- 3 **In the Policy Server login page, log in using the following credentials:**

User Name: SiteMinder

Password: password

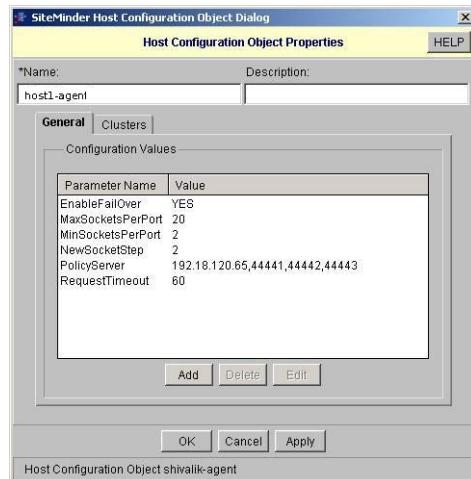
Creating a Sample User

Create a sample user in the SiteMinder Directory Server. In this use case, the new user is named test. You can base the name of this user on the attributes you use with SiteMinder. By default, Directory Server uses the uid naming attribute for the user.

▼ To Create a SiteMinder Policy Agent Configuration

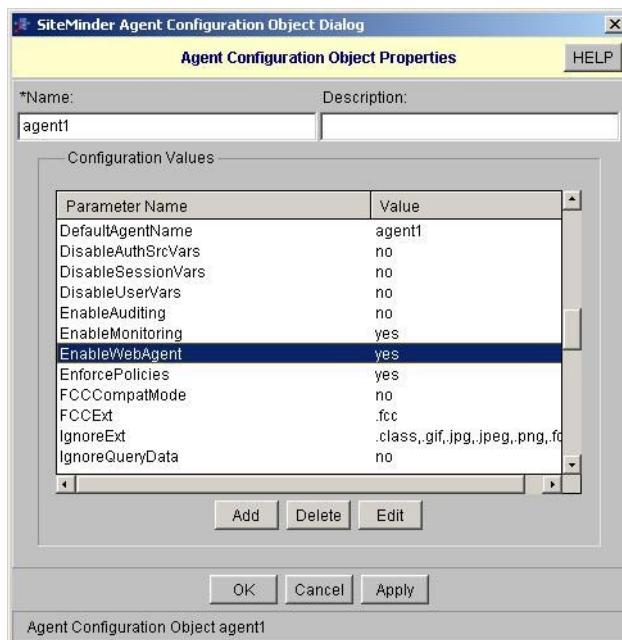
1 In SiteMinder, create a host configuration object.

In this example, the host configuration object is named `host1-agent`.



- 2 Create a web policy agent, and then create an appropriate Agent Configuration Object for the policy agent.**

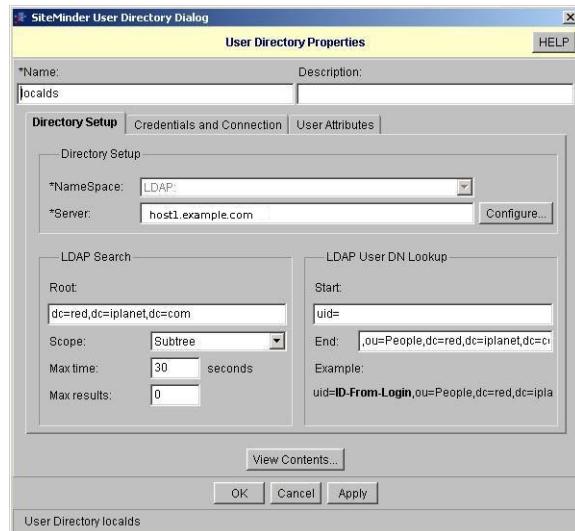
In this example, the Agent Configuration Object is named agent1.



▼ To Create and Configure the User Directory

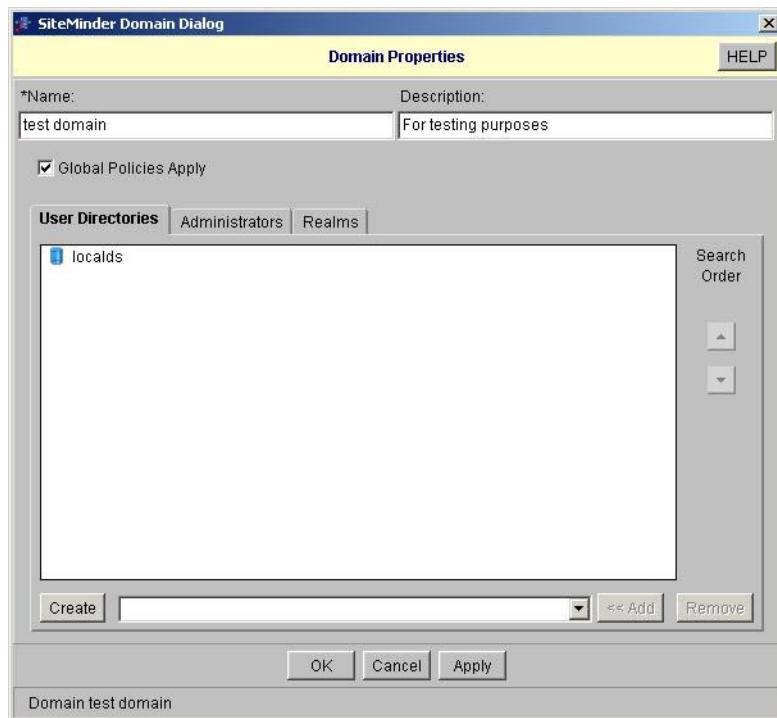
1 Create a user directory.

In this example, the user directory is named `localsd`.



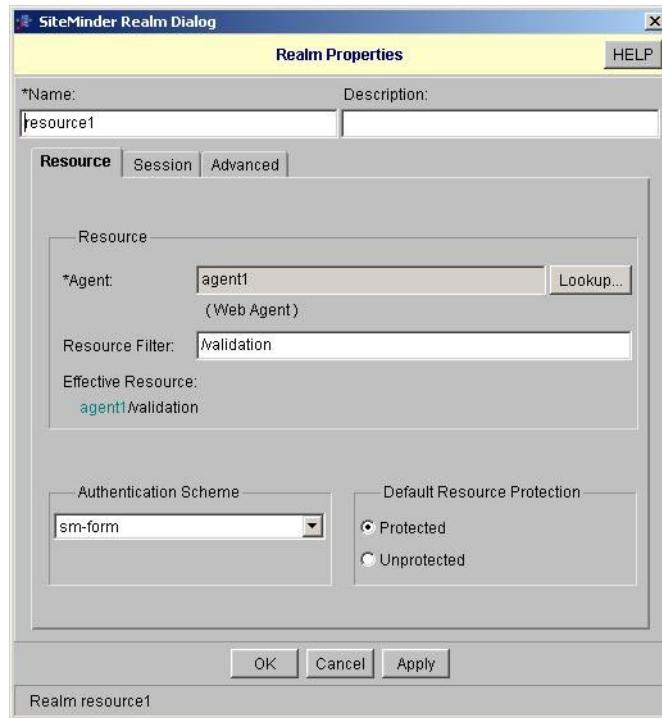
2 Create a domain.

In this example, the domain is named test domain. Under User Directories, specify localds.



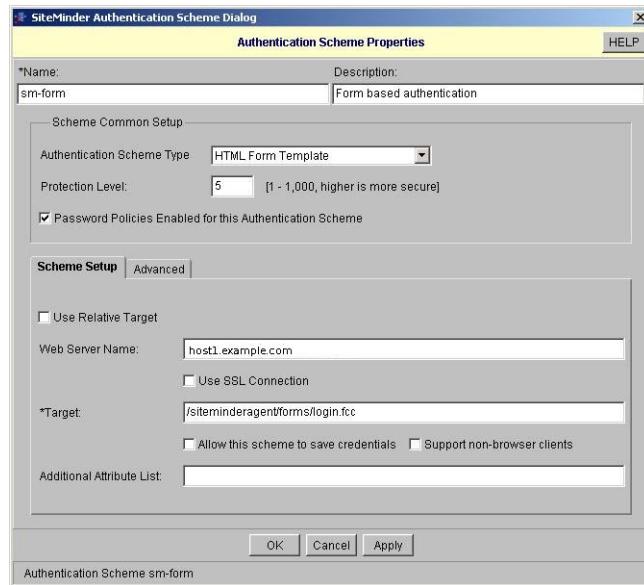
3 Create a realm.

In this example, the new realm is named resource1.



Creating and Configuring a Form-Based Authentication Scheme

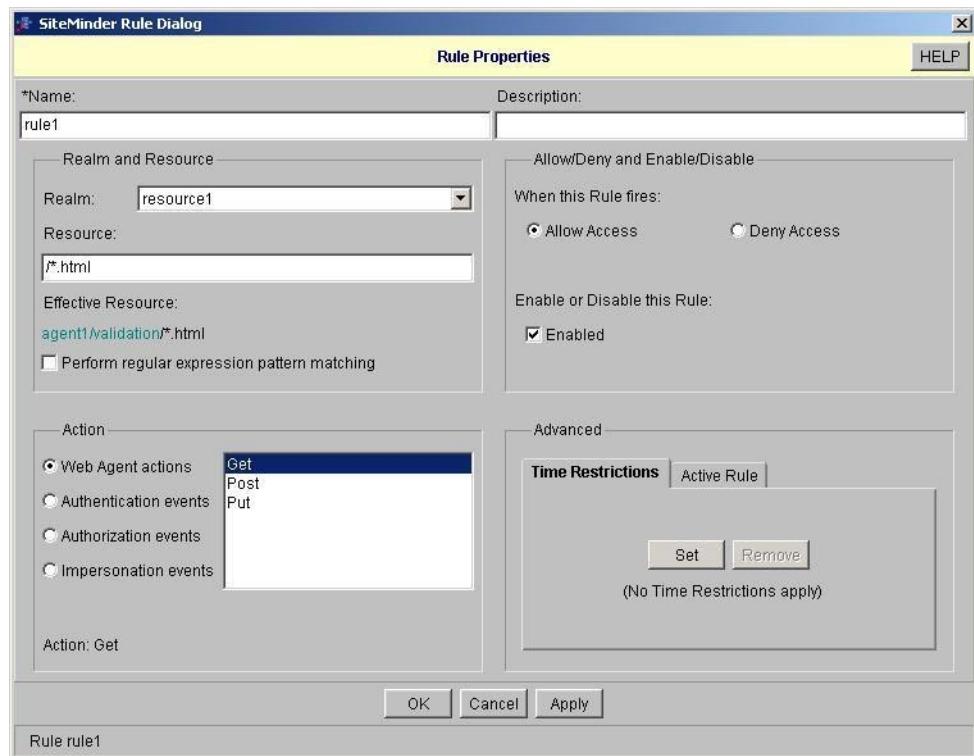
In SiteMinder, create a form authentication scheme, and then create a configuration for the authentication scheme.



▼ To Create a Policy

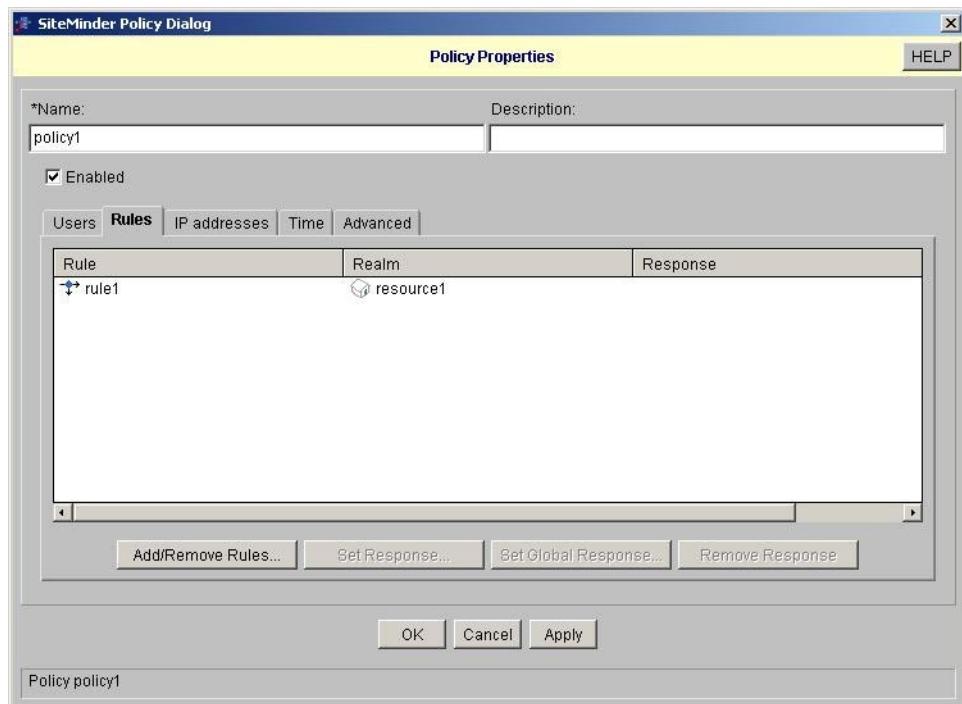
- 1 Create a rule under the **resource1** realm, and then configure the rule URLs.

In this example, the new rule is named rule1.



2 Create a policy.

In this example, the new policy is named *policy1*.

**3 Assign the users and add the rules to the policy.**

Using Federated Access Manager to Enable SiteMinder Federation in an Identity Provider Environment

The following is a high-level overview of the sequence you must follow to enable SiteMinder with Federated Access Manager in an Identity Provider Environment:

1. [Install the Principal Components.](#)
2. [Configure the Identity Provider Federated Access Manager to Use SAMLv2 Identity Provider Protocols.](#)
3. [Configure the SiteMinder Agent to Protect Federated Access Manager URLs.](#)
4. [Install the Federated Access Manager Policy Agent in the Service Provider.](#)
5. [Verify that Single Sign-On is Working Properly.](#)
6. [Review Sample Identity Provider Interactions.](#)

▼ To Install the Principal Components

The following are the principal components in this use case:

- Federated Access Manager in the Identity Provider container
- SiteMinder Policy Agent
- SiteMinder custom authentication module
- Federated Access Manager in the Service Provider container

Before You Begin

- The Identity Provider and Service Provider should be installed in different domains. If this is not possible, they should minimally use different cookie names or cookie domains.
- You can defer the installation of Federated Access Manager policy agent for protecting the Federated Access Manager Service Provider until the end of the installation procedures. This gives you the opportunity to verify that the SAML2 setup is working before you proceed.
- Before proceeding, be sure to read the general instructions in “[Installing SiteMinder](#)” on [page 99](#) and in “[Configuring SiteMinder After Installation](#)” on [page 100](#). The following steps provide additional installation information specific only to this use case.

1 **Install and configure Federated Access Manager in the same container in which the Identity Provider is installed.**

For detailed installation instructions, see the *Federated Access Manager Installation and Configuration Guide*.

- Be sure that the Identity Provider container supports SiteMinder policy agent installation.

- Configure Federated Access Manager to use the same user repository as the SiteMinder user repository. This enables both Federated Access Manager and SiteMinder to provide a single session for the same user.

2 Install and configure the SiteMinder policy agent on the Federated Access Manager container.

For now, configure the SiteMinder policy agent to protect an arbitrary URL on the container. In this example, the protected URL is /validation/index.html.

- As in the previous section, create a context root /validation, or create a directory named validation under the docroot.
- Be sure that the SiteMinder form authentication scheme is working for the protected URL.

3 Install the SiteMinder custom authentication module in Federation Access Manager.

After you unzip the Federated Access Manager binary, the SiteMinder custom authentication module is located under the directory *unzip-directory/integrations/siteminder/*. The *README.html* provides steps for building a custom authentication module. The following parameters must be set to enable the SiteMinder SDK to connect to the SiteMinder Policy Server:

SMCookieName:	SiteMinder cookie name. The default name is SMSESSION.
SharedSecret:	Unique policy agent configuration obtained from SiteMinder, and used by Federated Access Manager to point to the SiteMinder SDK.
PolicyServerIPAddress:	Indicates where the SiteMinder Policy Server is located.
CheckRemoteUserOnly:	This attribute should be enabled when the SiteMinder policy agent is installed on the same host as Federated Access Manager. The SiteMinder policy agent performs session validation. When this attribute is enabled, the rest of the configuration is not needed.
TrustedHostName:	Name of the SiteMinder SDK host name.
AccountPort	One of 3 TCP ports used by the SiteMinder Server to connect to the SiteMinder SDK.
AuthenticationPort:	One of 3 TCP ports used by the SiteMinder Server to connect to the SiteMinder SDK.
AuthorizationPort:	One of 3 TCP ports used by the SiteMinder Server to connect to the SiteMinder SDK.
MinimumConnection:	In a connection pool implementation, the maximum number of concurrent connections that a can be opened.
MaximumConnection:	In a connection pool implementation, the minimum number of concurrent connections that a can be opened.

StepConnection:	In a connection pool implementation, the number of concurrent connections that can be opened.
RequestTimeout:	Maximum time that the SiteMinder SDK waits before it connects to SiteMinder Policy Server.
RemoteUserHeaderName:	When configured, the SiteMinder policy agent sets a header name for the remote user after successful authentication. This parameter is used only when the checkRemoteHeaderOnly flag is set. The SMAuth module uses this parameter to create a Federated Access Manager session.

The following diagram shows an example of SiteMinder custom authentication module configuration.

The screenshot shows the Sun Java System Federated Access Manager configuration interface. The title bar reads "Sun Java System Federated Access Manager". The main menu bar includes "LOG OUT" and "HELP". The left sidebar shows the navigation path: "Access Control > Realm - opensso > Authentication Instance - SMAuth". The main content area is titled "SMAuth" and contains a section for "Realm Attributes". The configuration parameters listed are:

- SMCookieName: SMESSAGESESSION
- SharedSecret: (RC2)1r976MP0Vq5JPpkzsFsXxlutYkgfU
- PolicyServerIPAddres: 192.18.120.65
- CheckRemoteUserOnly: Enabled
- TrustedHostName: host1.example.com
- AccountPort: 44441
- AuthenticationPort: 44442
- AuthorizationPort: 44443
- MinimumConnection: 2
- MaximumConnection: 20
- StepConnection: 2
- RequestTimeout: 60
- RemoteUserHeaderName: REMOTE_USER

At the bottom of the configuration screen, there are "Save", "Reset", and "Back to Authentication" buttons. A "Done" button is located at the very bottom left. To the right of the "Done" button, there are three small icons labeled "Save", "Reset", and "Back to Authentication".

4 Install and configure Federated Access Manager in the container in which the Service Provider is installed.

For detailed installation instructions, see the Federated Access Manager Installation and Configuration Guide.

5 Install the SiteMinder Policy Agent in the Federation Access Manager container.

See the SiteMinder product documentation.

▼ To Configure the Identity Provider Federated Access Manager to Use SAMLv2 Identity Provider Protocols

Before you can enable the SAMLv2 Identity Provider protocols, you must generate, customize, and load each of the following:

- Identity Provider metadata
- Identity Provider extended metadata
- Service Provider metadata
- Service Provider extended metadata.

Before You Begin

- Read through the following instructions for the changes that you must make to the default metadata. The SAML2 samples contain instructions on how to setup SAML2.
- You must import Identity Provider metadata and Identity Provider extended metadata as hosted metadata. You must import Service Provider metadata and Service Provider extended metadata as remote entity metadata. To change a configuration from the default hosted to remote, modify the extended metadata XML element <EntityConfig>. Change the default attribute hosted=true to hosted=false.
- See the Federated Access Manager product documentation for commands and syntax.

1 Generate the metadata templates in both Identity Provider and Service Provider environments.

Use the `famadm` command. You can also use the browser-based interface at the following URL:

`http:host:port/opensso/famadm.jsp`

- At Identity Provider :

```
famadm create-metadata-templ -y idp_entity_id -u amadmin  
          -f admin_password_file_name -m idp_standard_metadata  
          -x idp_extended_metadata -i idp_meta_alias
```

where `idp_meta_alias` is `/idp`

- At Service Provider:

```
famadm create-metadata-templ -y sp_entity_id -u amadmin  
          -f admin_password_file_name -m sp_standard_metadata  
          -x sp_extended_metadata -s sp_meta_alias
```

where `sp_meta_alias` is `/sp`

2 Customize Identity Provider and Service Provider extended metadata.

The Identity Provider extended metadata should be added as an attribute named `AuthUrl`. This URL attribute is used by the SAML protocols to redirect for authentication purposes. In the following example, `AuthUrl` redirects to the SiteMinder authentication module.

```
<Attribute name="AuthUrl">
    <Value>http://host:port/opensso/UI/Login?module=SMAuth</Value>
</Attribute>
```

Another option is to make the SiteMinder custom authentication module the default login module in Federated Access Manager. The cost of using this option is that you must specify an LDAP login module for logging in as an administrator.

The Service Provider extended metadata uses the attribute named `transientUser`. Set this value to your anonymous user:

```
<Attribute name="transientUser">
    <Value>anonymous</Value>
</Attribute>
```

3 Load the Identity Provider and Service Provider metadata.

First create a Circle of Trust as mentioned in the URL. The Circle of Trust should also be added in the extended metadata.

In your extended template files, you will see a sample Circle of Trust. Modify the sample to create your Circle of Trust.

```
<Attribute name="cotlist">
    <Value>samplesaml2cot</Value>
</Attribute>
```

Load the hosted metadata in both the Identity Provider and the Service Provider using the `famadm` command or through Federated Access Manager administration console.

4 Exchange the metadata Service Provider with the Identity Provider metadata.**5 Exchange the Identity Provider metadata with the Service Provider.****6 Load all metadata.**

- 7 After successful metadata exchange, verify through the Federated Access Manager administration console that SAMLv2 is working properly.

The following shows a sample UI for SAMLv2 configuration.

The screenshot displays the Sun Java System Federated Access Manager administration interface. The top navigation bar includes 'VERSION', 'LOG OUT', 'HELP', and the Sun Microsystems, Inc. logo. The main header reads 'Sun Java System Federated Access Manager'. The top menu bar contains tabs for 'Access Control', 'Federation' (which is selected), 'Web Services', 'Configuration', and 'Sessions'. Below the menu, two collapsed sections are visible: 'Circle of Trust Configuration' and 'SAML1.x Configuration'. A section titled 'Circle of Trust Configuration' provides a brief description of its purpose: managing properties for a Circle of Trust, including importing and exporting providers. It features a table titled 'Circle of Trust (1 Items)' listing one provider entry:

Name	Entities	Realm	Status
samplesaml2cot	host2.example.com host1.example.com	/	active

Below this is another table titled 'Entity Providers (2 Items)', listing two provider entries:

Name	Protocol	Type	Location	Realm
http://host2.example.com:8080/opensso	SAMLv2	SP; IDP	Remote	/
http://host2.example.com:8080/opensso	SAMLv2	SP; IDP	Hosted	/

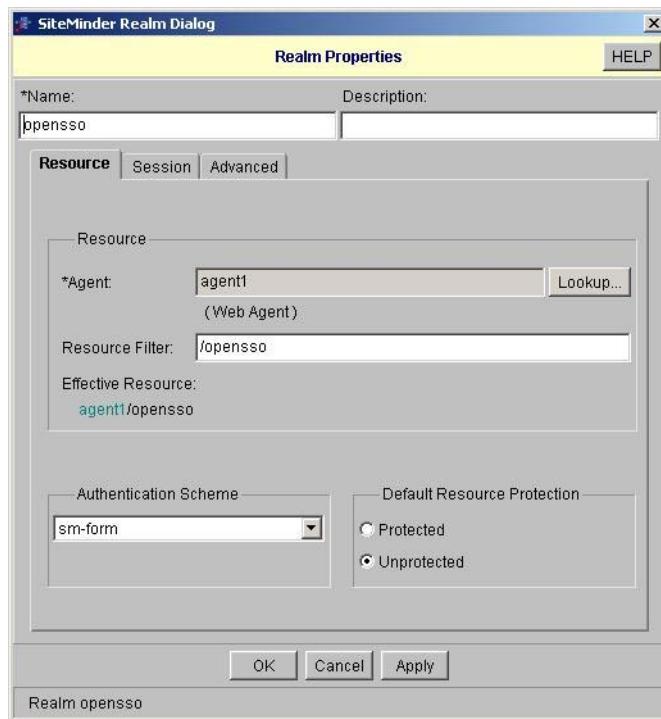
At the bottom left, there are 'Back to top' and 'Done' buttons.

▼ To Configure the SiteMinder Agent to Protect Federated Access Manager URLs

This configuration protects the SAML Single Sign-On Service URL so that the SiteMinder session must be established before the SAML assertion is generated.

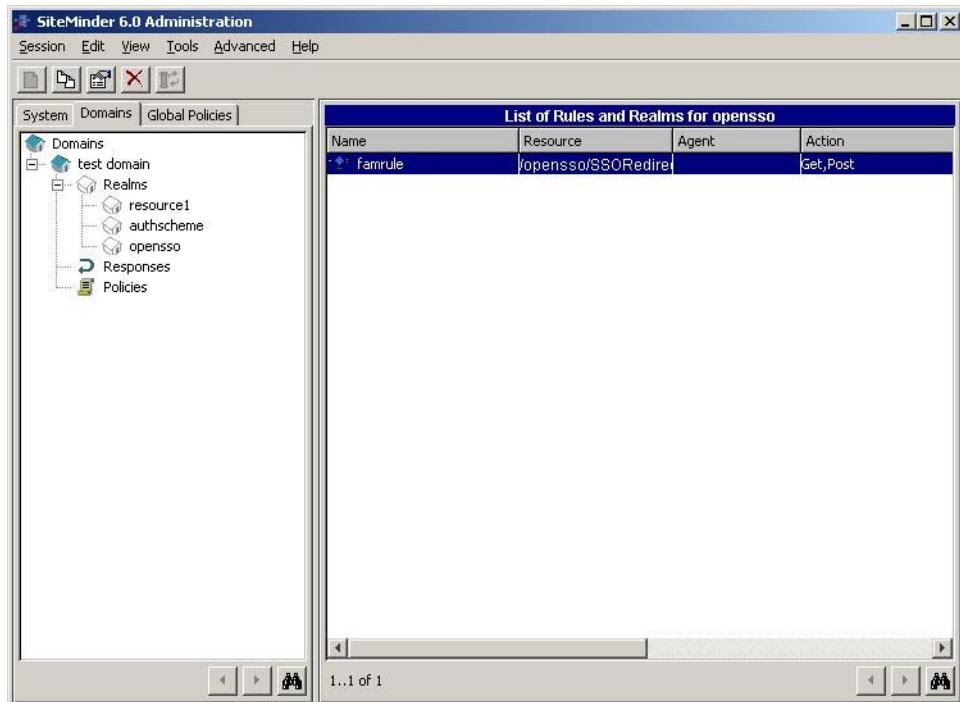
- 1 In the SiteMinder administration console, create a new realm in unprotected mode.

In this example, the realm is named opensso.



2 Create a rule that protects only the SAML2 SSO URL.

Other URLs are unprotected for now.



Installing the Federated Access Manager Policy Agent

The policy agent must be supported on the container where the enterprise application is deployed. For detailed installation information, see the policy agent documentation.

Change the policy agent login URL to the Federated Access Manager SAML2 Service Provider-initiated Single Sign-on Service URL. Example:

```
http://<sphost>:<spport>/opensso/saml2/jsp/spSSOInit.jsp?metaAlias=<Service Provider MetaAlias> &idpEntityID=<Identity Provider Entity ID>&NameIDFormat=transient
```

▼ To Verify that Single Sign-On is Working Properly

1 **Authenticate at the SiteMinder login page using user name and password.**

2 **Access the enterprise application in the Service Provider environment.**

The enterprise application is protected by Federated Access Manager Service Provider Agent. The agent should allow access to the application.

Sample Identity Provider Interactions

1. “[1. Access the SM Agent protected application](#)” on page 117
2. “[2. SiteMinder authentication](#)” on page 118
3. “[3. SAML Service Provider SSO initiation](#)” on page 120
4. “[4. Redirection to SiteMinder authentication module in Federated Access Manager](#)” on page 123
5. “[5. Finish SAML SSO](#)” on page 125

1. Access the SM Agent protected application

<http://HostName.example.com:9898/validation/index.html>

```
GET /validation/index.html HTTP/1.1
Host: HostName.example.com:9898
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive

HTTP/1.x 302 Moved Temporarily
Server: Netscape-Enterprise/6.0
Date: Fri, 01 Feb 2008 23:46:12 GMT
Cache-Control: no-cache
Location: http://HostName.example.com:9898/SiteMinderagent/forms/
login.fcc?TYPE=33554433&REALMID=06-1716e557-15f3-100f-b9a4-835cc8200cb3&GUID=
&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$sHjbzl4f9R%2bcSa0%2fEgnu6oUQQPMQnUg
kU6Zvx5zWzpQ%3d&TARGET=$SM$http%3a%2f%2fshivalik%2ered%2eiplanet%2ecom%3a9898%
2fvalidation%2findex%2ehtml
Connection: close
```

2. SiteMinder authentication

```
http://HostName.example.com:9898/SiteMinderagent/forms/login.fcc?TYPE=33554433&REALMOID=06-1716e557-15f3-100f-b9a4-835cc8200cb3&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$sHjbzl4f9R%2bcSa0%2fEgnu6oUQQPMQnUgkU6Zvx5zWzpQ%3d&TARGET=$SM$http%3a%2f%2fshivalik%2ered%2eiplanet%2ecom%3a9898%2fvalidation%2findex%2ehtml
```

```
GET /SiteMinderagent/forms/login.fcc?TYPE=33554433&REALMOID=06-1716e557-15f3-100f-b9a4-835cc8200cb3&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$sHjbzl4f9R%2bcSa0%2fEgnu6oUQQPMQnUgkU6Zvx5zWzpQ%3d&TARGET=$SM$http%3a%2f%2fshivalik%2ered%2eiplanet%2ecom%3a9898%2fvalidation%2findex%2ehtml HTTP/1.1
Host: HostName.example.com:9898
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9, text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

```
HTTP/1.x 200 OK
Server: Netscape-Enterprise/6.0
Date: Fri, 01 Feb 2008 23:46:12 GMT
Content-Type: text/html; charset=ISO-8859-1
Connection: close
```

```
-----  
http://HostName.example.com:9898/SiteMinderagent/forms/login.fcc?TYPE=33554433&REALMOID=06-1716e557-15f3-100f-b9a4-835cc8200cb3&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$sHjbzl4f9R%2bcSa0%2fEgnu6oUQQPMQnUgkU6Zvx5zWzpQ%3d&TARGET=$SM$http%3a%2f%2fshivalik%2ered%2eiplanet%2ecom%3a9898%2fvalidation%2findex%2ehtml
```

```
POST /SiteMinderagent/forms/login.fcc?TYPE=33554433&REALMOID=06-1716e557-15f3-100f-b9a4-835cc8200cb3&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$sHjbzl4f9R%2bcSa0%2fEgnu6oUQQPMQnUgkU6Zvx5zWzpQ%3d&TARGET=$SM$http%3a%2f%2fshivalik%2ered%2eiplanet%2ecom%3a9898%2fvalidation%2findex%2ehtml HTTP/1.1
Host: HostName.example.com:9898
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9, text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
```

```

Connection: keep-alive
Referer: http://HostName.example.com:9898/SiteMinderagent/forms/
login.fcc?TYPE=33554433&REALMID=06-1716e557-15f3-100f-b9a4-835cc8200cb3&
GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$hjbzl4f9R%2bcSa0%
2fEgnu6oUQQPMQnUgkU6Zvx5zWZpQ%3d&TARGET=$SM$http%3a%2f%2fshivalik%2ered%
2eiplanet%2ecom%3a9898%2fvalidation%2findex%2ehtml
Content-Type: application/x-www-form-urlencoded
Content-Length: 233
SMENC=ISO-8859-1&SMLOCALE=US-EN&USER=test&PASSWORD=test&target=http%
3A%2F%2FHostName.example.com%3A9898%2Fvalidation%
2Findex.html&smauthreason=0&smagentname=sHjbzl4f9R%2BcSa0%
2FEgnu6oUQQPMQnUgkU6Zvx5zWZpQ%3D&postpreservationdata=
HTTP/1.x 302 Moved Temporarily
Server: Netscape-Enterprise/6.0
Date: Fri, 01 Feb 2008 23:46:18 GMT
Content-Type: magnus-internal/fcc
Set-Cookie: SMSESSION=2xm2Iw6fTMBcjA6rlK/YUY1CRBudYxw0CkfpCo95YKAp2b4ZzLOPT
qi2S14CQ7nRja+fUq53Aj0pmTxDvPKTMKD10l1hGx0gPK7xx2eqMP3IyTAK3qNahRgt7mQRTIB
BDEE0r0JcpgrMRtsteC90yMdiJrrEeqfc38utU6mx09BejwjRuGN2rmf9WM40dl+4TE0iU0iP/k
iCR6sn2r03GBsbBj0i12oSlh/4JAYf0wxsgBJCwDiZVlFXNiKNaKdY1UQr80cKe033eNn3w9RW9
ZrjRibQTQcxxmiR+gsvAuM8etEzP6GCFKjc1s8I3DNuSBbDqfyt81YUSYdEYa9UKfvvOJplZOIT
Bk0ajcAEPOq+TYxQ4BH2RmjdpMVC1xRm2bibM90tuQD83C9QubTK1lq4j+ywPsutiYEoGHV+7
6VXws5NsvhK2gH4ZTC0xsd76X2/1n08xMv9c3W4DcSp9cQ074/7+a7gzT+hx0SpyQFF4mDTnq/D
XS5V7tcLS0EyFcf8RwSbvDPnICiebR3vtZgHLR1kEZheEh9ToHmwqIO9cCqz9rJXR7/NL+o/AQr
7M4o+LyA7KxozaEuj0pg8GINteUGVxMLWmR7Xm/Lp0pI9DjM5mbmP8Ka+w0T6H9LHNlQGaYZA
PCkeABAxqLb8q8yJuZPdI0BVlp1awNx579DereocIzCzdQ99rVDSQU$77KCQATnYXrHqTxqbXxw
beDf6gk9Zcf29XTz08hBLdScqGOBX10vDvzdghcjHnupQf1fYltt/3MrZ/Jrxonbpgxg4C5zVgSU
PrNqb66RYWQ0elZXooh7lTPoFHsMFodVnecsOZmEMXNI8DB08pyo5KhRZjk2Mr4o3rPNTiHPpnXc
d+imapuosG3FwF5Sv6flh8jbiE9/MzdIQ06hgWEIiCnUEYdboli4TWgy0/QpCbdJ70viU275Vzic
W6hMTTRyxnEvoQ=; path=/; domain=.red.example.com
Cache-Control: no-cache
Location: http://HostName.example.com:9898/validation/index.html
Connection: close
-----
http://HostName.example.com:9898/validation/index.html
GET /validation/index.html HTTP/1.1
Host: HostName.example.com:9898
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://HostName.example.com:9898/SiteMinderagent/forms/

```

```

login.fcc?TYPE=33554433&REALMOID=06-1716e557-15f3-100f-b9a4-835cc8200cb3&GUID=
&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$sHjbz14f9R%2bcSa%2fEgnu6oUQQPMQnUg
KU6Zvx5zWZpQ%3d&TARGET=$SM$http%3a%2f%2fshivalik%2ered%2eiplanet%2ecom%3a9898%
2fvalidation%2findex%2ehtml
Cookie: SMSESSION=2xm2Iw6fTMBCjA6rlK/YUY1CRBudYxw0CkfpCo95YKAp2b4ZzLOPTqi2S14
CQ7nRja+fUq53Aj0pmTxDvPKTMcKD1Ql1hGx0gPK7xx2eqMP3IyTAK3qNahRgt7mQRTIBBDE0r0J
cpgrMRtsteC90yMdiJrrEeqfc38utU6mx09BejwjRuGN2rmf9WM40dl+4TE0iU0iP/kicR6sn2r03
GBsbBj0i120sLh/4JAyf0wxsgBJCwDizVlFXNiKNaKdY1U0r80cKe033eNn3w9RW9ZrjRibQTQcxx
miR+gsvAuM8etEzP6GCFKj1s8I3DNuSBbDqfy81YUSYdEYa9UKfvvvOJplZOITBkQajcAEPOq+vT
YxQ4BH2RmjdpMVCIxRm2bibM9QtuQD83C9QubTk1lq4j+ywPsvutiYEoGHV+76VXws5NsvhK2gH4Z
TC0xsd76X2/1no8xMv9c3W4DcSp9cQ074/7+a7gzT+hxQSpyQFf4mDTnq/DXS5V7tcLS0EyFc f8Rw
SbvDPnICiebR3vtZgHRL1kEZheH9ToHmwqI09cCqz9rJXR7/NL+o/AQr7M4o+LyA7KxozaueUj0p
g8GINteUGVxMLWmR7Xm/Lp0pI9DjM5mfbdP8Ka+w0T6H9LHNlQGaYZAPCkeABAXqlb8q8yJUzPdI0
BVlp1awNCx579Dere0CIzCZd099rVDSQU$77KCQATnYXrHqTxqbXxWbeDf6gk9ZCf29XTz08hBLdS
cqGOBX10vDvzdghcjHnupQf1fYltt/3Mrz/Jrxonbpxg4C5zVgSUPrNqb66RYWQ0elZXooh7LTpo
FHsMFodVnecs0ZmEMXNI8DB08pyo5KhRZJk2Mr4o3rPntiHPpnXcd+imapu0sG3FwF5Sv6flh8jbi
E9/MZdIQ06hgWEIiCnUEYdboli4Twgy0/QpCbdJ70viU275VZiCW6hMTRyxnEvoQ=

```

```

HTTP/1.x 200 OK
Server: Netscape-Enterprise/6.0
Date: Fri, 01 Feb 2008 23:46:18 GMT
Set-Cookie: SMSESSION=j100TgMQfglpU+GH0CJqbnoE2Pevax6fdzPGU7ZAgJuPb/fxTjCbWx1
B1R060aLJn6VoVGNK8Sy6IeILAyv+LciS/OMK1E0tSXnL5Uvit3XiUwuiSMuklyDMIL0Q6n3ZSGGr
9sKBuCh5YVfGcfGjHQFcBILzeqzQxBRrgH/l2rc8aTEHdCrprvBiRHwQlxJbrclWmqfJw7h+HUEtiz9
bQCUkwMbpEW4eBfNyRlZTGov3K5hg4HK4tuoyv0eKdZaewLTB4Lm+QeGWo2qv2mPDP+eVtBiVtRVH
HTHGF5thTJYQ00c4rPV2dn18axpWppGByeUmfmService Provider9x5hVxDi91iyobTybKpDz0
bltkvnHbqwbLfehUPTJFxS3Z54y9dmiuoQ+B5Kdrs7DNuvrnAI1ZQdDKQEVA4Pt+vA9K018ah9V1I
7BZ9D/x60uWxafa3Tjy8lRgWhMYqdBulFMD1B29sxb0NHwdJ2FaxQJGjmPSEZ5iHB50ovF4YFXRyPP
5Tl7eJxIebLKX02LFrG/osNZ9UKhrMY1MRK5WWhJlyB040ADVcTNrFkc39vcYIA1eGDYhC/Na0d41
2HP5S0UX0/59ADMBlBsX/qbjcd0Dy3li+4eZnK1oHw/9yr3LCjewJ+H9w0k0/dQw99vgwEM2RPFgH5
Y7W6k6h1efp67VKXLBiJ10ZPJe2SCEDAOUla8qsC8fQ0VWTy/TfVhVtqJoaSLZrACX7uhPzbZE1EA
Pd8x7UeJquFl3WpdnZYObd0DQLeoWZcF2rPIcfBn+8X8oig5KzvAgQ9R8MR+h70kYfhmwBDaQkb
KPpIXjpeLNxKpkEVWJ9HoHOpZ/txCQUAHqPV41YjZ6CQfbUqd0Hbfje90+0pj1aHMntI4VYZ0qdx
sA+n9cgKjNQ8ruH0qSKhAQfEgipwcM2fMU3Uqmtr+0/+5bi7Cbs=; path=/;
domain=.red.example.com
Content-Type: text/html
Etag: "dcea10a4-1-0-88"
Last-Modified: Thu, 10 Jan 2008 01:42:07 GMT
Content-Length: 136
Accept-Ranges: bytes
-----
```

3. SAML Service Provider SSO initiation

```

http://ide-13.red.example.com:8080/opensso/saml2/jsp/spSSOInit.jsp?
metaAlias=/sp&idpEntityId=
http://HostName.example.com:8080/opensso&NameIDFormat=transient

```

```
GET /opensso/saml2/jsp/spSSOInit.jsp?metaAlias=/sp&idpEntityID=
http://HostName.example.com:8080/opensso&NameIDFormat=transient HTTP/1.1
Host: ide-13.red.example.com:8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: SMSESSION=jL00TgM0fglpU+GHQCJqbnoE2Pevax6fdzPGU7ZAgJuPb/fxTj
CbWX1B1R06QaLJn6VoVGNK8Sy6IeILAyv+LciS/OMK1E0tSXnL5Uvit3XIuWuiSMukly
DMIl0Q6n3ZSGGr9sKBUCH5YVfGcfGjHQFcBILzeqXbRrgH/l2rc8aTEHdCrprvBiRHw
QlxJbrcwMqfJw7h+HUEtiz9bQCUkwMbPWE4eBfNyRLZTGov3K5hg4HK4tuoyv0eKdZae
wLTB4Lm+QeGWo2qv2mPDP+eVtBiVtRVHHTHGfSthTJYQ00c4rPV2dn18axpWppGByeUm
fmeService Provider9x5hVxDi91iyobTybKpdz0bltkvnHbqwbLfehUPtJFxS3Z54y9
dmiuoQ+B5Kdrs7DNUvrnAI1ZQdDKQEVA4Pt+vA9K018ah9V1I7BZ9D/x60uWxfA3Ty8l
RgWhMYqdBuLFMD1B29sxboNHwdJ2FaxQJGjmPEZ5iHB50ovF4YFXRyPP5Tl7eJxIebLK
X02LFrG/osNZ9UKhrMY1MRK5WWhJlYB040ADVcTNrFkc39vcYIA1eGDYhC/Na0d412HP5
S0UX0/59ADMLBsX/qBjcd0Dy3li+4eZnK1oHw/9yr3LCjewJ+H9w0k0/dQw99vgwEM2RP
FgH5Y7W6k6h1efp67VXKLBIj10ZPJe2SCEDAOUla8qsC8fQ0VWTy/TfVhVtqJ0aSLZrAC
X7uhPzbZE1EAPd8x7UejquFll3WpdnZY0bd0DQLeoWZcF2rPifcBn+8X8oig5KzvAgQ9R8
MR+h70kYfhmwBDaQkbKPpIxjpeLnxKpkEVWJ9HoHOpZ/txCQUAHqPV41YjZ6CQfbfUqd
OHbfje90+0pj1aHMntI4YZ0qdxsA+n9cgKjNQ8ruH0qSKhAQfEgipwcM2fMU3Uqmtr+0
/+5bi7Cbs=
```

HTTP/1.x 302 Moved Temporarily

X-Powered-By: JService Provider/2.1

Server: Sun Java System Application Server 9.1

Set-Cookie: JSESSIONID=765d4c266461607b4b55811d34ca; Path=/opensso

Location: http://HostName.example.com:8080/opensso/SSORedirect/
metaAlias/idp?SAMLRequest=nVTNjtowEL7vU0S%2BQ5ywXcACJAqqirRtKbA99Gac
SbHq2KlnwtK3rx1YRNuv2nIdj2e%2B2P3uEsjK1mDa0syv41QBSkhwqY1G0J2PWeCucRI
3CypgQkBLo6adHKXe5ql0jp5xdh4v5mGHeH%2B2YPSvF80Nxu4aHkWZaDLp12Rts%2B8
PBu16ewZDFk5Z8A4%2Fa2TELiyQGxgYZGkpVdfNDheYdmn7wn7vuix7%2BzzB6gaS
upvbUjqkwA4k7vpdE%2Fux6Krq6NtEBd5Sox4AOehosokvX6y8rKLQHRWKFJKdGS0x1
UbPkg%2FMKwvJjVqkDELEsJaLew7myPLF8r22h7Y%2FrkmyPTsg%2BbjbLztSTLqUilk
wrWuFwM2exqcCwe%2B1gqfV45m0LqCT9a6Teb1%2BwQRrNrkRbtEK65%2FMPA6WPkc
ik3eDmGUxqw6La7F5zB8MV86o9XvWIUrakgXe%2B0FV10yrfZVkJcWNdig7noZ939tQh
hKdF5%2FFA3WG00eZx4kBc%2FJN8AmR45%2FszpTPb0TKNrgBEMIDnQL5Zmrauk1xkTD
IcZkcrTxcvDMBJdwUN5i6tU2JVQchcox8M%2FOFzHo4ZFA5YnK1s7TyevX8Jw1elWOIF
b679cy%2BQM%3D

Content-Type: text/html;charset=ISO-8859-1

Content-Length: 0

Date: Fri, 01 Feb 2008 23:47:30 GMT

<http://HostName.example.com:8080/openssso/SSORedirect/metaAlias/>
idp?SAMLRequest=nVTNjtowEL7vU0S%2BQ5ywXcACJAqqirRtKbA99GacSbHq2Klnw
tK3rx1YRNUn2nIdj2e%2BP3uEsjK1mDa0syv41QBSkhwY1G0J2PWeCucRI3CygpQkB
Lr6adHkXe5qL0jp5xhd4v5mGHeH%2BYPSvF80Nxu4aHkWZaDLPl2Rts%2B8PBu16ew
ZDfK5Z8A4%2Fa2TELY1iyQGxgYZGkpVDifNDheYdnm7wn7vuix7%2BzzB6gaSupvbUj
qkWa4k7vpdE%2Fux6Krq6NtEBd5Sox4A0euhosokvX6y8rKLQHRWkFJKdGS0x1UbPkg
%2FMKwVjVkqDELEsJaLew7myPLF8r22h7Y%2FrkmyPTSG%2BbjbLztSTLqUilkRwU
fwM2exqcCvwe%2B1gqfV45m0LqCT9a6Teb1%2BwQRrNrkbRbtEK6S%2FMPA6WPkCik3
eDmGUxqw6La7F5zB8MV86o9XvWxIUrakXe%2BOFV10yrZVkJcWNdig7noZ939tQhhK
Df5%2FFA3WG00eZx4kBc%2FJN8AmR45%2FszpTPb0TKNrgBEMIDnQL5Zmrauk1xkTDI
cZkcrTxcvDMBJdWUN5i6tU2JVQcHcox8M%2FOFzHo4ZFAyNk1s7TyevX8Jw1elWOIF
b679cy%2BQM%3D

GET /openssso/SSORedirect/metaAlias/idp?SAMLRequest=nVTNjtowEL7vU0S%2BQ5ywXcACJAqqirRtKbA99GacSbHq2KlnwK3rx1YRNUn2nIdj2e%2BP3uEsjK1mDa0syv41QBSkhwY1G0J2PWeCucRI3CygpQkB
Lr6adHkXe5qL0jp5xhd4v5mGHeH%2BYPSvF80Nxu4aHkWZaDLPl2Rts%2B8PBu16ewZDfK5Z8A4%2Fa2TELY1iyQGxgYZGkpVDifNDheYdnm7wn7vuix7%2BzzB6gaSupvbUj
qkWa4k7vpdE%2Fux6Krq6NtEBd5Sox4A0euhosokvX6y8rKLQHRWkFJKdGS0x1UbPkg%2FMKwVjVkqDELEsJaLew7myPLF8r22h7Y%2FrkmyPTSG%2BbjbLztSTLqUilkRwU
fwM2exqcCvwe%2B1gqfV45m0LqCT9a6Teb1%2BwQRrNrkbRbtEK6S%2FMPA6WPkCik3eDmGUxqw6La7F5zB8MV86o9XvWxIUrakXe%2BOFV10yrZVkJcWNdig7noZ939tQhhK
Df5%2FFA3WG00eZx4kBc%2FJN8AmR45%2FszpTPb0TKNrgBEMIDnQL5Zmrauk1xkTDI
cZkcrTxcvDMBJdWUN5i6tU2JVQcHcox8M%2FOFzHo4ZFAyNk1s7TyevX8Jw1elWOIF
b679cy%2BQM%3D HTTP/1.1

Host: HostName.example.com:8080

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)

Gecko/20071127 Firefox/2.0.0.11

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

Cookie: SMSESSION=jl00TgM0fglpU+GHQCJqbnoE2Pevax6fdzPGU7ZAqJuPb/fxTjCbWx1B1R06QaLJn6VoVGNK8Sy6IeILAyv+LciS/OMK1E0tSXnL5Uvit3XiUwUiSmuklyDM
IloQ6n3ZSGGr9sKBUCH5YVfGcfGjHQFcBILzeq0xBRrgH/l2rc8aTEHdCrprvBiRHwqlx
JbrcwMqfJw7h+HUEtiz9bQCUkwMbpEW4eBfNyRlZTGov3K5hg4HK4tuoyv0eKdZaewlTB
4Lm+0qeGWo2qv2mPDP+eVtBiVtRVHHTHGfShTJYQ00c4rPV2dn18axpwppGByeUmfm
Service Provider9x5hVxDi91iyobTybKpDz0blkvnHbqwbLfrehUPtJFxS3Z54y9dm
iuoQ+B5Kdrs7DNuvrnAI1ZqdDKQEVa4Pt+vA9K018ah9V1I7BZ9D/x60uWxfA3Ty8lRg
WhMYqdBulFMD1B29sxb0NHwdJ2FaxQJGjMpSEZ5iHB50ovF4YFXRyPP5Tl7eJxIebLKX02
LFrG/osNZ9UKHrMY1MRK5WHJlYB040ADVcTNrFkc39vcYIA1eGDYhC/Na0d412HP550UX
0/59ADMLBsX/qBjcd0Dy3li+4eZnK1oHw/9yr3LCjewJ+H9w0k0/dQw99vgwEM2RPFgH5Y
7W6k6h1efp67VKXLBIJ1OZPJe2SCEDA0Ula8qsC8fQ0VWTy/TfVhVtqJ0aSLzrACX7uhPz

```
bZE1EAPd8x7UeJquFl13WpdnZYObd0DQLeoWZcF2rPIcfBn+8X8oig5KzvAgQ9R8MR+h70
kYfhmwBDAqkbKPpIxjpeLNxKpkEVWJ9HoHOpZ/txCQUAHqPV41YjZ6CQfBfUqdOHbfje9
O+0pJ1aHMntI4VYZ0qdxsA+n9cgKjNQ8ruH0qSKhAQfEgipwcM2fMU3Uqmtr+0/+5bi7Cbs=
```

```
HTTP/1.x 302 Moved Temporarily
X-Powered-By: JService Provider/2.1
Server: Sun Java System Application Server 9.1
Set-Cookie: JSESSIONID=766be1d1028d55badd1ed0fe34ac; Path=/opensso
Location: http://HostName.example.com:8080/opensso/UI/Login?module=
SMAuth&goto=http%3A%2F%2FHostName.example.com%3A8080%2Fopensso%
2FSSORedirect%2FmetaAlias%2Fidp%3FReqID%3Ds27926cc0299bbe6f0112ead7
ff38b7985321e904c
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 0
Date: Fri, 01 Feb 2008 23:48:30 GMT
-----
```

4. Redirection to SiteMinder authentication module in Federated Access Manager

```
http://HostName.example.com:8080/opensso/UI/Login?module=SMAuth&goto=
http%3A%2F%2FHostName.example.com%3A8080%2Fopensso%2FSSORedirect%
2FmetaAlias%2Fidp%3FReqID%3Ds27926cc0299bbe6f0112ead7ff38b7985321e904c

GET /opensso/UI/Login?module=SMAuth&goto=http%3A%2F%2FHostName.example.com%
3A8080%2Fopensso%2FSSORedirect%2FmetaAlias%2Fidp%3FReqID%3Ds27926cc0299bbe6f0112
ead7ff38b7985321e904c HTTP/1.1
Host: HostName.example.com:8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=
0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: JSESSIONID=766be1d1028d55badd1ed0fe34ac; SMSESSION=j100TgMQfglpU+GHQ
CJqbnoE2Pevax6fdzPGU7ZAgJuPb/fxTjCbWXB1R06QaLJn6VoVGNK8Sy6IeILAyv+LciS/OMK1
E0tSXnL5Uvit3XIuWuiSMuklyDMl0Q6n3ZSGGr9sKBUCH5YVfGcfGjHQFcBILzeqQxBRrgH/l2r
c8aTEHdCrprvBiRHwQlxJbrcwMqfJw7h+HUEtiz9bQCUkwMbpEW4eBfNyRlZTGov3K5hg4HK4tuo
yv0eKdZaewLTB4Lm+QeGwo2qv2mPDP+eVtBiVtRVHHTHGfSthTJYQ00c4rPV2dn18axpWppGByeU
mfmeService Provider9x5hVxDi9liyobTybKpDz0bltkvnHbqwLfehuPtJFxS3Z54y9dmiuoQ+
B5Kdrs7DNuvrnAI1ZQdDKQEVA4Pt+vA9K018ah9V1I7BZ9D/x60uWxfaA3Ty8lRgWhMYqdBuIAMD
1B29sxboNHwdJ2FaxQJGjMpSEZ5iHB50ovF4YFXRyPP5Tl7eJxIebLKX02LFrG/osNZ9UKHrMY1M
RK5WHJlYB040ADVcTNrFkc39vcYIA1eGDYhC/Na0d412HP5S0UX0/59ADMIBsX/qBjcd0Dy3li+
4eZnK1oHw/9yr3LCjewJ+H9w0k0/dQw99vgwEM2RPFgH5Y7W6k6h1efp67VKLBiJ10ZPJe2SCED
```

AOUla8qsC8fQ0VwTy/TfVhVtqJ0aSLZrACX7uhPzbZE1EAPd8x7UeJquFll3WpdnZYObd0DQLeoW
ZcF2rPIcfBn+8X8oig5KzvAgQ9R8MR+h70kYfhmwBDaQkbKPpIxjpeLNxKpkEVWJ9HoHOpZ/txC
QUAHqPV41YjZ6C0fbUqdOHbfje90+0pJ1aHMntI4VYZ0qdxsA+n9cgKjNQ8ruHOqSKhAQfEgipw
cM2fMU3Uqmtr+0/+5bi7Cbs=

HTTP/1.x 302 Moved Temporarily
X-Powered-By: Servlet/2.5
Server: Sun Java System Application Server 9.1
Cache-Control: private
Pragma: no-cache
Expires: 0
X-DSAMEVersion: 8.0 (2007-November-29 01:17)
AM_CLIENT_TYPE: genericHTML
Set-Cookie: AMAuthCookie=AQIC5wM2LY4SfczvfJJpn1IfT3pStks2VjzPMebgYVAxtxE=@AAJTSQACMDE=#; Domain=HostName.example.com; Path=/
Set-Cookie: amlbcookie=01; Domain=HostName.example.com; Path=/
Set-Cookie: iPlanetDirectoryPro=AQIC5wM2LY4SfczvfJJpn1IfT3pStks2VjzPMebgYVAxtxE=@AAJTSQACMDE=#; Domain=HostName.example.com; Path=/
Set-Cookie: AMAuthCookie=LOGOUT; Domain=HostName.example.com;
Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
X-AuthErrorCode: 0
Location: http://HostName.example.com:8080/opensso/SSORedirect/metaAlias/
idp?ReqID=s27926cc0299bbe6f0112ead7ff38b7985321e904c&iPlanetDirectoryPro=
AQIC5wM2LY4SfczvfJJpn1IfT3pStks2VjzPMebgYVAxtxE%3D%40AAJTSQACMDE%3D%23
Content-Type: text/html; charset=iso-8859-1
Content-Length: 0
Date: Fri, 01 Feb 2008 23:48:30 GMT

http://HostName.example.com:8080/opensso/SSORedirect/metaAlias/idp?ReqID=
s27926cc0299bbe6f0112ead7ff38b7985321e904c&iPlanetDirectoryPro=
AQIC5wM2LY4SfczvfJJpn1IfT3pStks2VjzPMebgYVAxtxE%3D%40AAJTSQACMDE%3D%23

GET /opensso/SSORedirect/metaAlias/idp?ReqID=s27926cc0299bbe6f0112ead7ff38b7985321e904c&iPlanetDirectoryPro=AQIC5wM2LY4SfczvfJJpn1IfT3pStks2VjzPMebgYVAxtxE%3D%40AAJTSQACMDE%3D%23 HTTP/1.1
Host: HostName.example.com:8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: JSESSIONID=766be1d1028d55badd1ed0fe34ac; SMSESSION=jl00TgMQfglpU+GHQCJqbnoE2Pevax6fdzPGU7ZAgJuPb/fxTjCbWX1B1R06QaLJn6VoVGNK8Sy6IeILAyv+Lci

```
S/OMK1E0tSXnL5Uvit3XIuWuiSMuklyDMIL0Q6n3ZSGGr9sKBUCH5YVfGcfGjHQFcB1lzeqQx
BRrgH/l2rc8aTEHdCrprvBiRHwQlxJbrcwMqfJw7h+HUEtiz9bQCUkwMbpEW4eBfNyR1ZTGov
3K5hg4HK4tuoyv0eKdZaewLTB4Lm+QeGWo2qv2mPDP+eVtBiVtRVHHTHgfSthTJYQ00c4rPV2
dn18axpWppGByeUmfmService Provider9x5hVxDi91iyobTybKpDz0blkvnHbqwbLfehUP
tJFxS3Z54y9dmuoQ+B5Kdrs7DNvrnAI1ZQdDKQEVA4Pt+vA9K018ah9V1I7BZ9D/x60uWxfA
A3Ty8lRgWhMYqdBulFMD1B29sxboNHwDj2FaxQJGjMpSEZ5iHB50ovF4YFXRyPP5Tl7eJxIebL
KX02LFrG/osNZ9UKhrMY1MRK5WHJ1YB040ADvcTNrFkc39vcYIA1eGDYhC/Na0d412HP5S0UX
0/59ADMbSx/qbjcd0dy3li+4eZnKloHw/9yr3LCjewJ+H9w0k0/dQw99vgwEM2RPFgh5Y7W6
k6h1efp67VKXLBIj10ZPJe2SCEDAOula8qsC8fQ0VWtTy/TfVhVtqJ0aSLzrACX7uhPzbZE1EAP
d8x7UeJquFll3WpdnZYObd0DQLeoWZcF2rPIcfBn+8X8oig5KzvAgQ9R8MR+h70kYfhmwBDaQ
kbKpIxjpeLNxKpkEVWJ9HoHOpZ/txCQUAHqPV41YjZ6CQfbUqdOHbfje90+0pJ1aHMntI4VY
Z0qdxsA+n9cgKjNQ8ruHOqSKhAQfEgipwcM2fMU3Uqmtr+0/+5bi7Cbs=; amlbcookie=01;
iPlanetDirectoryPro=AQIC5wM2LY4SfczvfJJpn1IfT3pStks2VjzPMebgYVAxtxE=@AAJTS
QACMDE=#

```

HTTP/1.x 302 Moved Temporarily
 X-Powered-By: JService Provider/2.1
 Server: Sun Java System Application Server 9.1
 Location: http://ide-13.red.example.com:8080/opensso/Consumer/metaAlias/
 sp?SAMLart=AAQAAE6JQxQxFQ72nsd5qDmVUTW5T3ieNSAqIA DayEcXVxKAZQSjzCxJMDE%3D
 Content-Type: text/html; charset=ISO-8859-1
 Content-Length: 0
 Date: Fri, 01 Feb 2008 23:48:30 GMT

5. Finish SAML SSO

<http://ide-13.red.example.com:8080/opensso/Consumer/metaAlias/sp?SAMLart=AAQAAE6JQxQxFQ72nsd5qDmVUTW5T3ieNSAqIA DayEcXVxKAZQSjzCxJMDE%3D>

GET /opensso/Consumer/metaAlias/sp?SAMLart=AAQAAE6JQxQxFQ72nsd5qDmVUTW5T3ieNSAqIA DayEcXVxKAZQSjzCxJMDE%3D HTTP/1.1
 Host: ide-13.red.example.com:8080
 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
 Gecko/20071127 Firefox/2.0.0.11
 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
 text/plain;q=0.8,image/png,*/*;q=0.5
 Accept-Language: en-us,en;q=0.5
 Accept-Encoding: gzip,deflate
 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
 Keep-Alive: 300
 Connection: keep-alive
 Cookie: JSESSIONID=765d4c266461607b4b55811d34ca; SMSESSION=j100TgMQfglpU+
 GHQCJqbn0e2Pevax6fdzPGU7AgJuPb/fxTjCbWX1B1R06QaLJn6VoVGNK8Sy6IeILAyv+Lci
 S/OMK1E0tSXnL5Uvit3XIuWuiSMuklyDMIL0Q6n3ZSGGr9sKBUCH5YVfGcfGjHQFcB1lzeqQx
 BRrgH/l2rc8aTEHdCrprvBiRHwQlxJbrcwMqfJw7h+HUEtiz9bQCUkwMbpEW4eBfNyR1ZTGov
 3K5hg4HK4tuoyv0eKdZaewLTB4Lm+QeGWo2qv2mPDP+eVtBiVtRVHHTHgfSthTJYQ00c4rPV2

```
dnl8axpWppGByeUmfmeService Provider9x5hVxDi91iyobTybKpDz0bltkvnHbqwbLfehU  
PtJFxS3Z54y9dmiuoQ+B5Kdrs7DNuvrnAI1ZQdDKQEVA4Pt+vA9K018ah9V1I7BZ9D/x60uWx  
faA3Ty8lRgwHMYqdBu1FMD1B29sxb0NHwdj2FaxQJGjmPSEZ5iHB500vF4YFXRyPP5Tl7eJxI  
ebLKX02LFrG/osN9ZUKHrMY1MRK5WWHJLYB040ADvCtnrFkc39vcYIA1eGDYhC/Na0d412HP5  
S0UX0/59ADMLBsX/qBjcd0Dy3l1+4eZnK1oHw/9yr3LCjewJ+h9w0k0/dQw99vgwEM2RPFgH5Y  
7W6k6h1efp67VKXLBiJ10ZPJe2SCEDAOUla8qsC8fQ0WTy/TfVhVtqJ0aSLzrACX7uhPzbZE1  
EAPd8x7UeJquFl3WpdnZYObd0DQLe0WZcF2rPIcfBn+8X8oig5KzvAgQ9R8MR+h70kYfhmwB  
DaQkbKPpIxjpeLNxKpkEVWJ9HoHOpZ/txCQUAHqPV41YjZ6CQfBfUqdOHbfje90+0pJ1aHMntI  
4VYZ0qdxsA+n9cgKjNQ8ruH0qSKhAQfEgiwcM2fMU3Uqmtr+0/+5bi7Cbs=
```

```
HTTP/1.x 200 OK  
X-Powered-By: JService Provider/2.1  
Server: Sun Java System Application Server 9.1  
Set-Cookie: iPlanetDirectoryPro=AQIC5wM2LY4SfcxHYS5DBuFiEDZVArdPot5Wt07zTqK06+w=  
@AAJTSQACMDE=#; Domain=ide-13.red.example.com; Path=/  
Content-Type: text/html; charset=ISO-8859-1  
Transfer-Encoding: chunked  
Date: Fri, 01 Feb 2008 23:47:30 GMT
```

Using Federated Access Manager to Enable SiteMinder Federation in a Service Provider Environment

The following is a high-level overview of the sequence you must follow to enable SiteMinder with Federated Access Manager in a Service Provider Environment:

1. [Install Federated Access Manager Instances.](#)
2. [Install and Configure SiteMinder in Service Provider Domain.](#)
3. [Configure Federated Access Manager Identity Provider and Service Provider for SAML2 protocols.](#)
4. [Review Sample Single Sign-On Interactions.](#)

▼ To Install Federated Access Manager Instances

1 [Install Federated Access Manager in the Identity Provider Environment.](#)

Federated Access Manager is not the only supported access control software that can be used in the Identity Provider. But for optimum protocol interoperability, choosing Federated Access Manager is a good practice. For detailed installation and configuration information, see the *Sun Federated Access Manager Installation and Configuration Guide*.

Ideally, Service Provider and Identity Provider are deployed in two different domains. At minimum, the cookie domains should be different to ensure cookie validation consistency.

2 Install Federated Access Manager in the Service Provider Environment.

The Federated Access Manager in the Service Provider environment is the SAML2 protocols initiator. The SiteMinder policy agent can protect the enterprise application, but will still redirect to Federated Access Manager for single sign-on purposes.

▼ To Install and Configure SiteMinder in the Service Provider Domain

Before You Begin Before proceeding, be sure to read the general instructions in “[Installing SiteMinder](#)” on [page 99](#) and in “[Configuring SiteMinder After Installation](#)” on [page 100](#). The following steps provide additional installation information specific only to this use case.

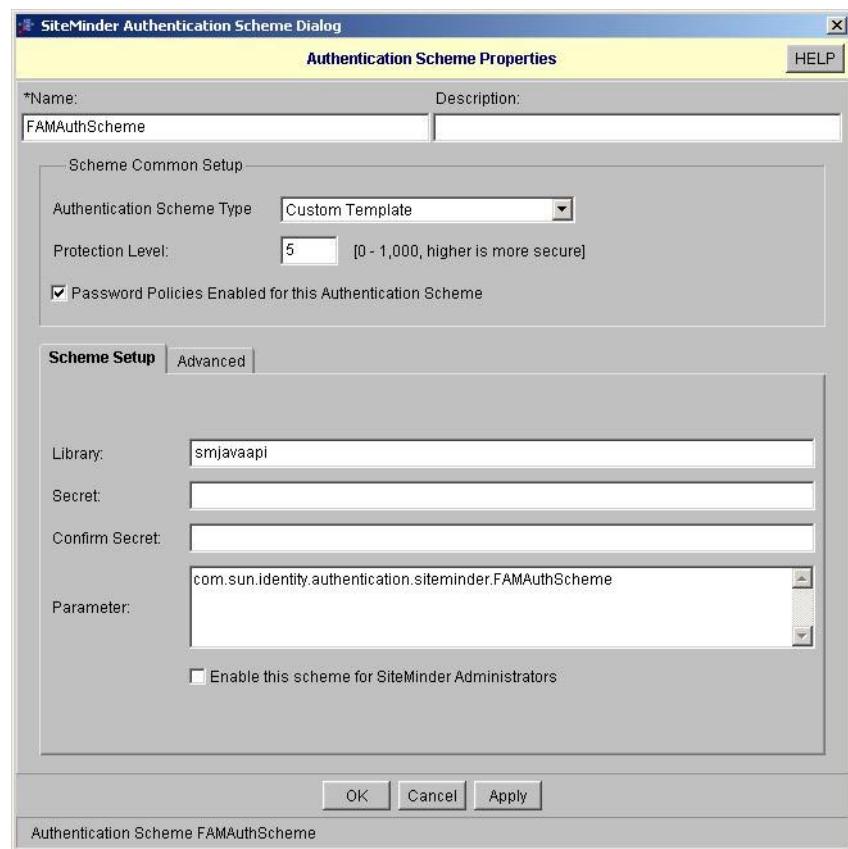
1 Install SiteMinder.

This is the domain that protects its enterprise applications using their SiteMinder agents. For the installation of SiteMinder and SiteMinder agents, see the CA SiteMinder product documentation.

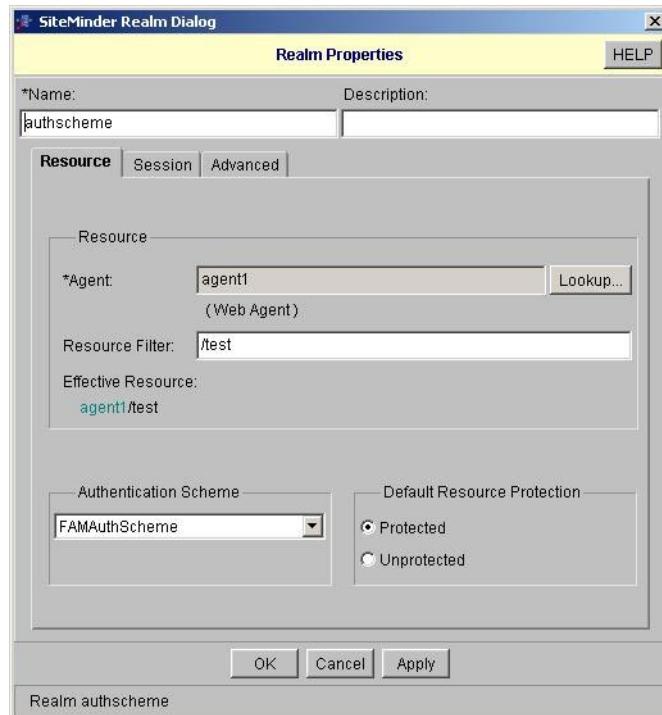
2 Create a custom authentication scheme.**a. Copy the compiled SiteMinder authentication scheme JAR files into the SiteMinder lib directory.**

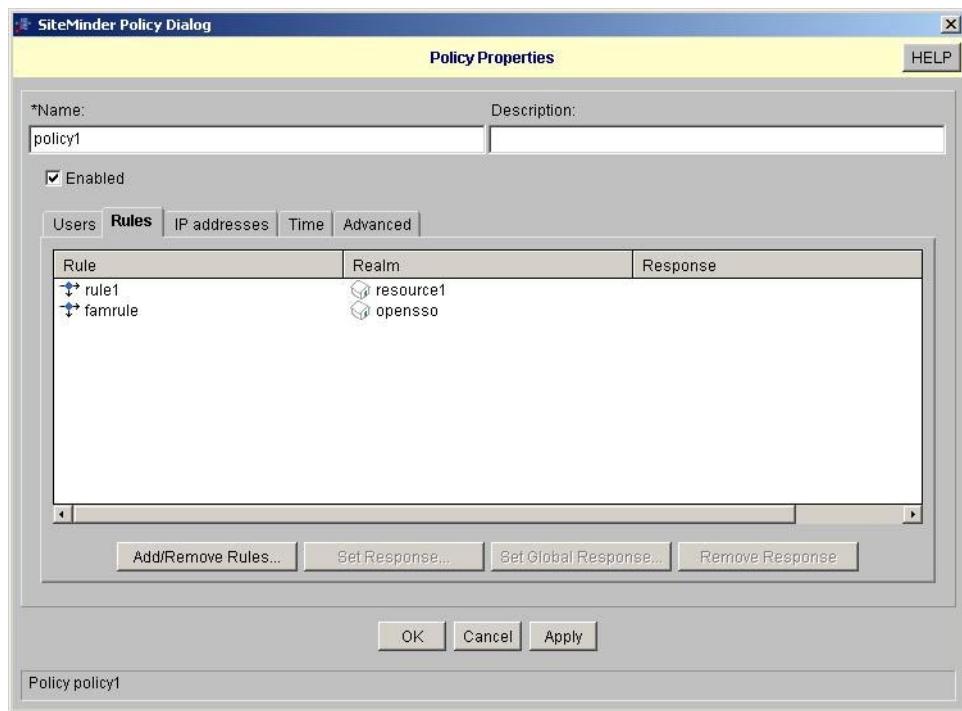
After you unzip the Federated Access Manager binary, the SiteMinder custom authentication module is located under the directory *unzip-directory/integrations/siteminder/*. The *README.html* provides steps for building a custom authentication module. The Federated Access Manager authentication module is a Java-based authentication scheme in SiteMinder. The *README.html* explains the steps for configuring the SiteMinder authentication scheme.

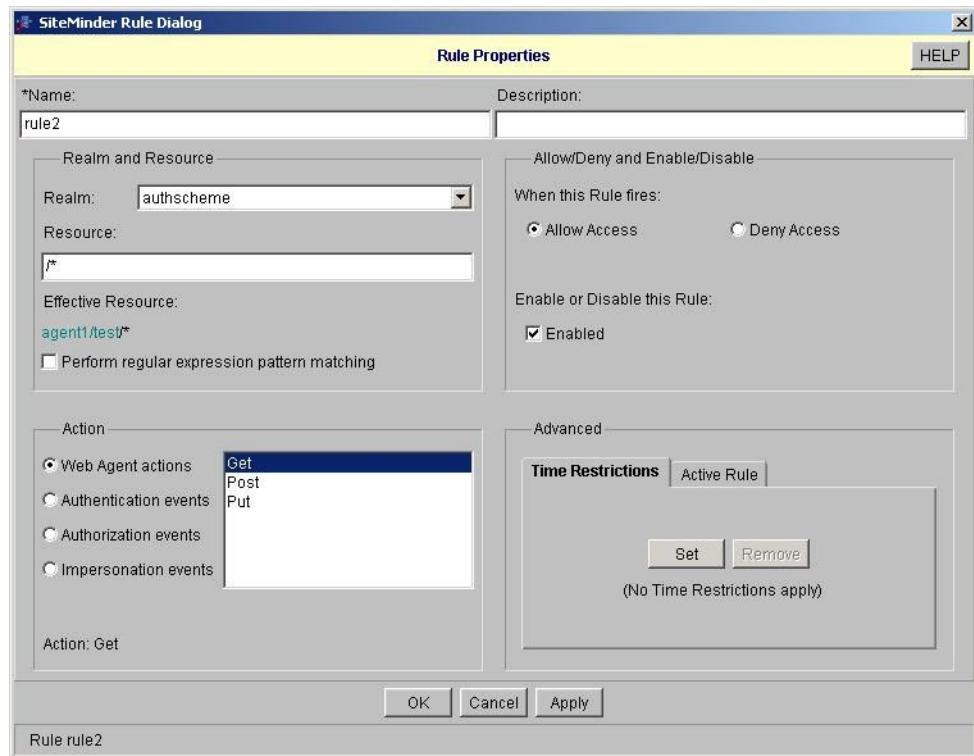
- b. In the SiteMinder console, click Authentication Scheme, and then click “Create Custom Authentication Scheme.”



3 Configure a resource and a policy to trigger the Federated Access Manager authentication module.







▼ To Configure the Federated Access Manager Identity Provider and Service Provider for SAML2 protocols

For these configurations, you must have the following:

- Identity Provider metadata
- Identity Provider extended metadata
- Service Provider metadata
- Service Provider extended metadata

In Identity Provider, import Identity Provider metadata and Identity Provider extended metadata as hosted metadata. Import Service Provider metadata and Service Provider extended metadata as remote entity metadata.

Before You Begin Before loading metadata, read through the following steps for the changes that you must make to the metadata. See the SAML2 samples for detailed instructions on how to setup SAML2. See the OpenSSO website for commands and syntax.

1 Edit the extended metadata XML element <EntityConfig>.

Change the hosted attribute from true to false.

2 Generate the metadata templates in both Identity Provider and Service Provider environments.

You can generate the metadata templates in one of two ways:

- Use the browser-based URL `http://host:port/opensso/famadm.jsp`
- Use the `famadm` command.

At the Identity Provider, where `idp_meta_alias` is `/idp`:

```
famadm create-metadata-templ -y idp_entity_id -u amadmin  
-f admin_password_file_name -m idp_standard_metadata -x idp_extended_metadata  
-i idp_meta_alias
```

At the Service Provider, where `sp_meta_alias` is `/sp`:

```
famadm create-metadata-templ -y sp_entity_id -u amadmin  
-f admin_password_file_name -msp_standard_metadata  
-x sp_extended_metadata -s sp_meta_alias
```

3 Customize the extended metadata at the Service Provider.

Add the Service Provider extended metadata as an attribute. This attribute is used by the SAML protocols to do any post-SSO Authentication process. In this example, the attribute is named `spAdapter`. In the architecture diagram, this is the SiteMinder Plug-In. The SiteMinder Plug-In uses the Federated Access Manager session to authenticate against SiteMinder and to establish the SiteMinder session. The Service Provider metadata must have the following attributes:

```
<Attribute name="spAdapter">  
    <Value>com.sun.identity.saml2.plugins.SMAdapter</Value>  
</Attribute>  
<Attribute name="spAdapterEnv">  
    <Value>AgentIP=192.18.120.65</Value>  
    <Value>AgentID=agent1</Value>  
    <Value>PolicyServerIPAddress=192.18.120.65</Value>  
    <Value>AuthorizationPort=44443</Value>  
    <Value>AuthenticationPort=44442</Value>  
    <Value>AccountingPort=44441</Value>  
    <Value>AgentHostName=HostName.example.com</Value>  
    <Value>ConnectionMinimum=2</Value>  
    <Value>ConnectionMaximum=20</Value>  
    <Value>ConnectionStep=2</Value>  
    <Value>RequestTimeout=60</Value>  
    <Value>FAMCookieName=iPlanetDirectoryPro</Value>  
    <Value>SMCookieName=SMSESSION</Value>  
    <Value>CookieDomain=.red.example.com</Value>  
    <Value>Resource=/test/index.html</Value>
```

```
<Value>SharedSecret={RC2}1r976MPOVq5JPpKzxFsXxIlut/YkgtUeklaceAoONCN  
mFJKDY+W8CkVpGY0to+x6apsIQAMPWLsgrm6NcdvyXv7K9Vf0vEALeW0y5BqlAhw  
fgKp4TbFRQspgv4w24Z0wsk57rwJ0N4kJdM9lsLRu5hGKXArRJNpF80vS/U53TZ  
vM/qE5I3DcC0WKY4lJBZh</Value>  
</Attribute>
```

4 Set the Service Provider extended metadata attribute transientUser to your anonymous user.

```
<Attribute name="transientUser">  
    <Value>anonymous</Value>  
</Attribute>
```

Also verify that the Federated Access Manager Service Provider is enabled for Anonymous authentication. See the Federated Access Manager product documentation for more information.

5 Add the Circle of Trust through the Federated Access Manager administration console.

Before loading, verify that the hosted attribute in the extended metadata has been changed to false.

6 Load the hosted metadata in both the Identity Provider and the Service Provider.

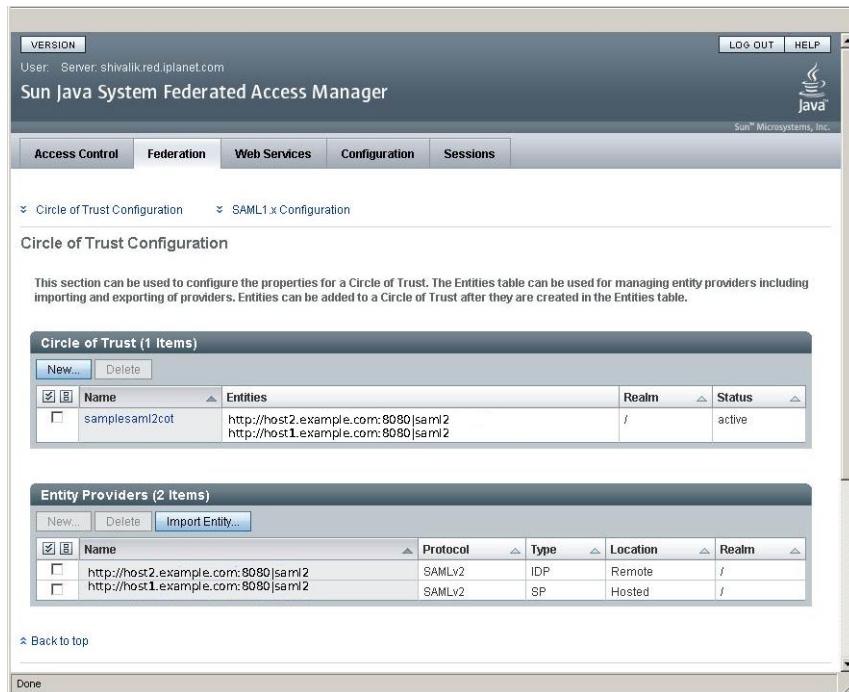
You can use the famadm command or the Federated Access Manager administration console.

7 Exchange the Service Provider metadata with the Identity Provider.

8 Exchange the Identity Provider metadata with the Service Provider metadata.

9 Load the metadata.

10 After successful metadata exchange, verify through Federated Access Manager administration console that metadata is properly configured.



11 Verify that Single Sign-On works properly.

Access the enterprise application protected by SiteMinder Service Provider Agent. This should redirect to the Federated Access Manager for authentication where the SAML2 SSO is initiated.

Sample Service Provider Interactions

This section provides sample output from the following interactions:

1. “1. Invocation of SAML SSO request” on page 134
2. “2. Redirection to Identity Provider” on page 135
3. “3. Redirection to Login” on page 136
4. “4. Redirection to Service Provider Assertion Consumer Service ” on page 139
5. “5. Check the SMSESSION Creation” on page 139

1. Invocation of SAML SSO request

```
http://HostName.example.com:8080/opensso/saml2/jsp/
spSSOInit.jsp?metaAlias=/sp&idpEntityID=
http://ide-13.red.example.com:8080/opensso&NameIDFormat=transient
```

```
GET /opensso/saml2/jsp/spSSOInit.jsp?metaAlias=/sp&idpEntityID=
```

```

http://ide-13.red.example.com:8080/opensso&NameIDFormat=transient HTTP/1.1
Host: HostName.example.com:8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: JSESSIONID=5fa8300161a1d5dc746ad8f9fb31

```

2. Redirection to Identity Provider

```

HTTP/1.x 302 Moved Temporarily
X-Powered-By: JService Provider/2.1
Server: Sun Java System Application Server 9.1
Location: http://ide-13.red.example.com:8080/opensso/SSORedirect/
metaAlias/idp?SAMLRequest=nVRfb9owEH%2Fvp4j8DnEsaMECJAaahtRtD0ge9
maSy7Dm2JnvQtm3rx0oYmqFVF7P57vfP3uEstK1mDa0Myv42wBSFB0qbVC0J2PWOCO
sRIXCyApQUC7W06%2BPIu1yUTtLNrea3S3mY4bpYJvxLNsW5Rb60089DNNhWQ4l7yV
8cJ8kUAzT7J5nKYt%2BgkNlzZj5MSxaIDawMEjSkC9xPujwtMN7m2Qoej3Rf%2FjFo
rmHpoyk9ta0qBZxrAroJFnXqdFvtZYgqJvbSgz4gMe2BoNo4%2FX6%2BwoK5SCnuAK
SU60k%2Bps1iz5bl0NLfcxKqRECKqVEVhs4V5Ynjp%2BUKZT5fV2Q7bEJxZfNZtmZO
lKlzIlFU0RwAfrMGmwqcgTwe5XD0%2BrxTAZ3ai%2B1%2Bn0dzuuACy5Ys8ndKNglWi
HdhYHX4cpXWGzyERCj%2BGLzaXutvvnxi%2FnSapX%2FuyVDwY5K0vXuUFFp2xbBTl
pUIHxCq%2BXYf%2BPxoMvFbiPqeoN0to%2BzxxI8s6Ta4BNjiz%2F53Ume3orULTx8a
YQHOgW0jNb1dIpDKmGQwjL5Gjl5eCZ9k6toLzF2KttucjDaF80sX%2B2rghx908Fik3
QtraOTm6%2Fh%2Bes0byteLHit9%2FL5AU%3D
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 0
Date: Mon, 04 Feb 2008 19:44:57 GMT
-----
http://ide-13.red.example.com:8080/opensso/SSORedirect/metaAlias/
idp?SAMLRequest=nVRfb9owEH%2Fvp4j8DnEsaMECJAaahtRtD0ge9maSy7Dm2Jn
vQtm3rx0oYmqFVF7P57vfP3uEstK1mDa0Myv42wBSFB0qbVC0J2PWOCOsRIXCyApQ
UC7W06%2BPIu1yUTtLNrea3S3mY4bpYJvxLNsW5Rb60089DNNhWQ4l7yV8cJ8kUAz
T7J5nKYt%2BgkNlzZj5MSxaIDawMEjSkC9xPujwtMN7m2Qoej3Rf%2FjFormHpoyk
9ta0qBZxrAroJFnXqdFvtZYgqJvbSgz4gMe2BoNo4%2FX6%2BwoK5SCnuAKSU60k%
2Bps1iz5bl0NLfcxKqRECKqVEVhs4V5Ynjp%2BUKZT5fV2Q7bEJxZfNZtmZOlkzI
lFU0RwAfrMGmwqcgTwe5XD0%2BrxTAZ3ai%2B1%2Bn0dzuuACy5Ys8ndKNglWiHdh
YHX4cpXWGzyERCj%2BGLzaXutvvnxi%2FnSapX%2FuyVDwY5K0vXuUFFp2xbBTlp
pUIHxCq%2BXYf%2BPxoMvFbiPqeoN0to%2BzxxI8s6Ta4BNjiz%2F53Ume3orULTx8a
aYQHOgW0jNb1dIpDKmGQwjL5Gjl5eCZ9k6toLzF2KttucjDaF80sX%2B2rghx908F
ik3QtraOTm6%2Fh%2Bes0byteLHit9%2FL5AU%3D

```

```
GET /opensso/SSORedirect/metaAlias/idp?SAMLRequest=nVRfb9owEH%2Fvp
4j8DnESaMECJAahhRtD0ge9maSy7Dm2JnvQt3rx0oYmqFVF7P57vfP3uEstK1mDa
0Myv42wBSFB0qbVC0J2PWOCosRIXCyApQUC7W06%2BPIu1yUTtLNrea3S3mY4bpYJv
xLNsW5Rb60089DNNhWQ4l7yV8cJ8kUAzT7J5nKYt%2BgkNlzZj5MSxaIDawMEjSkC9
xPuwtMN7m2Qoej3Rf%2FjFormHpoyk9ta0qBzxrAroJFnXQdFVtZYGqJvbSgz4gMe
2BoNo4%2FX6%2BwoK5SCnuAKSU60k%2Bps1iz5bl0NLfcxKqRECKqVEVHs4V5Ynjp%
2BUKZT5fV2Q7bEJxZfNZtmZ0lKlzIlFU0RwAfrMGmwqcGtwe5XD0%2BrxTAZ3ai%2B
1%2Bn0duuAcY5Ys8ndKNglWiHdhYHX4cpXWGzyERCj%2BGLZaXUtvvnxi%2FnSapX
2FuyVDwY5K0vXuUFFp2xbBTlpUIHxCq%2BXYf%2BPxoMvFbiPqeon0to%2BzxxI8s6
Ta4BNjiz%2F53Um3orULTx8aYQHOgW0jNb1dIpDKmGwjL5Gjl5eCZ9k6toLzF2Ktt
ucjDaF8OsX%2B2rghx908Fik3Qtra0Tm6%2Fh%2Bes0btyeLHit9%2FL5AU%3D HTTP/1.1
Host: ide-13.red.example.com:8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

3. Redirection to Login

```
HTTP/1.x 302 Moved Temporarily
X-Powered-By: JService Provider/2.1
Server: Sun Java System Application Server 9.1
Set-Cookie: JSESSIONID=5f9f32d1896460b979b16ac14fb3; Path=/opensso
Location: http://ide-13.red.example.com:8080/opensso/UI/Login?realm=
&goto=http%3A%2F%2Fide-13.red.example.com%3A8080%2Fopensso%
2FSSORedirect%2FmetaAlias%2Fidp%3FReqID%3Ds28b3033bdfbe5e547929ff9a
04108611ed9236032
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 0
Date: Mon, 04 Feb 2008 19:43:58 GMT
-----
http://ide-13.red.example.com:8080/opensso/UI/Login?realm=&goto=
http%3A%2F%2Fide-13.red.example.com%3A8080%2Fopensso%2FSSORedirect%
2FmetaAlias%2Fidp%3FReqID%3Ds28b3033bdfbe5e547929ff9a04108611ed9236032
```

```
GET /opensso/UI/Login?realm=/&goto=http%3A%2F%2Fide-13.red.example.com%
3A8080%2Fopensso%2FSSORedirect%2FmetaAlias%2Fidp%3FReqID%3Ds28b3033bdfb
e5e547929ff9a04108611ed9236032 HTTP/1.1
Host: ide-13.red.example.com:8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
Gecko/20071127 Firefox/2.0.0.11
```

```

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: JSESSIONID=5f9f32d1896460b979b16ac14fb3

HTTP/1.x 200 OK
X-Powered-By: JService Provider/2.1
Server: Sun Java System Application Server 9.1
Cache-Control: private
Pragma: no-cache
Expires: 0
X-DSAMEVersion: 8.0 (2007-November-29 01:17)
AM_CLIENT_TYPE: genericHTML
Set-Cookie: AMAuthCookie=AQIC5wM2LY4Sfcz0j691d2eiNkQCzmce014vekWbCSzRU/E=@AAJTSQACMDE=#; Domain=ide-13.red.example.com; Path=/
Set-Cookie: amlbcookie=01; Domain=ide-13.red.example.com; Path=/
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Mon, 04 Feb 2008 19:43:58 GMT
-----
```

```

http://ide-13.red.example.com:8080/opensso/UI/Login?AMAuthCookie=
AQIC5wM2LY4Sfcz0j691d2eiNkQCzmce014vekWbCSzRU%2FE%3D%40AAJTSQACMDE%3D%23

POST /opensso/UI/Login?AMAuthCookie=AQIC5wM2LY4Sfcz0j691d2eiNkQCzmce014vekWbCSzRU%2FE%3D%40AAJTSQACMDE%3D%23 HTTP/1.1
Host: ide-13.red.example.com:8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://ide-13.red.example.com:8080/opensso/UI/Login?realm=/&goto=http%3A%2F%2Fide-13.red.example.com%3A8080%2Fopensso%2FSSORedirect%2FmetaAlias%2Fidp%3FReqID%3Ds28b3033bdfbe5e547929ff9a04108611ed9236032
Cookie: JSESSIONID=5f9f32d1896460b979b16ac14fb3; AMAuthCookie=AQIC5wM2LY4Sfcz0j691d2eiNkQCzmce014vekWbCSzRU/E=@AAJTSQACMDE=#; amlbcookie=01
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 254
IDToken0=&IDToken1=amadmin&IDToken2=admin123&IDButton=Log+In&goto=
aHR0cDovL2lkZS0xMy5yZWQuaXBsYW5ldC5jb2060DA4MC9vcGVuc3NvL1NTT1JlZGlyZWN0L2
1ldGFBBgGlhcypHZA%2FUUmVxSUQ9czI4YjMwMzNiZGz1ZTVlNTQ3OTI5ZmY5YTA0MTA4NjExZW
Q5MjM2MDMy&encoded=true&gx_charset=UTF-8
HTTP/1.x 302 Moved Temporarily
X-Powered-By: Servlet/2.5
Server: Sun Java System Application Server 9.1
Cache-Control: private
Pragma: no-cache
Expires: 0
X-DSAMEVersion: 8.0 (2007-November-29 01:17)
AM_CLIENT_TYPE: genericHTML
X-AuthErrorCode: 0
Set-Cookie: iPlanetDirectoryPro=AQIC5wM2LY4Sfcz0j691d2eiNkQCzmce014vekWbCSzRU/
E=@AJTSQACMDE=#; Domain=ide-13.red.example.com; Path=/
Set-Cookie: AMAuthCookie=LOGOUT; Domain=ide-13.red.example.com;
Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
Location: http://ide-13.red.example.com:8080/opensso/SSORedirect/
metaAlias/idp?ReqID=s28b3033bdfbe5e547929ff9a04108611ed9236032
Content-Type: text/html; charset=iso-8859-1
Content-Length: 0
Date: Mon, 04 Feb 2008 19:44:05 GMT
-----
http://ide-13.red.example.com:8080/opensso/SSORedirect/metaAlias/
idp?ReqID=s28b3033bdfbe5e547929ff9a04108611ed9236032

GET /opensso/SSORedirect/metaAlias/idp?ReqID=s28b3033bdfbe5e54792
9ff9a04108611ed9236032 HTTP/1.1
Host: ide-13.red.example.com:8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://ide-13.red.example.com:8080/opensso/UI/Login?realm=
&goto=http%3A%2F%2Fide-13.red.example.com%3A8080%2Fopensso%2FSSORedirect%
2FmetaAlias%2Fidp%3FReqID%3Ds28b3033bdfbe5e547929ff9a04108611ed9236032
Cookie: JSESSIONID=5f9f32d1896460b979b16ac14fb3; amlbcookie=01;
iPlanetDirectoryPro=AQIC5wM2LY4Sfcz0j691d2eiNkQCzmce014vekWbCSzRU/E=@AJTSQACMDE=#
HTTP/1.x 302 Moved Temporarily
X-Powered-By: JService Provider/2.1
```

Server: Sun Java System Application Server 9.1
 Location: http://HostName.example.com:8080/opensso/Consumer/metaAlias/
 sp?SAMLart=AAQAAI4sWYpfoDDYJrHzsMnG%2BjyNM94p5ejn49a%2BnZ0s3yLY7knQ6tKLMD%3D
 Content-Type: text/html; charset=ISO-8859-1
 Content-Length: 0
 Date: Mon, 04 Feb 2008 19:44:05 GMT

4. Redirection to Service Provider Assertion Consumer Service

<http://HostName.example.com:8080/opensso/Consumer/metaAlias/sp?SAMLart=AAQAAI4sWYpfoDDYJrHzsMnG%2BjyNM94p5ejn49a%2BnZ0s3yLY7knQ6tKLMD%3D>

GET /opensso/Consumer/metaAlias/sp?SAMLart=AAQAAI4sWYpfoDDYJrHzsMnG%
 2BjyNM94p5ejn49a%2BnZ0s3yLY7knQ6tKLMD%3D HTTP/1.1
 Host: HostName.example.com:8080
 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.11)
 Gecko/20071127 Firefox/2.0.0.11
 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
 text/plain;q=0.8,image/png,*/*;q=0.5
 Accept-Language: en-us,en;q=0.5
 Accept-Encoding: gzip,deflate
 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
 Keep-Alive: 300
 Connection: keep-alive
 Referer: http://ide-13.red.example.com:8080/opensso/UI/Login?realm=%
 &goto=http%3A%2F%2Fide-13.red.example.com%3A8080%2Fopensso%2FSSORedirect%
 2FmetaAlias%2Fidp%3FReqID%3Ds28b3033bdfbe5e547929ff9a04108611ed9236032
 Cookie: JSESSIONID=5fa8300161a1d5dc746ad8f9fb31

5. Check the SMSESSION Creation

HTTP/1.x 200 OK
 X-Powered-By: JService Provider/2.1
 Server: Sun Java System Application Server 9.1
 Set-Cookie: iPlanetDirectoryPro=AQIC5wM2LY4SfcwFsRqmpq0e6m+iL+tjmqYhTDsKeAbB4Eg=@AAJTSQACMDE=#; Domain=HostName.example.com;
 Path=/Set-Cookie: SMSESSION=jnNjdOyhPMa6A7FKeD0tCgHyq3yt8Tsvtmj6G4NjbP05ftAMggw+
 hqolfo32FJ8i0nggFoZ19qXVAJyqf0DvMqhM+X0oUVw3P3R83sBAT4uKtUaib70xyTSi8W5pBI+hLexr
 NczdpVWN9vCGDU97uBLJgpI8L9aeSNBgCSwo+gluvd1I72KGyFVgMLkIkfLMJhctpz+zKvt252yEf50h
 QZLGhzT/DzNqBc+142eek5VwMzxABLhwuEQ1jI1VAGOYAeyQpSmikgNfWphDSV3X36L3+ZQqHZmzCwj
 b8QK5rBZnMdGuZKCYc9U6N8VJ1Ft5zwi/lotOU198apSU2bI5nQzWnGjpz60Dxc6Ycy83bj0qby/ZYHrl
 30Lv2wJ0RtEN8FPYFjbHLGg=; Domain=.red.example.com
 Content-Type: text/html; charset=ISO-8859-1
 Transfer-Encoding: chunked
 Date: Mon, 04 Feb 2008 19:45:04 GMT

Integrating Oracle Access Manager

Oracle Access Manager (previously known as Oblix NetPoint and Oracle COREid) is an enterprise single sign-on product with many of the same features as Sun Federation Access Manager and CA SiteMinder (previously known as Netegrity SiteMinder). Oracle Access Manager is usually used for both single sign-on and delegated administration. Many companies have an existing Oracle Access Manager deployed to protect both internal and external applications. This chapter describes options for integrating Oracle Access Manager with Sun Federation Access Manager. The chapter also provides instructions for configuring end-to-end Oracle Access Manager single sign-on using Sun Federation Access Manager.

About Oracle Access Manager

Oracle has two solutions for web-based single sign-on. One solution is to use the legacy Oracle single sign-on product which is integrated in the Oracle Application Server. Another solution is to use the Oracle Access Manager product, previously known as Oblix Access, with Identity Server. The following major components comprise the Oracle Access System:

Oracle Identity Server	Provides user management and delegated administration functionality and workflows.
Oracle Policy Manager	Provides a web-based interface where administrators can create and manage access policies. The Policy Manager communicates with the directory server to write policy data, and communicates with the Access Server over the Oracle Access Protocol (OAP) to update the Access Server when certain policy modifications are made.
Oracle Access Server	Provides centralized authentication, authorization, and auditing to enable single sign-on and secure access control across enterprise resources.
Web Pass	An Oracle Access Manager web server plug-in (NSAPI filter). Web Pass passes information back and forth between a web server and the

Identity Server. Depending upon its configuration, the Identity Server processes a request as either an XML or HTML file.

WebGate	A web server plug-in access client analogous to Sun Access Manager Policy Agent. WebGate intercepts HTTP requests for Web resources and forwards them to the Access Server for authentication and authorization.
---------	--

Overview of a Typical Oracle Access Manager Session

The Access Server generates a session token with a URL that contains the `ObSSOCookie`. When the cookie is generated, part of the cookie is used as an encrypted session token. The encrypted session token contains the following:

- Distinguished name (DN) of the user
- Level of the authentication scheme
- IP address of the client to which the cookie was issued
- Time the cookie was originally issued
- Time the cookie was last updated

If the user has not been idle, the cookie is updated at a fixed interval to prevent the session from logout. The update interval is 1/4th of idle the session timeout parameter.

Unencrypted `ObSSOCookie` data includes the following:

- Cookie expiration time
- Domain in which the cookie is valid
- Optional flag that determines if the cookie can only be sent over SSL

The `ObSSOCookie` is a secure mechanism for user authentication. When the Access System generates the cookie, an MD-5 hash is taken of the session token. When `ObSSOCookie` is used to authenticate a user, the MD-5 hash is compared with the original cookie contents to be sure no one has tampered with the cookie. MD-5 is a one-way hash, so it cannot be unencrypted. The Access Server does the comparison by hashing the session token again and comparing the output with the hash of the token already present in the Oracle Access Server cookie. If the two hashes do not match, the cookie is corrupt. The system relies on the fact that if someone tampers with the session token, the hashes will not match.

Understanding the Oracle Access Manager Use Cases

The following uses cases illustrate common Oracle Access Manager process flows:

- Simple Single Sign-On
- Federated Single Sign-On in a Service Provider Environment
- Federated Single Sign-On in an Identity Provider Environment

Single logout for any of these use cases can be implemented in many ways. The logout for federation use cases must have a link in the partner portal for the following URL:

```
http:<sphost>:<spport>/opensso/saml2/jsp/spSingleLogoutInit.jsp?metaAlias=<metaalias>&idpEntityID=<idp entityid>&RelayState=<integrated product logout url>
```

Single logout can also be achieved using Identity Provider-initiated single logout.

Simple Single Sign-On Use Case

Simple single sign-on integration is useful when an Oracle Access Manager instance is already deployed and configured to protect intranet enterprise applications. Additionally, Federation Access Manager is deployed to protect the same intranet applications by honoring the user session obtained by Oracle Access Manager. In the following illustration, both Federated Access Manager and Oracle Access Manager share the same user repository for user profile verification. Federated Access Manager can also be configured to use the Ignore Profile option if it relies on the Oracle Access Manager session for attributes.

The following figure illustrates architecture in the simple single sign-on use case.

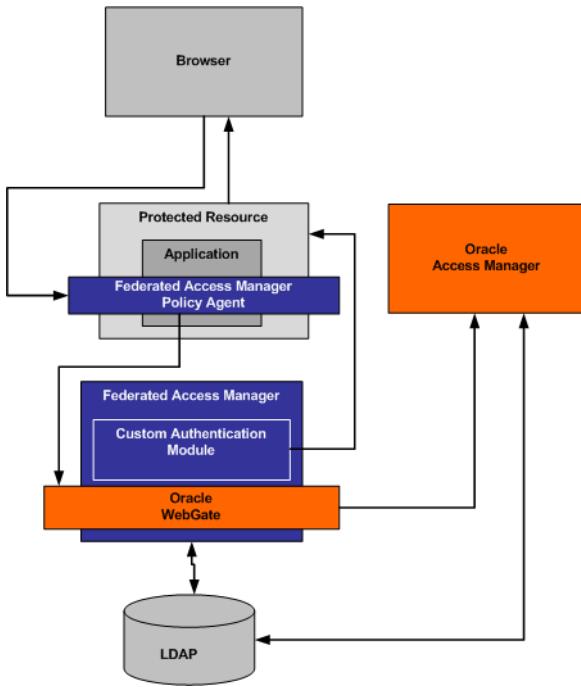


FIGURE 3–1 Simple Oracle Access Manager Single Sign-On

The following figure illustrates the process flow among components in the Identity Provider environment and Service Provider environment.

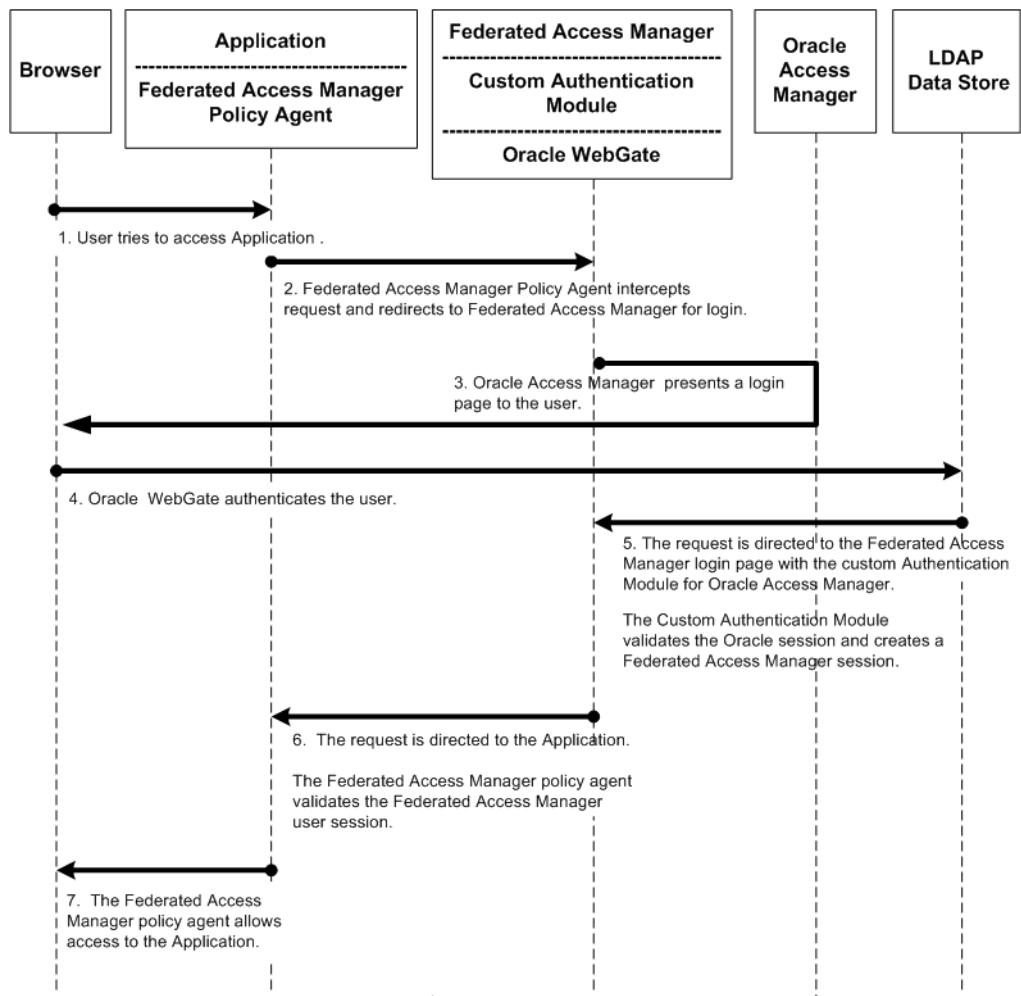


FIGURE 3–2 Process Flow for Simple Oracle Access Manager Single Sign-On

Federated Single Sign-On Use Cases

The SAML, ID-FF, and WS-Federation protocols provide cross-domain single sign-on among multiple trusted business entities. These protocols are also used in Identity Federation. Identity Federation involves an Identity Provider, also known as an authentication provider, and a Service Provider where the user authentication session at the Identity Provider is consumed. The following are common use cases in which Oracle Access Manager is enabled for federation protocols:

- Enabling Oracle Access Manager for federation protocols in a Service Provider environment

- Enabling Oracle Access Manager for federation protocols in an Identity Provider environment

The deployment examples in this chapter are built upon simple single sign-on integration. You must set up single sign-on before enabling federation. For more information about setting up simple single sign-on, see the *Sun Federated Access Manager Installation and Configuration Guide*. After setting up simple single sign-on, you can enable Oracle Access Manager for Federation in either the Identity Provider environment or in the Service Provider environment.

In the following examples, both Identity Provider and Service Provider are configured for transient federation. In most use cases, bulk federation is configured between the Identity Provider and Service Provider.

In transient federation, users exist only in the Identity Provider environment. The Service Provider honors the user authentication at the Identity Provider, and then creates an anonymous session. The anonymous session enables the Service Provider applications, protected by single sign-on, to be accessed. During SAML interactions, there is a possibility of exchanging user attribute information back to the Service Provider for authorization and other purposes. But that scenario is beyond the scope of this document.

Using Federated Access Manager to Enable Oracle Federation in an Identity Provider Environment

In this example, Oracle Access Manager is the authentication provider in an Identity Provider environment and protects some of the intranet applications. The Federation Access Manager in this deployment resolves the single sign-on issues among enterprise applications in partner environments while Oracle Access Manager provides authentication.

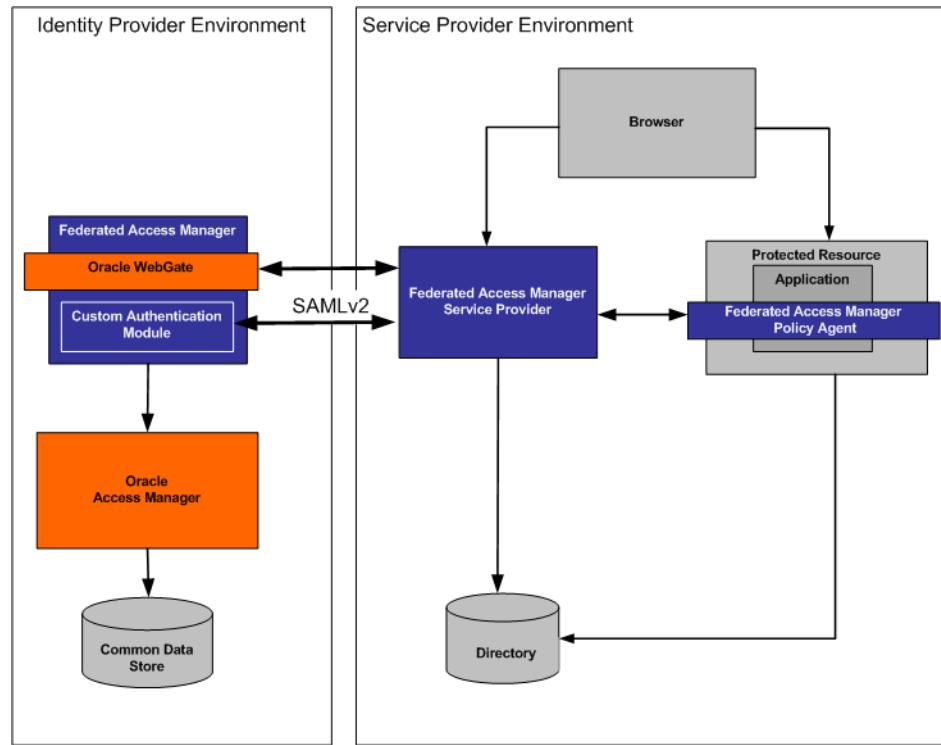


FIGURE 3–3 Oracle Access Manager Federation in an Identity Provider Environment

The following two figures illustrate the process flow among components in the Identity Provider environment and Service Provider environment.

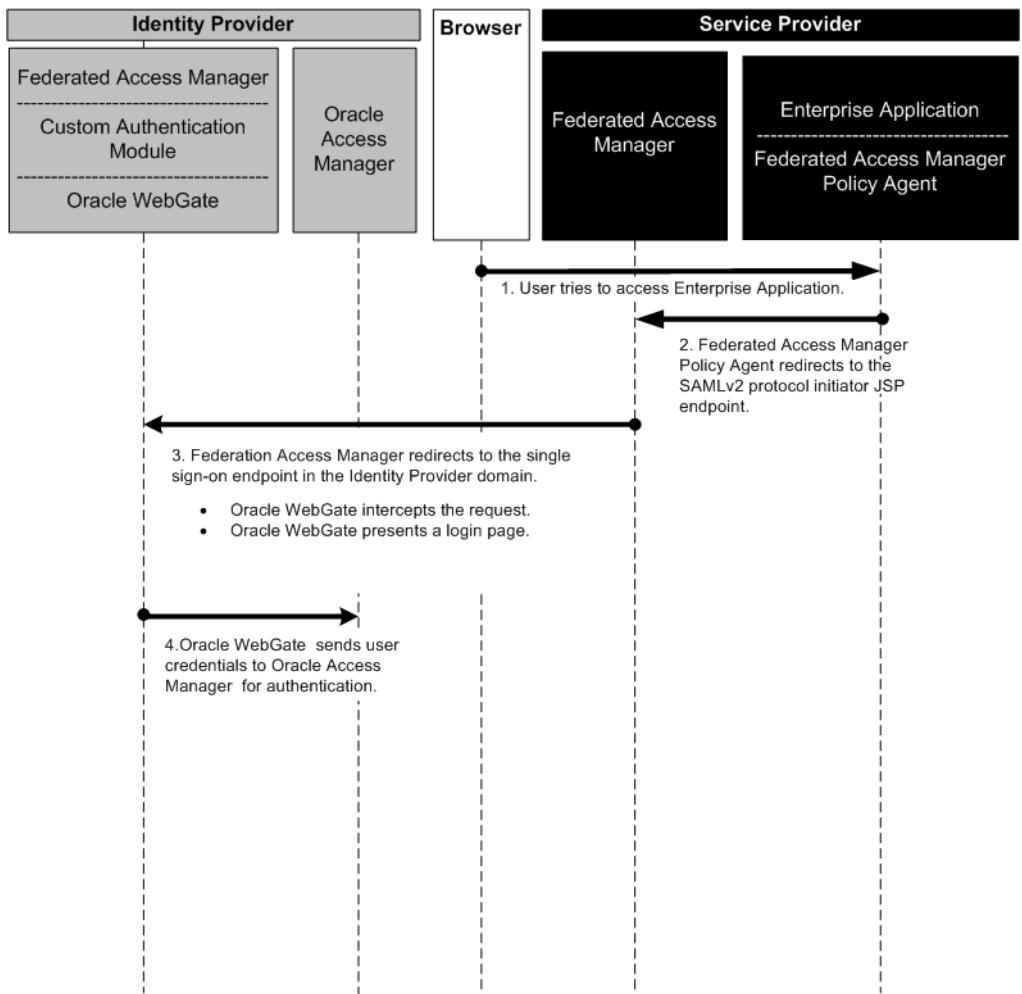


FIGURE 3–4 Process flow for Oracle Access Manager Federation in an Identity Provider Environment

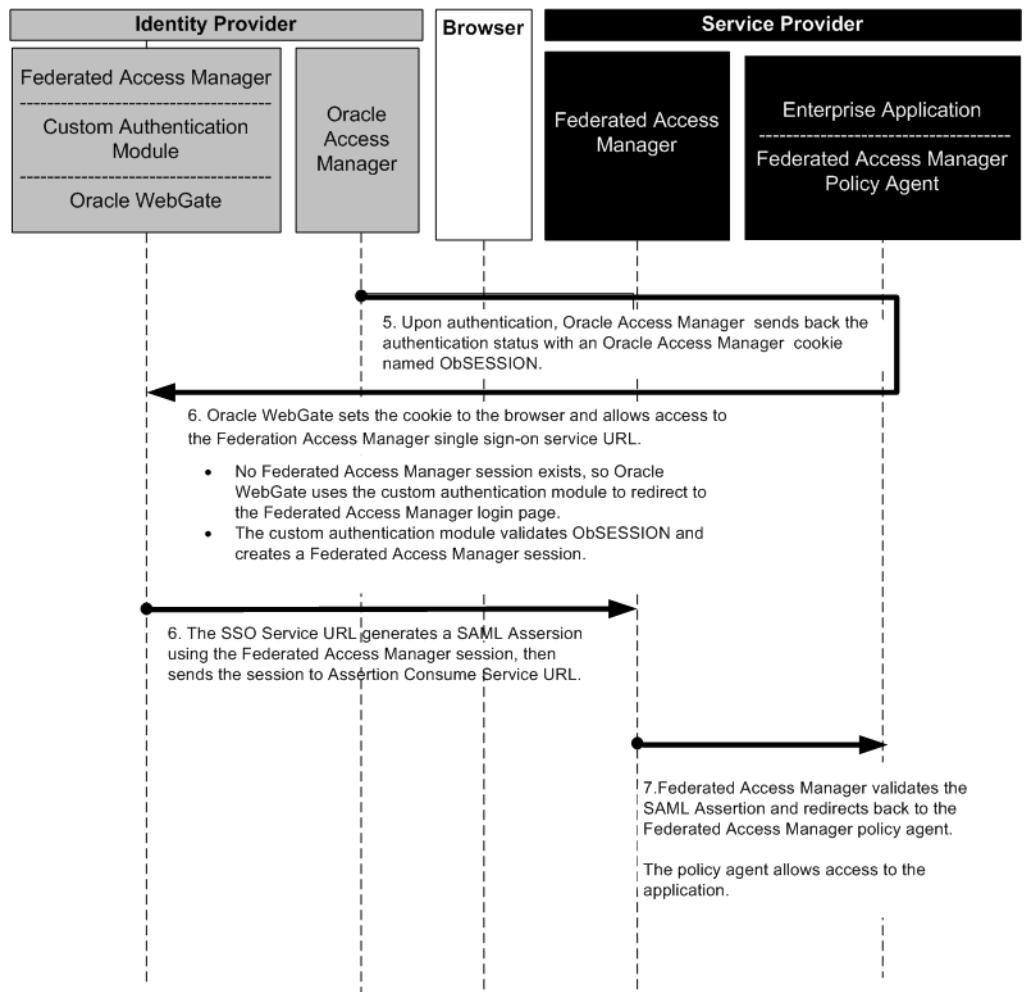


FIGURE 3–5 Process flow for Oracle Access Manager Federation in an Identity Provider Environment (continued)

Using Federated Access Manager to Enable Oracle Federation in a Service Provider Environment

In this deployment, Oracle Access Manager is installed and configured in Service Provider Environment to protect legacy applications.

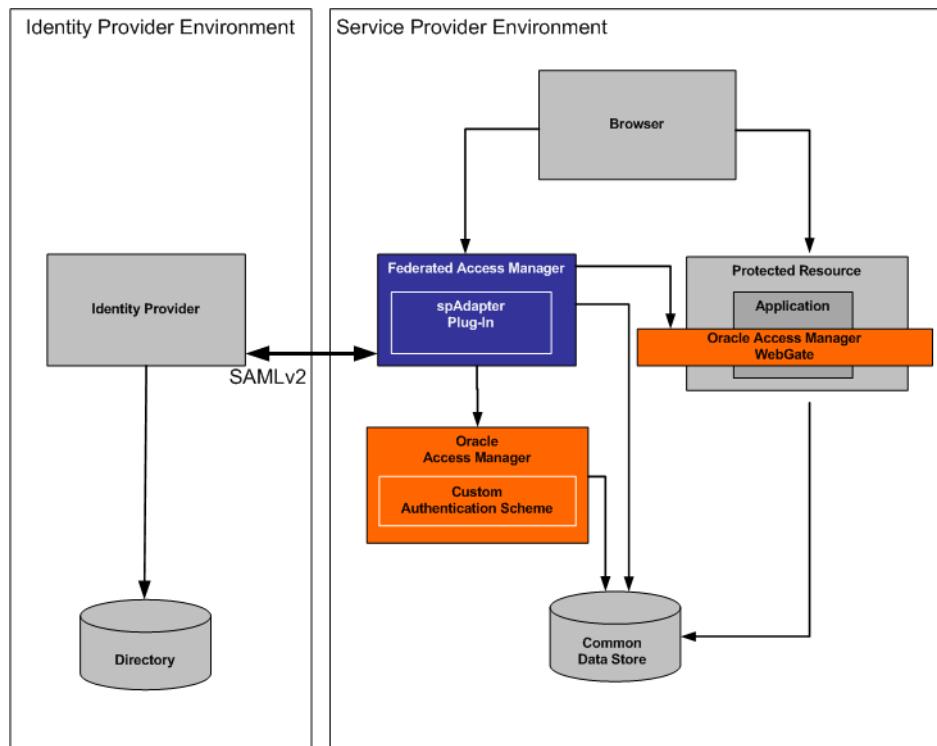


FIGURE 3–6 Oracle Access Manager Federation in a Service Provider Environment

The following two figures illustrate the process flow among components in the Identity Provider environment and Service Provider environment.

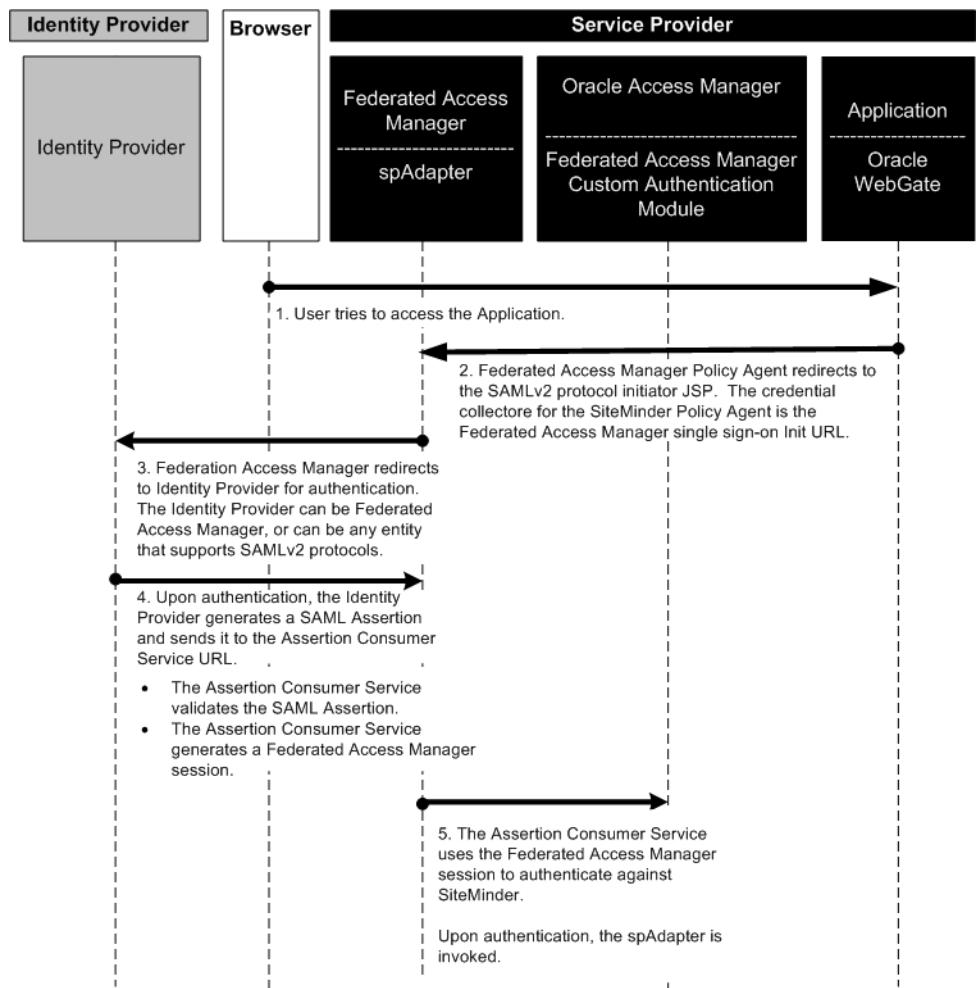


FIGURE 3-7 Process Flow for Oracle Access Manager Federation in a Service Provider Environment

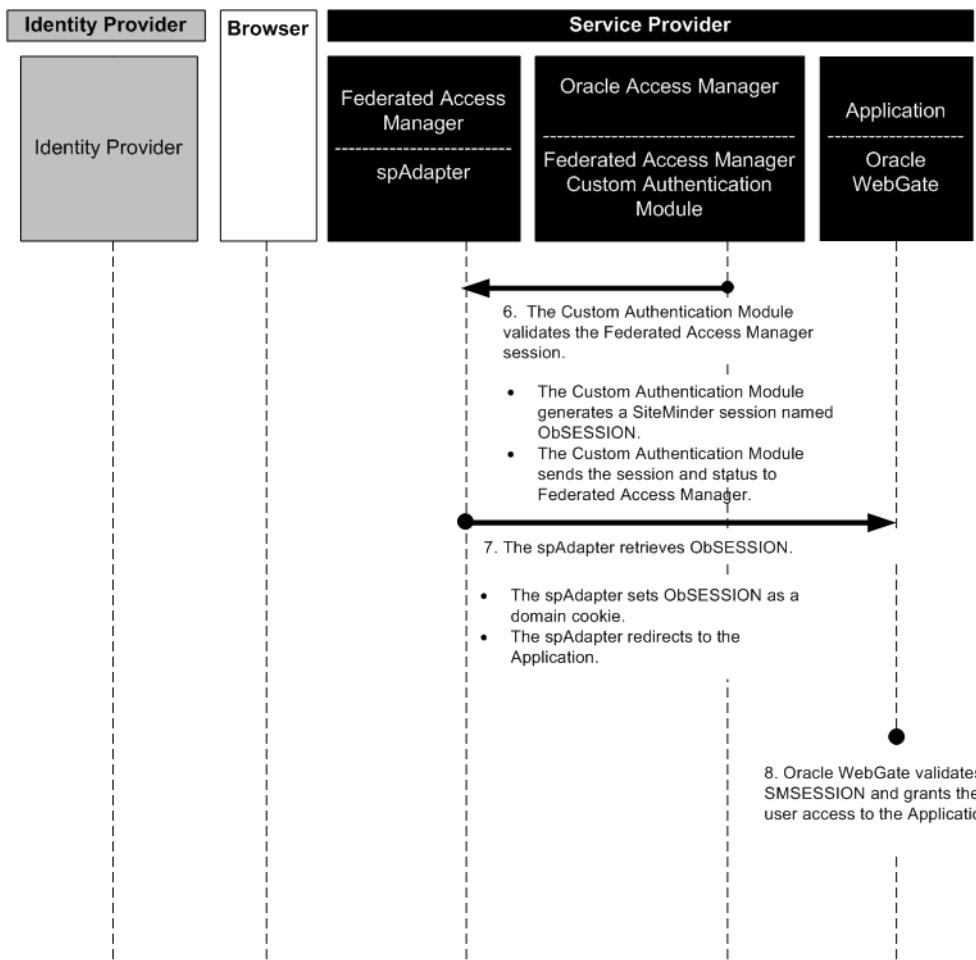


FIGURE 3-8 Process Flow for Oracle Access Manager Federation in a Service Provider Environment
(continued)

Installing and Configuring Oracle Access Manager

To enable the legacy Oracle Access Manager single sign-on applications for SAML 2 federation protocols using Federation Access Manager 8.0, follow these steps:

1. [“To Install Oracle Access Manager and Oracle Access Manager Web Policy Agent” on page 153](#)
2. [“To Configure Oracle Access Manager” on page 154](#)

▼ To Install Oracle Access Manager and Oracle Access Manager Web Policy Agent

1 Install Oracle Identity Server, and then install the Oracle Access Server component.

Obtain all required Oracle Access Manager components before you begin installation procedures. See *Oracle Access Manager Installation Guide* for detailed installation instructions.

For the examples in this document, Solaris-based installation was conducted. The system was tested with Sun Web Server 6.1 SP5 as the Oracle Administration plug-in interface, and Sun Directory Server 6.3 as the user data and configuration repository.

2 After the successful installation, access the administration console.

Go to the URL `http://host:port/access/oblix` and log in using the following credentials:

User Name: oadmin

Password: password

The administrative interface for managing core access server components, policy manager, and identity console is displayed.

3 Install Oracle WebGate.

See the section in the *Oracle Access Manager Installation Guide*.

▼ To Configure Oracle Access Manager

See the [Oracle Access Manager Installation Guide](#) for detailed configuration instructions. For the examples in this document, the Oracle Access and Policy Servers are tested using the configurations described below.

1 Create an Access Server Configuration named access1.

The screenshot shows the Oracle Access Administration interface. The left sidebar has a tree view with the following items:- Access Server Clusters
- AccessGate Configuration
- Add New Access Gate
- **Access Server Configuration** (selected)
- Authentication Management
- Authorization Management
- User Access Configuration
- Common Information Configuration
- Host Identifiers
The main panel title is "Details for Access Server". It displays the following configuration settings:| Name | access1 |
| --- | --- |
| Hostname | host.example.com |
| Port | 9081 |
| Debug | On |
| Debug File Name | /export/oblix-access-debug/debug |
| Transport Security | Open |
| Maximum Client Session Time (hours) | 24 |
| Number of Threads | 60 |
| Access Management Service | On |
| Audit to Database (on/off) | |
| Audit to Database (on/off) | Off |
| Audit to File (on/off) | |
| Audit File Name | |
| Audit File Size (bytes) | 0 |
| Buffer Size (bytes) | 512000 |
| File Rotation Interval (seconds) | 0 |
| Engine Configuration Refresh Period (seconds) | 14400 |
| URL Prefix Reload Period (seconds) | 7200 |
| Password Policy Reload Period (seconds) | 7200 |
| Maximum Elements in User Cache | |
| User Cache Timeout (seconds) | 1800 |
| Maximum Elements in Policy Cache | 10000 |
| Policy Cache Timeout (seconds) | 7200 |
| SNMP State | |
| SNMP Agent Registration Port | Off |
| Session Token Cache | |
| Session Token Cache | Enabled |
| Maximum Elements in Session Token Cache | 10000 |

At the bottom of the panel are buttons: Modify, View Associated AccessGates, Back, Associate DB Profile(s).

2 Create access gate configuration named webgate1.

The screenshot shows the Oracle Access Administration interface. The left sidebar has a tree view with nodes like Access Server Clusters, AccessGate Configuration (which is selected), Add New Access Gate, Access Server Configuration, Authentication Management, Authorization Management, User Access Configuration, Common Information Configuration, and Host Identifiers. The main panel is titled "Details for AccessGate" and shows the configuration for "AccessGate Name: webgate1". It includes fields for State (Enabled), Hostname (host.example.com), Port (9082), Access Gate Password (<Not Displayed>), Debug (Off), Maximum user session time (seconds) (3600), Idle Session Time (seconds) (1800), Maximum Connections (1), Transport Security (Open), IPValidation (On), IPValidationException, Maximum Client Session Time (hours) (24), Failover threshold (1), Access server timeout threshold, Sleep For (seconds) (60), Maximum elements in cache (100000), Cache timeout (seconds) (1800), Impersonation username, Impersonation password (<Not Displayed>), ASDK Client (Access Management Service On), and Web Server Client (Primary HTTP Cookie Domain example.com, Preferred HTTP Host host.example.com, Deny On Not Protected Off, CachePragmaHeader no-cache, CacheControlHeader no-cache, LogOutURLs). At the bottom, there is a "User Defined Parameters" section.

3 Create an access gate configuration for the SDK.

The SDK configuration is used for custom authentication modules and for other remote APIs.

The screenshot shows the Oracle Access Administration interface. The left sidebar has a tree view with the following nodes:

- Access Server Clusters
- AccessGate Configuration** (selected)
- Add New Access Gate
- Access Server Configuration
- Authentication Management
- Authorization Management
- User Access Configuration
- Common Information Configuration
- Host Identifiers

The main panel is titled "Details for AccessGate". It contains the following configuration settings:

Setting	Value
AccessGate Name	accessgate1
Description	
State	Enabled
Hostname	host.example.com
Port	<No Port Specified>
Access Gate Password	<Not Displayed>
Debug	Off
Maximum user session time (seconds)	3600
Idle Session Time (seconds)	3600
Maximum Connections	1
Transport Security	Open
IPValidation	Off
IPValidationException	
Maximum Client Session Time (hours)	24
Failover threshold	1
Access server timeout threshold	
Sleep For (seconds)	60
Maximum elements in cache	100000
Cache timeout (seconds)	1800
Impersonation username	
Impersonation password	<Not Displayed>
ASDK Client	
Access Management Service	On
Web Server Client	

4 Associate the web gates with Oracle Access Server.

This establishes a trust relationship.

The screenshot shows the 'ORACLE Access Administration' interface. The left sidebar has a tree view with the following nodes:- Access Server Clusters
- AccessGate Configuration
- Add New Access Gate
- Access Server Configuration** (selected)
- Authentication Management
- Authorization Management
- User Access Configuration
- Common Information Configuration
- Host Identifiers
The main panel title is 'Associated with server access'. It includes search filters for 'AAA role' (checked), 'Primary Server' (checked), and 'Secondary Server' (unchecked). There are also buttons for 'All' (radio button checked) and '0' (radio button uncheckable). A 'Results' button and a 'Go' button are also present. Below these filters, it says 'Displaying 1 to 2 of 2 results'. A table lists two entries:| Name | Hostname | Port | Transport Security | Access Management |
| --- | --- | --- | --- | --- |
| accessgate1 | host.example.com | <No Port Specified> | Open | Enabled |
| webgate1 | host.example.com | 9082 | Open | Enabled |

Below the table are 'Previous' and 'Next' buttons, followed by a 'Back' button.

5 Create a form-based authentication scheme

By default, Oracle Access Manager provides a credential collector form you can use it. You can also customize the form. For the examples in this document, the following properties are used.

The screenshot shows the Oracle Access Administration interface. The left sidebar has a tree view with the following nodes:- Access Server Clusters
- AccessGate Configuration
- Add New Access Gate
- Access Server Configuration
- Authentication Management** (selected)
- Authorization Management
- User Access Configuration
- Common Information Configuration
- Host Identifiers
The main content area has tabs: General (selected), Plugins, Steps, Authentication Flow. The sub-section "Details for Authentication Scheme" displays the following configuration:

Name	Form Over LDAP
Description	Redirects back to original request after login
Level	1
Challenge Method	Form
Challenge Parameter	Form: /login.html creds: login password action: /access/login passthrough: No
SSL Required	No
Challenge Redirect	
Enabled	Yes

At the bottom are "Modify" and "Back" buttons.

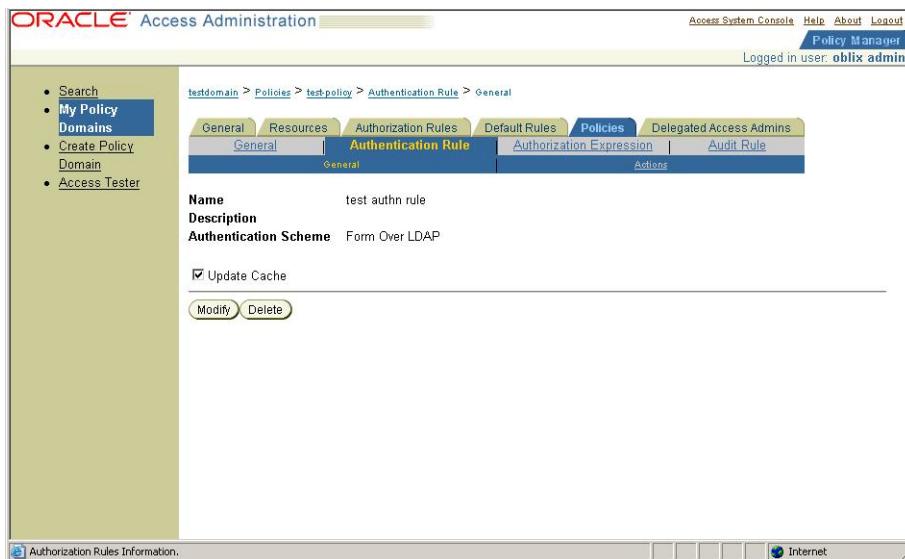
6 Configure the plug-ins.

The screenshot shows the Oracle Access Administration interface. The top navigation bar includes links for Policy Manager, Help, About, and Logout, along with the current user information: Logged in user: oblix admin. Below the navigation bar, there are tabs for System Configuration, System Management, and Access System Configuration, with Access System Configuration being the active tab. A sub-navigation menu on the left lists various configuration options, with Authentication Management selected. The main content area displays a table titled "Plugins for Authentication Scheme". The table has two columns: "Plugin Name" and "Plugin Parameters". It contains two rows: one for "credential_mapping" with parameters "obMappingBase='ou=oblixusers,dc=oracle,dc=com'", "obMappingFilter='(&(objectclass/inetOrgPerson)(uid=%login%))'", and another for "validate_password" with parameters "obCredentialPassword='password'", "obAnonUser='cn=anonymous,dc=oracle,dc=com'". At the bottom of the table are "Modify" and "Back" buttons.

Plugin Name	Plugin Parameters
credential_mapping	obMappingBase="ou=oblixusers,dc=oracle,dc=com",obMappingFilter="(&(objectclass=inetOrgPerson)(uid=%login%))"
validate_password	obCredentialPassword="password",obAnonUser="cn=anonymous,dc=oracle,dc=com"

7 Access the Policy Manager console (top-right link) and create a policy for your protected resource.

Protect the resource with the form-based authentication.



Accessing your protected application should redirect to the form login page. Upon successful authentication, the protected application will redirect to the protected resource with a valid Oracle Access Manager session.

Using Federated Access Manager to Enable Oracle Federation in the Identity Provider Environment

To enable Oracle Access Manager for federation in the Identity Provider environment, follow these steps:

1. [Install and configure Federation Access Manager in the Identity Provider container.](#)
2. [Install and configure Oracle Web Gate.](#)
3. [Install the Custom Authentication Module.](#)
4. [Install and configure Federated Access Manager in the Service Provider container.](#)
5. [Set up SAML2.](#)
6. [Configure Federated Access Manager for SAMLv2 Identity Provider protocols.](#)
7. [Configure Oracle Access Manager Agent to protect Federation Access Manager URLs.](#)
8. [Configure the Service Provider.](#)
9. [Verify that Single Sign-On is working properly.](#)

Installing and Configuring Federated Access Manager in the Identity Provider Container

Follow the installation instructions in the [*Sun Federated Access Manager Installation and Configuration Guide*](#). Make sure that the Identity Provider container is one of the supported Oracle Web Gate containers. Also make sure that the user repository is same as the Oracle Access Manager so that both Federated Access Manager and Oracle Access Manager provide a session for the same user.

Installing and Configuring the Oracle WebGate

Follow the instructions in the section [*Installing the WebGate*](#) in the [*Oracle Access Manager Installation Guide*](#).

Make sure that Oracle single sign-on is working for the protected URLs. Do not protect the Federated Access Manager URLs yet because you must first configure Federated Access Manager for authentication modules. For now, protect a temporary URL to ensure that Oracle WebGate is working properly. A temporary policy in Oracle Access Manager could be configured as in the following figure:



FIGURE 3–9 Configuring a temporary policy

Installing the Custom Oracle Authentication Module

In Federation Access Manager, install a custom authentication module for Oracle Access Manager. After exploding the Federated Access Manager WAR file, the custom authentication module is located under the directory *base-dir/samples/thirdparty/oblix*. Follow the instructions in the *README.txt* file for building and configuring a custom authentication module. Make sure that the custom authentication module is working before proceeding.

The custom authentication module implements the Federated Access Manager pluggable interface *AMLoginModule*. The *AMLoginModule* interface validates the Oracle Access Manager session using the Oracle Access Manager SDK, and then creates a Federation Access Manager session.

To configure the custom Oracle Authentication Module, provide the following information:

<i>OblixCookieName:</i>	Name of the Oblix session cookie
<i>OblixSDKInstallDir:</i>	Directory where the Oblix SDK is installed and configured. Make sure that <i>ObAccessClient.xml</i> is configured.
<i>RemoteUserHeaderName:</i>	The name of the header for an authenticated user after successful authentication.
<i>CheckRemoteUserOnly:</i>	If true, the auth modules looks only for the remote user header name.

Installing and Configuring Federated Access Manager in the Service Provider Container

Follow the installation instructions in the *Sun Federated Access Manager Installation and Configuration Guide*. A good practice is to install the Identity Provider and Server Provider in different domains. If that is not possible, make sure they use different cookie names or cookie domains. You do not have to install the Federated Access Manager web policy agent to protect the Federated Access Manager URLs at this time. First make sure that SAML2 is set up and working properly.

Setting Up SAML2

Before loading metadata, read the following sections and be sure you understand the changes that must be made to the metadata. The SAML2 samples contains instructions on how to setup SAML2.

In all, you must have Identity Provider metadata and extended metadata, as well as Service Provider metadata and extended metadata. In the Identity Provider, import Identity Provider metadata and extended metadata as hosted metadata. Import Service Provider metadata and extended metadata as remote entity metadata. To change the hosted or remote attributes, locate the extended metadata XML element <EntityConfig> which contains the following attribute with default value:

```
hosted=true
```

Change the value to `false`.

▼ To Configure the Identity Provider Federated Access Manager for SAMLv2 Identity Provider Protocols

1 Generate the metadata templates on both Identity Provider and Service Provider environments.

You can use one of the following methods:

- Use the `famadm` command.
- Use a browser:

```
http://host:port/opensso/famadm.jsp
```

a. At the Identity Provider, run the following command:

```
famadm create-metadata-templ -y idp_entity_id -u amadmin  
-f admin_password_file_name -m idp_standard_metadata
```

```
-x idp_extended_metadata -i idp_meta_alias  
where idp_meta_alias is "/idp".
```

b. At the Service Provider, run the following command:

```
famadm create-metadata-templ -y sp_entity_id -u amadmin  
-f admin_password_file_name -m sp_standard_metadata  
-x sp_extended_metadata -s sp_meta_alias  
where sp_meta_alias is "/sp".
```

2 Customize extended metadata.

Use one of the following options:

- **To the Identity Provider extended metadata, add an attribute named AuthUrl.**

This URL attribute is used by the SAML protocols to redirect to a Federated Access Manager authentication module. In this use case, the redirect is to the custom Oracle Authentication Module. Example:

```
<Attribute name="AuthUrl">  
<Value>http://host:port/opensso/UI/Login?module=OAMAuth</Value>  
</Attribute>
```

- **Make the custom Oracle authentication module as the default login module in Federation Access Manager.**

A consequence of using this option is that you have to specify an LDAP login module for logging in as administrator. The Service Provider extended metadata has an attribute named as transientUser. Set this value to your anonymous user. Example:

```
<Attribute name="transientUser">  
  <Value>anonymous</Value>  
</Attribute>
```

3 Change the hosted attribute in the Identity Provider and Service Provider extended metadata when loading remote metadata.

For a remote Identity Provider or Service Provider, set the value to "false" or "0".

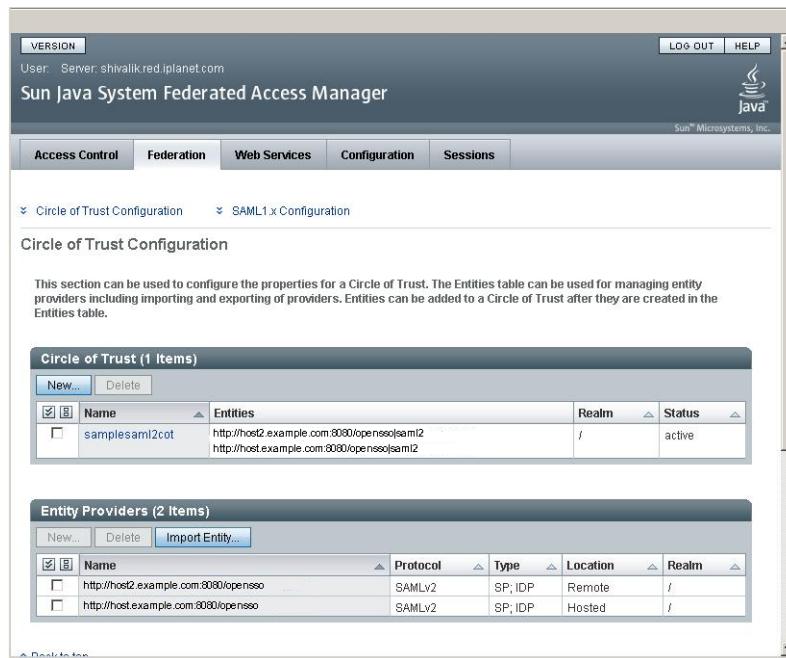
4 Load the metadata.

a. Create circle of trust.

Add the circle of trust to the extended metadata. In the extended template files, you will see a sample circle of trust. Edit the following to correspond to your circle of trust.

```
<Attribute name="cotlist">  
<Value>samplesaml2cot</Value>  
</Attribute>
```

- b. Load the hosted metadata in both the Identity Provider and Service Provider.**
You can use either the `famadm` command or the Federated Access Manager console.
 - c. Exchange the metadata .**
Import the Service Provider metadata into the Identity Provider, and import the Identity Provider metadata into the Service Provider.
 - d. Load the metadata.**
- 5 After successfully exchanging the metadata, verify through the Federated Access Manager administration console that the metadata has been configured correctly.**



To Configure Oracle Access Manager Agent to protect Federation Access Manager URLs

There are many different ways to configure Oracle Access Manager Policy to protect Federated Access Manager URLs. At minimum, you must configure a policy to protect the SAML Single Sign-On Service URL. The real-time policy can be different based on other deployment requirements. The Oracle Access Manager session must be established before the SAML Assertion is generated.

In Oracle Access Server Policy Console, create a policy domain named fampolicy to protect only the Federated Access Manager Single Sign-On Service URL.



FIGURE 3–10 Creating a policy domain

▼ To Configure the Service Provider

- 1 **Install the Federated Access Manager web policy agent in the Service Provider environment to protect Federation Access Manager Service Provider.**

Follow the instructions in the *Sun Java System Access Manager Policy Agent 2.2 Release Notes*.

There is no restriction on the type of policy agent you use. However, be sure use an agent that is supported on the container where the application to be protected is deployed.

- 2 **Change the policy agent login URL.**

After verifying that simple single sign-on with the Federated Access Manager works properly, change the policy agent login URL to the Federated Access Manager SAML2 SP initiated Single Sign-on Service URL. Example:

```
http://<sphost>:<spport>/opensso/saml2/jsp/spSSOInit.jsp?metaAlias
=<SP MetaAlias>
&idpEntityID=<IDP Entity ID>&NameIDFormat=transient
```

▼ To Test the Single Sign-On

- 1 **Authenticate at Oracle Access Manager with username and password.**

- 2 Access the enterprise application protected by the Federated Access Manager Service Provider policy agent in the Service Provider environment.

You should automatically be granted access to the protected application.

Using Federated Access Manager to Enable Oracle Federation in a Service Provider Environment

To enable Oracle Access Manager for Federation in the Service Provider environment, follow these steps:

1. [Install Federated Access Manager in the Identity Provider environment.](#)
2. [Install Federated Access Manager in the Service Provider environment.](#)
3. [Install Oracle Access Manager in the Service Provider domain.](#)
4. [Configure Oracle Access Manager for the Federation Access Manager scheme.](#)
5. [Configure a resource.](#)
6. [Set Up SAMLv2.](#)
7. [Configure the Federated Access Manager Identity Provider and Service Provider for SAML2 protocols.](#)
8. [Verify that single sign-on is working properly.](#)

Installing Federation Access Manager in the Identity Provider Environment

The Identity Provider does not have to be a Federated Access Manager deployment. But for optimum protocol interoperability, use Federated Access Manager. See the [Sun Federated Access Manager Installation and Configuration Guide](#) for detailed installation and configuration steps.

A good practice is to install the Identity Provider and Server Provider in different domains. If that is not possible, make sure they use different cookie names or cookie domains. This eliminates cookie validation inconsistency.

Installing Federation Access Manager in the Service Provider Environment

See the [*Sun Federated Access Manager Installation and Configuration Guide*](#) for detailed installation and configuration steps.

The Federated Access Manager in the Service Provider environment initiates the SAML2 protocols. The Oracle Access Manager Agent can protect the enterprise application by redirecting to Federated Access Manager for single sign-on purposes.

Installing Oracle Access Manager

Install Oracle Access Manager in the Service Provider domain where enterprise applications are protected by Oracle WebGate agents. See the *Oracle Access Manager Installation Guide* for detailed installation instructions.

The plug-in name must be same as the name of the shared library.

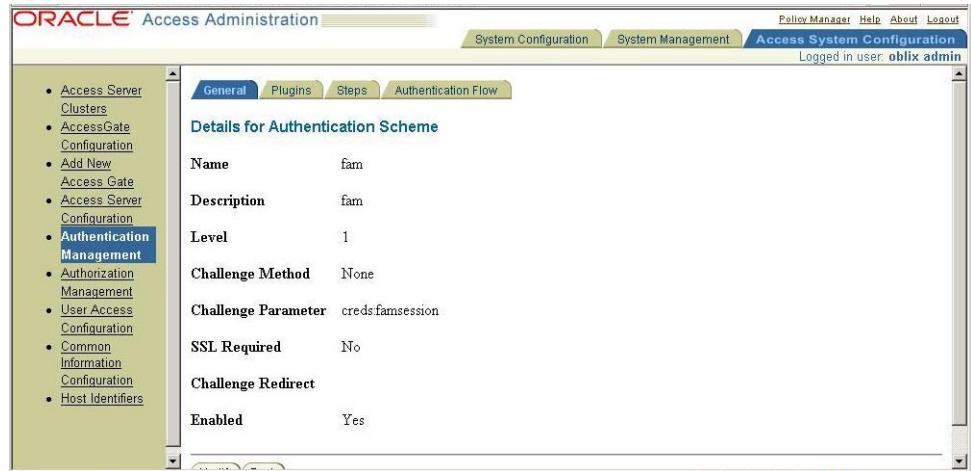


FIGURE 3-11 The plug-in name must be same as the name of the shared library

Configuring Oracle Access Manager for Federation Access Manager Scheme

The custom authentication scheme for Oracle Access Manager is a C-based implementation, and the custom authentication scheme should be built like a shared library. The custom authentication scheme in this chapter is a Solaris-based shared library and can be ported onto other platforms with similar semantics. This custom authentication module also uses Federation Access Manager C-SDK for validating the Federated Access Manager session. When a Federated Access Manager WAR file is exploded, the custom authentication module is located under the *base-dir/samples/thirdparty/oblix* directory. The *README.txt* contains instructions for configuring the Oracle Access Manager authentication scheme. The following figure provides some details for configuring Federated Access Manager AuthSchemein Oracle Access Manager.

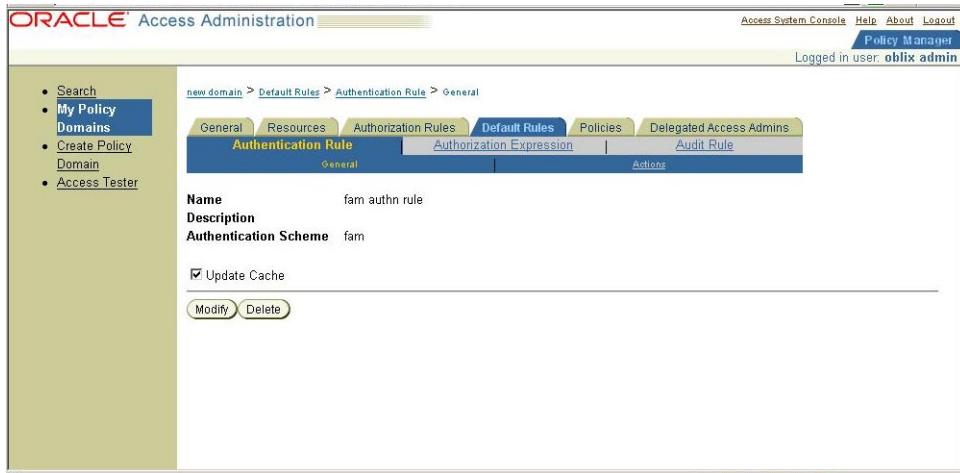


FIGURE 3-12 Configuring Federated Access Manager AuthSchemein Oracle Access Manager

Configuring a Resource

The following figure provides some details for configuring a resource in Oracle Access Manager.

The screenshot shows the Oracle Access Manager web interface. At the top, it displays the user information "User: Server: shivalik:red.iplanet.com" and the title "Sun Java System Federated Access Manager". Below the title is a navigation bar with tabs: Access Control (selected), Federation, Web Services, Configuration, and Sessions. The main content area has two expandable sections: "Circle of Trust Configuration" and "SAML1.x Configuration". The "Circle of Trust Configuration" section is expanded, showing a table titled "Circle of Trust (1 Items)". The table has columns: Name, Entities, Realm, and Status. It contains one row with the name "samplesaml2cot" and the entity URLs "http://host2.example.com:8080/openSSO/saml2" and "http://host.example.com:8080/openSSO/saml2". The "Status" column shows "active". The "Realm" column shows a small icon. The "Entity Providers (2 Items)" section is also visible below, showing a table with columns: Name, Protocol, Type, Location, and Realm. It lists two entries: "http://host2.example.com:8080/openSSO" (Protocol SAMLv2, Type IDP, Location Remote, Realm /) and "http://host.example.com:8080/openSSO" (Protocol SAMLv2, Type SP, Location Hosted, Realm /). Both entries have their "Protocol" and "Type" fields set to "SAMLv2".

FIGURE 3–13 Configuring a resource in Oracle Access Manager

Later you will use the resource name here in the SAML Adapter configuration. The policy will trigger the Federated Access Manager authentication module.

Setting Up SAMLv2

In all, you must have Identity Provider metadata and extended metadata, as well as Service Provider metadata and extended metadata. In the Identity Provider, import Identity Provider metadata and extended metadata as hosted metadata. Import Service Provider metadata and extended metadata as remote entity metadata. To change the hosted or remote attributes, locate the extended metadata XML element <EntityConfig> which contains the following attribute with default value:

```
hosted=true
```

Change the value to false.

▼ To Configure the Federated Access Manager Identity and Service Providers for SAML2 Protocols

1 Generate the metadata templates on both Identity Provider and Service Provider environments.

Use the famadm command, or used use a browser to go to the following URL:

```
http:<host>:<port>/opensso/famadm.jsp
```

- At the Identity Provider:

```
famadm create-metadata-templ -y idp_entity_id  
-u amadmin -f admin_password_file_name -m idp_standard_metadata  
-x idp_extended_metadata -i idp_meta_alias
```

where idp_meta_alias is /idp

- At the Service Provider:

```
famadm create-metadata-templ -y sp_entity_id  
-u amadmin -f admin_password_file_name -m sp_standard_metadata  
-x sp_extended_metadata -s sp_meta_alias
```

where sp_meta_alias is /sp

2 Customize the Service Provider extended metadata.

Add the Service Provider extended metadata as an attribute named as spAdapter. This attribute is used by the SAML protocols to do any post single sign-on authentication processes. In the architecture diagram, this the Oracle Access Manager Plug-in. The OAMPlugin uses the Federated Access Manager session to authenticate against Oracle Access Manager and establish ObSSOCookie. The Service Provider metadata must have the following attributes:

```
<Attribute name="spAdapter">  
<Value>com.sun.identity.saml2.plugins.SMAdapter</Value>  
</Attribute>  
  
<Attribute name="spAdapterEnv">  
<Value>FAMCookieName=iPlanetDirectoryPro</Value>  
<Value>OAMCookieName=ObSSOCookie</Value>  
<Value>CookieDomain=.red.example.com</Value>  
<Value>Resource=/test/index.html</Value>
```

```
<Value>ObSDKInstallDir=/export/oam/AccessServerSDK</Value>
</Attribute>
```

3 Set the value for transientUser to the anonymous user.

The Service Provider extended metadata has an attribute named as `transientUser`. Make sure that the Federated Access Manager Service Provider is enabled for Anonymous authentication. Check the documentation for more information.

```
<Attribute name="transientUser">
<Value>anonymous</Value>
</Attribute>
```

4 Create a circle of trust as mentioned in the URL.

The circle of trust should also be added in your extended metadata.

5 Load the metadata.

6 Edit the following attribute to one of your circle of trust.

The extended template files contains a sample circle of trust.

```
<Attribute name="cotlist">
<Value>samplesaml2cot</Value>
</Attribute>
```

You can also add the circle of trust through the Federated Access Manager administration console.

7 Load the hosted metadata in both the Identity Provider and Service Provider.

You can use the `famadm` command or the Federated Access Manager administration console.

8 Exchange the metadata between Identity Provider and Service Provider.

and load the metadata.

a. Import the Identity Provider metadata into the Service Provider metadata.

b. Import the Service Provider metadata into the Identity Provider metadata.

c. Change the hosted attribute value in the extended metadata to false.

d. Load all metadata.

- 9 Verify through Federated Access Manager administration console that the metadata is configured properly.

The screenshot shows the Sun Java System Federated Access Manager administration console. The top navigation bar includes 'LOG OUT' and 'HELP' buttons, and a 'java' logo. The main menu tabs are 'Access Control', 'Federation', 'Web Services', 'Configuration', and 'Sessions'. The 'Federation' tab is selected. Below the tabs, there are two dropdown menus: 'Circle of Trust Configuration' and 'SAML1.x Configuration'. The 'Circle of Trust Configuration' section is expanded, showing a table titled 'Circle of Trust (1 Items)'. It contains one row with a checkbox, name 'samplesaml2cot', and URL 'http://host2.example.com:8080/openSSO/saml2'. The 'Status' column shows 'active'. The 'Entity Providers (2 Items)' section is also expanded, showing a table with two rows. The first row has a checkbox, name 'http://host2.example.com:8080/openSSO', protocol 'SAMLv2', type 'IDP', location 'Remote', and realm '/'. The second row has a checkbox, name 'http://host.example.com:8080/openSSO', protocol 'SAMLv2', type 'SP', location 'Hosted', and realm '/'. At the bottom left, there is a link 'Back to top'.

Verifying that Single Sign-On Works Properly

Access the enterprise application protected by Oracle WebGate. Oracle WebGate redirects to Federated Access Manager for authentication where the SAML2 single sign-on is initiated.