

Best Practices for Oracle FMW Identity and Access Management (11.1.2.3): Extending an Enterprise Deployment with Oracle Adaptive Access Manager

ORACLE WHITE PAPER | JULY 2016





Table of Contents

Introduction	1
The Enterprise Deployment Topology with OAAM	1
Typical Memory, File Descriptors, and Processes Required for an Oracle Identity and Access Management Enterprise Deployment	3
Using the Enterprise Deployment Workbook	1
OAAM Details	1
Overview of Extending the Domain to Include OAAM	2
Prerequisites	2
Creating a Highly Available Database	2
Creating OAAM Users and Groups in LDAP	2
Create OAAM Users and Groups as follows:	2
Create users using idmConfigTool.	4
Extending Domain for Oracle Adaptive Access Manager	4
Restarting Administration Server on OAMHOST1	8
Deploying Managed Server Configuration to Local Storage	8
Adding OAAM Servers to Start and Stop Scripts	8
Starting and Validating OAAM on OAMHOST1	9
Starting Oracle Adaptive Access Manager on OAMHOST1	9
Validating OAAM on OAMHOST1	9
Starting and Validating OAAM on OAMHOST2	9
Starting Oracle Adaptive Access Manager on OAMHOST2	9
Validating OAAM on OAMHOST2	10

Configuring OAAM to Work with Web Tier	10
Configuring Access from Oracle HTTP Server	10
Updating IADADMIN.example.com	10
Updating login.example.com	10
Restarting Oracle HTTP Servers and OAAM Managed Servers	11
Changing Host Assertion in WebLogic	11
Validating Oracle Adaptive Access Manager	12
Loading Oracle Adaptive Access Manager Seed Data	12
Integrating Oracle Adaptive Access Manager with Oracle Access Management Access Manager	12
Retrieving the Global Passphrase for Simple Mode	13
Registering OAAM as a Third Party Application	13
Adding an Agent Password to the IAMSuiteAgent Profile	14
Validation	15
Setting OAAM properties for Access Manager	16
Creating a Test Resource	18
Creating Oracle Adaptive Access Manager Policies	19
Creating a Resource in Access Manager	19
Validating Oracle Adaptive Access Manager	19
Moving TAP Resource to LDAP Policy	20
Integrating Oracle Adaptive Access Manager with Oracle Identity Manager	21
Configuring Oracle Identity Manager Encryption Keys in CSF	21



Configuring Cross Domain Trust Between Oracle Identity Manager and Oracle Adaptive Access Manager	21
Setting Oracle Adaptive Access Manager Properties for Oracle Identity Manager	22
Setting Oracle Identity Manager Properties for OAAM	23
Restarting IAMAccessDomain and IAMGovernanceDomain	23
Validating OAAM - Oracle Identity Manager Integration	23
Validating Oracle Identity Manager-OAAM Integration	24
Changing Domain to Oracle Adaptive Access Manager Protection	23
Backing Up the Application Tier Configuration	24
Conclusion	24





Introduction

The Oracle Enterprise Deployment Guide for Identity and Access Management 11.1.2.3 describes how to setup an Enterprise Deployment of Oracle Identity and Access Management. By following the processes in this guide, you can setup a mission critical deployment of:

- » Oracle Unified Directory, Oracle Internet Directory, or, Active Directory.
- » Oracle Access Manager
- » Oracle Identity Manager

This document describes how to take this deployment and extend it further with Oracle Adaptive Access Manager.

Oracle Adaptive Access Manager helps organizations prevent fraud and misuse by strengthening existing authentication flows, evaluating the risk of events as they happen and providing risk-based interdiction mechanisms such as multi-factor out-of-band authentication. Intuitive policy administration and standardized integrations with the Identity and Access Management Suite components makes Oracle Adaptive Access Manager uniquely flexible and effective at reducing an enterprise's security exposure. Oracle Adaptive Access Manager provides real-time and batch risk analytics to combat fraud and misuse across multiple channels of access. Oracle Adaptive Access Manager automates reviews of access and transaction events to detect fraud and misuse resulting in saved time and money. The proven capabilities and quick return on investment Oracle Adaptive Access Manager provides makes it a must have for any enterprise.

Oracle Adaptive Access Manager (OAAM) is built on a Java EE-based, multi-tiers deployment architecture that separates the platform's presentation, business logic, and data tiers. Because of this separation of tiers, OAAM can rapidly scale with the performance needs of the customer. The architecture can leverage the most flexible and supported cross-platform Java EE services available: a combination of Java, XML and object technologies. This architecture makes OAAM a scalable, fault-tolerant solution.

Oracle Adaptive Access manager consists of the following two components.

- » OAAM Administration Applications
- » OAAM Server Applications

The Enterprise Deployment Topology with OAAM

After completing the steps in this document your Enterprise Deployment Topology will look like the following:

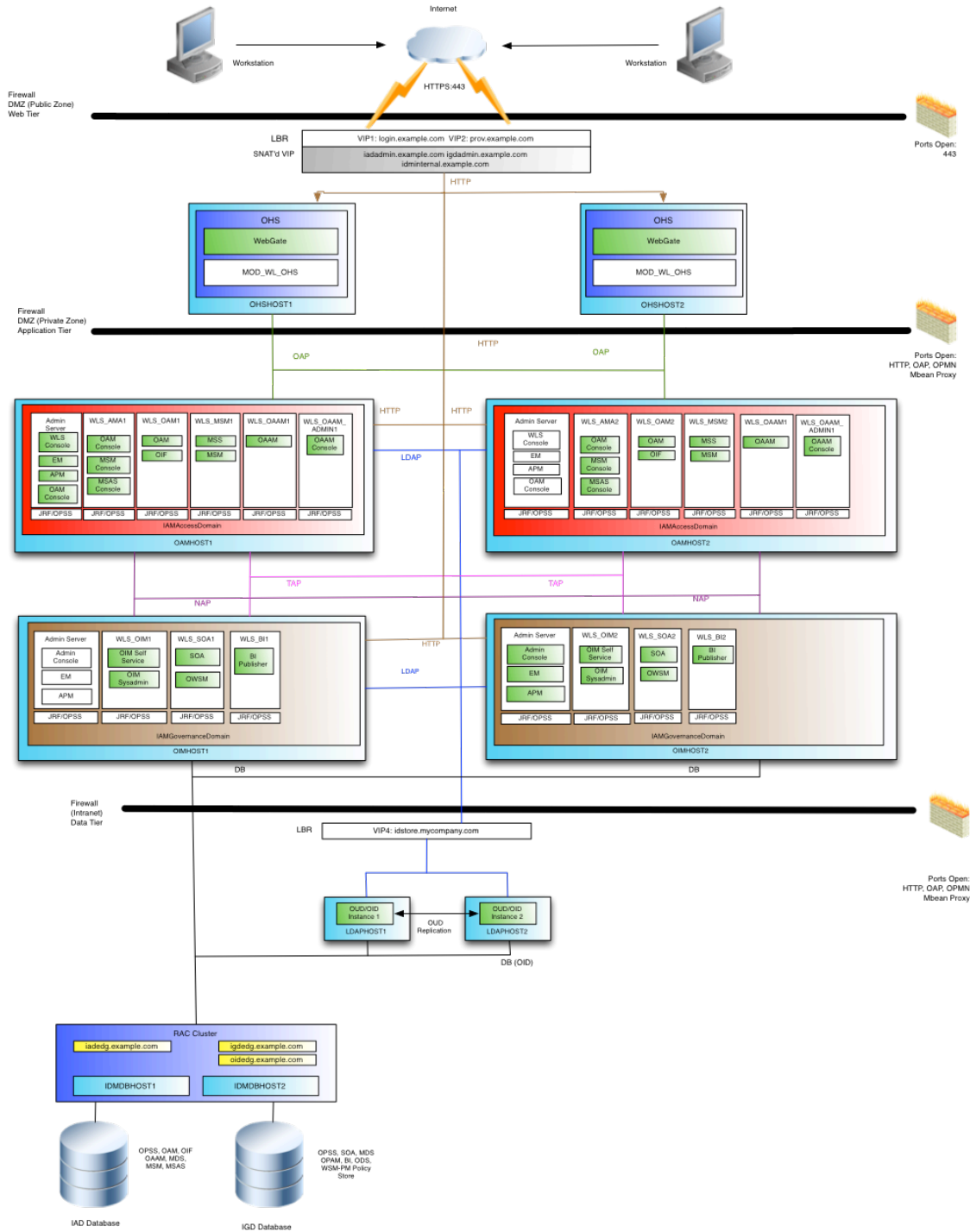


Figure 1. Oracle Identity and Access Management Topology

Typical Memory, File Descriptors, and Processes Required for an Oracle Identity and Access Management Enterprise Deployment

Table 1 summarizes the memory, file descriptors, and processes required for the Administration Server and each of the Managed Servers computers in a typical Oracle SOA Suite enterprise deployment. These values are provided as an example only, but they can be used to estimate the minimum amount of memory required for an initial enterprise deployment.

The example in Table 1 reflects the minimum requirements for configuring the Managed Servers and other services required on OAMHOST1, as depicted in the reference topologies in Section Deployment Topology

When you are procuring machines, use the information in the Approximate Top Memory column as a guide when determining how much physical memory each host computer should have available.

After you procure the host computer hardware and verify the operating system requirements, review the software configuration to be sure the operating system settings are configured to accommodate the number of open files listed in the File Descriptors column and the number processes listed in the Operating System Processes and Tasks column..

TABLE 1: TYPICAL MEMORY, FILE DESCRIPTORS, AND PROCESSES REQUIRED FOR EACH ENTERPRISE DEPLOYMENT HOST

Managed Server, Utility, or Service	Approximate Top Memory	Number of File Descriptors	Operating System Processes and Tasks
WLS_OAAM_ADMIN	2 GB	800	100
WLS_OAAM	1.5 GB	750	100

Using the Enterprise Deployment Workbook

The Oracle Fusion Middleware Enterprise Deployment Workbook is a companion document to this guide. It is a spreadsheet that can be used by architects, system engineers, database administrators, and others to plan and record all the details for an environment installation (such as server names, URLs, port numbers, installation paths, and other resources). Refer to the Oracle Enterprise Deployment Guide for Identity and Access Management 11.1.2.3, for more details about Enterprise Deployment Workbook.

The Oracle Identity and Access Management Enterprise Deployment Workbook is available as a Microsoft Excel Spreadsheet in the Oracle Fusion Middleware documentation library. It is available as a link on the Install, Patch, and Upgrade page of the library.

OAAM Details

In addition to the Enterprise Deployment Workbook that you would have created for the Identity and Access Management Deployment, use this worksheet to keep track of additional OAAM specific information

TABLE 2: OAAM DETAILS

Description	Documented Variable	Documented Value	Actual Value
OAAM Managed Server Names		WLS_OAAM1 WLS_OAAM2	
OAAM Managed Server Port	OAAM_PORT	14300	
OAAM Managed Server SSL Port	OAAM_SSL_PORT	14301	
OAAM Administrative Managed Server Names		WLS_OAAM_ADMIN1 WLS_OAAM_ADMIN2	
OAAM Administrative Managed Port	OAAM_ADMIN_PORT	14200	
OAAM Administrative Managed SSL Port	OAAM_ADMIN_SSL_PORT	14201	
Identity Store Host	LDAPHOST	LDAPHOST1.EXAMPLE.COM	
Identity Store Port	LDAP_PORT	1389	
Identity Store Bind DN	LDAP_ADMIN_USER	cn=oudadmin	



Identity Store Administrator Port	LDAP_ADMIN_PORT	4444	
Identity Store Group Search Base	LDAP_GROUP	cn=Groups,dc=example,dc=com	
OAAM Administrative User	OAAMADMINUSER	oaamadmin	
Access Manager Host1	OAMHOST1	OAMHOST1	
Access Manager Host2	OAMHOST2	OAMHOST2	

Overview of Extending the Domain to Include OAAM

Oracle Adaptive Access manager consists of the following two components.

- » OAAM Administration Applications
- » OAAM Server Applications

Prerequisites

Before you extend the domain to include Oracle Adaptive Access Manager (OAAM), the following prerequisites must be in place.

Creating a Highly Available Database

Create a highly available database to hold the OAAM data, if you are not using the IADDB. Pre-seed the database with OAAM data objects using the repository creation utility. This document assumes that the Access Database Service is used for OAAM schema.

Creating OAAM Users and Groups in LDAP

Create OAAM Users and Groups as follows:

Create a configuration file with the following contents:

```
# Common
```

```
IDSTORE_HOST: LDAPHOST1.example.com
```

```
IDSTORE_PORT: 1389
```



IDSTORE_ADMIN_PORT: 4444

IDSTORE_BINDDN: cn=oudadmin

IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com

IDSTORE_SEARCHBASE: dc=example,dc=com

IDSTORE_USERNAMEATTRIBUTE: cn

IDSTORE_LOGINATTRIBUTE: uid

IDSTORE_USERSEARCHBASE: cn=Users, dc=example,dc=com

IDSTORE_OAAMADMINUSER: oaamadmin

Where:

- » IDSTORE_HOST (*LDAP_HOST*) and IDSTORE_PORT (*LDAP_PORT*) are, respectively, the host and port of your Identity Store directory, for example:

- » OUD: LDAPHOST1 and 1389

- » IDSTORE_ADMIN_PORT (*LDAP_ADMIN_PORT*) is the administration port of your Oracle Unified Directory instance.

- » IDSTORE_BINDDN (*LDAP_ADMIN_USER*) is an administrative user in the Identity Store Directory.

- » IDSTORE_GROUPSEARCHBASE is the location in the directory where groups are stored. For example:
cn=Groups,dc=example,dc=com

- » IDSTORE_SEARCHBASE is the location in the directory where users and groups are stored. For example:
cn=Users,dc=example,dc=com

- » IDSTORE_USERNAMEATTRIBUTE is the name of the directory attribute containing the user's name, for example: cn. Note that this is different from the login name.

- » IDSTORE_LOGINATTRIBUTE is the LDAP attribute which contains the users Login name, for example: uid.

- » IDSTORE_USERSEARCHBASE is the location in the directory where users are stored. For example:
dc=example,dc=com

- » IDSTORE_OAAMADMINUSER (*OAAMADMINUSER*) is the name of the user you want to create as your Oracle Adaptive Access Manager Administrator.



Create users using `idmConfigTool`.

You must seed the Identity Store with users and groups that are required by the Identity and Access Management components. To seed users and groups in Identity Store, perform the following tasks on OAMHOST1:

1. Set environment variables.
Set `MW_HOME` to `IAD_MW_HOME`.
Set `ORACLE_HOME` to `IAD_ORACLE_HOME`.
Set `JAVA_HOME` to `JAVA_HOME`.
2. Configure the Identity Store by using the command `idmConfigTool`, which is located at:
`IAD_ORACLE_HOME/idmtools/bin`

The syntax of the command on Linux is:

```
idmConfigTool.sh -prepareIDStore mode=OAAM input_file=configfile
```

Where `configfile` is the name of the configuration file you created at the beginning of this section.

3. When the command runs, you are prompted to enter the password of the account you are connecting to the Identity Store with.

During the command execution you are prompted to supply passwords for the accounts being created. For ease of use, it is recommended that you supply the `COMMON_IDM_PASSWORD` if you are using a common password throughout.

After running each command, check the log file for any errors or warnings and correct them. The file with the name `automation.log` is created in the directory where you run the tool.

Extending Domain for Oracle Adaptive Access Manager

Start the configuration wizard by executing the following command on OAMHOST1:

```
IAD_MW_HOME/oracle_common/common/bin/config.sh
```

Then proceed as follows:

1. On the Welcome Screen, select **Extend an Existing WebLogic Domain**. Click **Next**
2. On the Select a WebLogic Domain screen, using the navigator select the domain home of the Administration Server, for example: `IAD_ASERVER_HOME`
Click **Next**.
3. On the Select Extension Source screen, select the following:
 - o Oracle Adaptive Access Manager - Server
 - o Oracle Adaptive Access Manager - Admin ServerClick **Next**
4. On the Configure JDBC Component Schema screen, do the following:
Select:
 - o OAAM Admin Schema
 - o OAAM Server Schema
 - o OAAM Admin MDS Schema

For the Oracle RAC configuration for component schemas, select **Convert to GridLink**.
Click **Next**.

5. The Gridlink RAC Component Schema screen appears. In this screen, enter values for the following fields, specifying the connect information for the Oracle RAC database that was seeded with RCU. For Exadata SDP Connections, enter the TCP parameters below. Later, this must be converted to an SDP Connect String.
 - » **Driver:** Select Oracle's driver (Thin) for GridLink Connections, Versions: 10 and later.
 - » Select **Enable FAN**.
 - » Do one of the following:
 - If SSL is not configured for ONS notifications to be encrypted, deselect SSL.
 - Select SSL and provide the appropriate wallet and wallet password.
 - **Service Listener:** Enter the SCAN address and port for the RAC database being used. You can identify this address by querying the parameter `remote_listener` in the database:

```
SQL>show parameter remote_listener;

NAME                TYPE        VALUE
-----
remote_listener      string      iamdbscan.example.com:1521
```

Note:

For Oracle Database 11g Release 1 (11.1), use the virtual IP and port of each database instance listener, for example: `DBHOST1-VIP.example.com (port 1521)` and `DBHOST2-VIP.example.com (port 1521)`, where 1521 is `DB_LISTENER_PORT`

- **ONS Host:** Enter the SCAN address for the Oracle RAC database and the ONS remote port as reported by the database:

```
srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

Note:

For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service, for example:

```
DBHOST1.example.com (port 6200)
and
DBHOST2.example.com (port 6200)
```

Enter the following RAC component schema information:

TABLE 3: RAC COMPONENT SCHEMA INFORMATION

Schema Name	Service Name	Schema Owner	Password
OAAM Admin Schema	EDGIAD.example.com	EDGIAD_OAAM	Password

OAAM Admin MDS Schema	EDGIAD.example.com	EDGIAD_MDS	Password
OAAM Server Schema	EDGIAD.example.com	EDGIAD_OAAM	Password

- On the Test Component Schema screen, the configuration wizard attempts to validate the data source. If the data source validation succeeds, click **Next**.
If it fails, click **Previous**, correct the issue, and try again.
- On the Select Optional Configuration screen, select **Managed Server Clusters and Machines**. Click **Next**
- When you first enter the Configure Managed Servers screen, you will see entries for components already configured such as Access Manager. In addition the wizard will create 2 new managed servers for OAAM.

Note:

When you first enter this screen the config wizard has created default Managed Servers for you.

Change the details of the default Managed Server to reflect the following details. That is, **change one entry and add one new entry**.

Do not change the configuration of any Managed Servers which have already been configured as part of previous application deployment

TABLE 4: OAAM MANAGED SERVER DETAILS

Default Name	Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
OAAM_SERVER_SERVER1	WLS_OAAM1	OAMHOST1	14300 (OAAM_ADMIN_PORT)	14301 (OAAM_ADMIN_SSL_PORT)	selected
	WLS_OAAM2	OAMHOST2	14300 (OAAM_ADMIN_PORT)	14301 (OAAM_ADMIN_SSL_PORT)	selected
OAM_ADMIN_SERVER1	WLS_OAAM_ADMIN1	OAMHOST1	14200 (OAAM_PORT)	14201 (OAAM_SSL_PORT)	selected
	WLS_OAAM_ADMIN2	OAMHOST2	14200 (OAAM_PORT)	14201 (OAAM_SSL_PORT)	selected

Note: You must use the names listed in the Table 4, to facilitate automatic patching.

Leave all other fields at the default settings and click **Next**.

- On Configure Clusters screen, create a cluster by clicking Add and provide the values shown for oaam_cluster in the following table. Then create a second cluster by clicking Add and provide the values shown for oaam_admin_cluster in the table.

TABLE 5: CLUSTER DETAILS

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
OAAM_CLUSTER	Unicast	n/a	n/a	Leave it empty.
OAAM_ADMIN_CLUSTER	Unicast	n/a	n/a	Leave it empty.

Leave all other fields at the default settings and click **Next**.

- On the Assign Servers to Clusters screen, associate the Managed Servers with the cluster. Click the cluster name in the right pane. Click the Managed Server under Servers, then click the arrow to assign it to the cluster.

Assign servers to the clusters as follows:

TABLE 6: ASSIGN SERVERS TO CLUSTERS

Cluster	Server
OAAM_CLUSTER	WLS_OAAM1, WLS_OAAM2
OAAM_ADMIN_CLUSTER	WLS_OAAM_ADMIN1, WLS_OAAM_ADMIN2

Note: Do not change the configuration of any clusters which have already been configured as part of previous application deployments.

Click **Next**.

- On the Configure Machines screen, click **Next**.

Note: Deployment will have created Machines for you

- On the Assign Servers to Machines screen, assign servers to machines as follows:
 - » OAMHOST1: wls_oaam1, wls_oaam_admin1
 - » OAMHOST2: wls_oaam2, wls_oaam_admin2


Click **Next** to continue.

- On the Configuration Summary screen, click **Extend** to extend the domain

Note: If you receive a warning that says:

CFGFWK: Server listen ports in your domain configuration conflict with ports in use by active processes on this host

Click **OK**.



This warning appears if Managed Servers have been defined as part of previous installs and can safely be ignored.

Restarting Administration Server on OAMHOST1

Restart WebLogic Administration Server on OAMHOST1.

Deploying Managed Server Configuration to Local Storage

Once the configuration is complete, you must propagate the Oracle Adaptive Access Manager configuration to the managed server directory on OAMHOST1 and OAMHOST2.

Propagate the Oracle Adaptive Access Manager by packing first the domain IAMAccessDomain from the shared storage location and unpacking it to managed server directory on local storage.

You do this by packing and unpacking the domain, you pack the domain first on IAMAccessDomain on OAMHOST1 then unpack it on OAMHOST1 and OAMHOST2.

Follow these steps to propagate the domain to the managed server domain directory.

14. Invoke the *pack* utility from `ORACLE_COMMON_HOME/common/bin/` on OAMHOST1

```
./pack.sh -domain=IAD_ASERVER_HOME -template=iam_domain.jar -template_name="IAM Domain" -managed=true
```

15. On OAMHOST1 and OAMHOST2, invoke the utility *unpack*, which is also located in the directory: `ORACLE_COMMON_HOME/common/bin/`

```
./unpack.sh -domain=IAD_MSERVER_HOME -template=iam_domain.jar -overwrite_domain=true -  
app_dir=IAD_MSERVER_HOME/applications
```

If you see a message similar to this, you may safely ignore it:


```
>> Server listen ports in your domain configuration conflict with ports in use by active processes on this  
host.
```

```
Port 14100 on wls_oam2
```

Adding OAAM Servers to Start and Stop Scripts

Deployment creates a set of scripts to start and stop managed servers defined in the domain. Whenever you create a new managed server in the domain you must update the domain configuration so that these start and stop scripts can also start the newly created managed server. You must now do this for each of the OAAM managed servers.

To update the domain configuration, edit the file `serverInstancesCustom.txt`, which is located in the directory: `SHARED_CONFIG_DIR/scripts`



If you want to start a node manager on a new machine, add an entry which looks like this:

```
newmachine.example.com NM nodemanager_pathname nodemanager_port
```

For example:

```
OAMHOST3.example.com NM /u01/oracle/config/nodemanager/oamhost3.example.com 5556
```

On each of the OAAM managed servers in the Table 4: OAAM Managed Server Details, add an entry which looks like this:

```
newmachine.example.com OAAM ManagedServerName
```

For example:

```
OAMHOST1 OAAM wls_oaam1 IADADMINVHN 7001
OAMHOST1 OAAM wls_oaam_admin1 IADADMINVHN 7001
OAMHOST2 OAAM wls_oaam2 IADADMINVHN 7001
OAMHOST2 OAAM wls_oaam_admin2 IADADMINVHN 7001
```

Save the file.

Starting and Validating OAAM on OAMHOST1

Starting Oracle Adaptive Access Manager on OAMHOST1

Start the WebLogic Administration Console for IAMAccessDomain

Select **Environment**, **Servers** from the domain structure menu then click the **Control** tab.

Select the servers **wls_oaam_admin1** and **wls_oaam1** and click **Start**.

Validating OAAM on OAMHOST1

Validate the implementation by connecting to the OAAM Administration Server at http://OAMHOST1.example.com:14200/oaam_admin. The implementation is valid if OAAM Administration console login page is displayed and you can login using the oaamadmin account you created in Section, "[Creating OAAM Users and Groups in LDAP](#)."

Validate the implementation by connecting to the OAAM Server at:


http://OAMHOST1.example.com:14300/oaam_server

The implementation is valid if the OAAM Server login page is displayed.

Starting and Validating OAAM on OAMHOST2

This section describes how to configure Oracle Adaptive Access Manager on OAMHOST2

Starting Oracle Adaptive Access Manager on OAMHOST2



Start Oracle Adaptive Access Manager on OAMHOST2 using the WebLogic Administration Console for IAMAccessDomain, for WebLogic Managed Servers wls_oaam2 and wls_oaam_admin2.

Validating OAAM on OAMHOST2

Validate the implementation by connecting to the OAAM Administration Server at `http://OAMHOST2.example.com:14200/oaam_admin`. The implementation is valid if OAAM Administration console login page is displayed and you can login using the `oaamadmin` account you created in Section, "[Creating OAAM Users and Groups in LDAP](#)."

Validate the implementation by connecting to the OAAM Server at: `http://OAMHOST2.example.com:14300/oaam_server` The implementation is valid if the OAAM Server login page is displayed.

Configuring OAAM to Work with Web Tier

This section describes how to configure Oracle Adaptive Access Manager to work with the Oracle HTTP Server.

Configuring Access from Oracle HTTP Server

You must include OAAM in the Web Tier configuration by updating the following files on WEBHOST1 and WEBHOST2:

Updating `IADADMIN.example.com`

Add the following to `OHS_ORACLE_INSTANCE/config/OHS/component_name/moduleconf/iadadmin_vh.conf`:

```
#####
```

```
## Entries Required by Oracle Adaptive Access Manager
```

```
#####
```

```
# OAAM Console
```

```
<Location /oaam_admin>
```

```
    SetHandler weblogic-handler
```

```
    WebLogicCluster OAMHOST1.example.com:14200,OAMHOST2.example.com:14200
```

```
</Location>
```

Updating `login.example.com`

Add the following to `OHS_ORACLE_INSTANCE/config/OHS/component_name/moduleconf/login_vh.conf`:

```
#####
```

```
## Entries Required by Oracle Adaptive Access Manager
```

```
#####
```



```
<Location /oaam_server>
```

```
SetHandler weblogic-handler
```

```
WebLogicCluster OAMHOST1.example.com:14300,OAMHOST2.example.com:14300
```

```
WLProxySSL ON
```

```
WLProxySSLPassThrough ON
```

```
</Location>
```

Restarting Oracle HTTP Servers and OAAM Managed Servers

Restart the Oracle HTTP Server on WEBHOST1 and WEBHOST2

Restart the managed servers wls_oaam1, wls_oaam2, wls_oaam_admin1, and wls_oaam_admin2

Changing Host Assertion in WebLogic

Because the Oracle HTTP Server acts as a proxy for WebLogic, by default certain CGI environment variables are not passed through to WebLogic. These include the host and port. You must tell WebLogic that it is using a virtual site name and port so that it can generate internal URLs appropriately.

To do this, log in to the WebLogic administration console in the IAMAccessDomain.

Then proceed as follows:

1. Select Clusters from the home page or, alternatively, select **Environment -> Clusters** from the Domain structure menu.
2. Click **Lock and Edit** in the Change Center Window to enable editing.
3. Click the Cluster Name (oaam_cluster).
4. Select HTTP and enter the following values:
 - o Frontend Host: login.example.com (IAM_LOGIN_URI)
 - o Frontend HTTP Port: 80 (HTTP_PORT)
 - o Frontend HTTPS Port: 443 (HTTP_SSL_PORT)

This ensures that any HTTPS URLs created from within WebLogic are directed to port 443 on the load balancer.

5. Click **Save**.
6. Select Clusters from the home page or, alternatively, select **Environment -> Clusters** from the Domain structure menu.
7. Click the Cluster Name (oaam_admin_cluster).
8. Select **HTTP** and enter the following values :
 - » **Frontend Host:** IADADMIN.example.com (IAD_DOMAIN_ADMIN_LBRVHN)
 - » **Frontend HTTP Port:** 80 (HTTP_PORT)
9. Click **Save**.

10. Click **Activate Changes** in the Change Center window to enable editing.

Validating Oracle Adaptive Access Manager

Log in to the Oracle Adaptive Access Management Administration console," using the oaadmin account.

Check that the following URL can be accessed:

https://login.example.com:443/oaam_server/oamLoginPage.jsp

Loading Oracle Adaptive Access Manager Seed Data


This section describes how to load seed data into Oracle Adaptive Access Manager.

NOTE: Either copy the files from OAMHOST1 to your local machine (where you are running the browser) or run this step from a browser started on OAMHOST1.

1. Log in to Oracle Adaptive Access Management Administration console
Connect using the oaadmin account.
2. Click System **Snapshots**, which is located on the Navigation -> **Environment** menu.
Click **Open**.
3. Click **Load From File**.
4. Enter the following information:
Name: Default Snapshot
Notes: Default Snapshot
Select **Backup Current System Now**.
Click **Continue**.
5. Click **OK** to acknowledge backup creation.
6. Click **Browse**.
7. Select the file oaam_base_snapshot.zip which is located in:
IAD_ORACLE_HOME/oaam/init
Click **open**.
8. Click **Load**.
9. You will see a message that says that the snapshot file was loaded successfully. Acknowledge this message by clicking **OK**.
10. Click **Restore** near the top right.
11. When loading is complete, a message is displayed. Click **OK**.

Integrating Oracle Adaptive Access Manager with Oracle Access Management Access Manager

This section describes how to integrate OAAM with Access Manager and Oracle Identity Manager. Once OAAM has been integrated with Access Manager, you can use OAAM instead of the standard Access Manager login to validate access to resources. Even though OAAM is performing the authentication, it is authenticating against users in Access Manager.



When OAAM is integrated with Oracle Identity Manager, Oracle Identity Manager is used to help users who have forgotten their username or password.

Retrieving the Global Passphrase for Simple Mode

Access Manager generates a random global passphrase for Simple mode communication during installation. The following procedure describes how to retrieve this passphrase. You will need it later in this chapter.

To retrieve the random global passphrase for Simple mode communication, on OAMHOST1 invoke the WebLogic Scripting Tool located in *IAD_ORACLE_HOME/common/bin*. Once you are in the wlst shell, enter the command to connect.

```
./wlst.sh
wls:/offline> connect()
```

Respond to the prompts as shown:

```
Please enter your username [weblogic] : weblogic
Please enter your password [weblogic] : COMMON_IDM_PASSWORD
Please enter your server URL [t3://localhost:7001] : t3://IADADMINVHN:7001
wls:/IAMAccessDomain/serverConfig>
```

Enter the following command to change the location to the read-only domainRuntime tree. For help, use `help(domainRuntime)`.

```
wls:/IAMAccessDomain/domainRuntime>domainRuntime()
```

View the global passphrase by entering the following command.

```
wls:/IAMAccessDomain/domainRuntime> displaySimpleModeGlobalPassphrase()
```

Make a note of this passphrase and exit wlst by using the exit command:

```
wls:/IAMAccessDomain/domainRuntime> exit()
```

Registering OAAM as a Third Party Application

If you have configured Access Manager to use the Simple Security Transportation protocol, you must register OAAM as a third-party application.

To register OAAM as a third-party application:

1. Create a directory to hold the OAAM Keystore. Placing this directory in the *IAD_ASERVER_HOME* ensures that it is available to all OAAM Hosts.

```
mkdir -p SHARED_CONFIG_DIR/keystores
```

2. From OAMHOST1, start the WLST shell from the *IAD_ORACLE_HOME/common/bin* directory. For example, on Linux, you would type:

```
./wlst.sh
```

3. Connect to the WebLogic Administration Server using the following wlst connect command:

```
connect('AdminUser', "AdminUserPassword", t3://hostname:port')
```

For example:

```
connect("weblogic", "admin_password", "t3://IADADMINVHN.example.com:7001")
```

4. Run the registerThirdPartyTAPPartner command as follows:

```
registerThirdPartyTAPPartner(partnerName = "partnerName", keystoreLocation= "path to keystore" ,  
password="keystore password", tapTokenVersion="v2.0", tapScheme="TAPScheme", tapRedirectUrl="OAAM login  
URL")
```

For example:

```
registerThirdPartyTAPPartner(partnerName = "OAAMTAPPartner", keystoreLocation= "  
SHARED_CONFIG_DIR/keystores/oaam_keystore.jks" , password="password", tapTokenVersion="v2.0",  
tapScheme="TAPScheme", tapRedirectUrl="https://login.example.com/oaam_server/oamLoginPage.jsp")
```

Where:

- » partnerName is a unique name. If the partner exists in Access Manager, the configuration will be overwritten.
- » keystoreLocation is an existing Key Store location. If the directory path you specified is not present, you get an error.
- » password is the password specified to encrypt the key store. Remember this, as you will need it later.
- » tapTokenVersion is always v2.0.
- » tapScheme is the authentication scheme to be updated.
- » tapRedirectUrl is a reachable URL. If it is not, registration fails with the message: Error! Hyperlink reference not valid.

tapRedirectUrl is:

```
https://login.example.com/oaam_server/oamLoginPage.jsp
```

5. Exit WLST.

```
exit()
```

6. Log in to the Access Management Administration Console
7. Click **Authentication Schemes** in the Access Manager section.

The Search Authentication Schemes Page is displayed.

Enter TAPScheme in the Search Name box and click **Search**.

8. Click **TAPScheme**.
9. Verify that the Challenge URL is set to:

```
/oaam_server/oamLoginPage.jsp
```

The parameters TAPPartnerId=OAAMTAPPartner and SERVER_HOST_ALIAS=OAMSERVER should already be listed as Challenge Parameters. Add the following Challenge Parameters:

```
MatchLDAPAttribute=uid
```


```
TAPOverrideResource=https://login.example.com:443/oamTAPAuthenticate
```

NOTE: For the parameter MatchLDAPAttribute, set the value to the username attribute specified in your identity store

10. Click **Apply**.
11. Restart wls_oaam1 and wls_oaam2

Adding an Agent Password to the IAMSuiteAgent Profile

When Access Manager is installed, the IAMSuiteAgent (Security Provider in WebLogic and corresponding 10g Webgate Profile in Access Manager) is created. By default there is no password set. In OAAM and Access Manager



integration using TAP, when OAAM connects to Access Manager, it uses the IAMSuiteAgent profile (configured while setting up TAP integration in OAAM using the OAAM CLI) and that connection requires an agent password.

You must set an agent password for the IAMSuiteAgent profile in Access Manager. It is a required step for Access Manager and Oracle Adaptive Access Manager integration since the password is used in multiple places. To set the password, proceed as follows:

1. Login to the Oracle Access Management console:
`http://iadadmin.example.com:IAD_HTTP_PORT/oamconsole`
2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. In the **Application Security** console, click **Agents** in the Agents section.
The Search SSO Agents page opens with the WebGates tab active.
4. In the Search SSO Agents page that appears, enter IAMSuiteAgent as the name of the agent you want to find.
5. Click the **Search** button to initiate the search.
6. Choose **IAMSuiteAgent** in the Search Results table and click **Edit**.
7. In the IAMSuiteAgent Webgate page, specify the password in the Access Client Password field and click **Apply** to save the changes.

Validation

Use the OAM Access Tester tool to ensure that this integration has been completed successfully.

To ensure the integration is completed successfully:

1. Ensure that JAVA_HOME is set in your environment.
2. Add JAVA_HOME/bin to your PATH, for example:
`export PATH=$JAVA_HOME/bin:$PATH`
3. Change directory to:
`IAD_ORACLE_HOME/oam/server/tester`

Start the test tool in a terminal window using the command:

```
java -jar oamtest.jar
```

4. Connect using the following values:
 - o **Primary OAM Host:** OAMHOST1
 - o **Port:** 5575 (*OAM_PROXY_PORT*)
 - o **Agent ID:** IAMSuiteAgent
 - o **Agent Password:** Password you assigned to the IAMSuiteAgent profile
 - o **Mode:** Select Open for AIX platforms. Otherwise, select Simple.
 - o **Global Passphrase:** If you selected Simple mode, enter the Access Manager global passphrase obtained in Section, "[Retrieving the Global Passphrase for Simple Mode](#)".



Click **Connect**.

5. Provide Protected Resource URI:

- o **Scheme:** http
- o **Host:** IAMSuiteAgent
- o **Port:** Leave blank
- o **Resource:** /oamTAPAuthenticate

Click **Validate**.

6. Provide User Identity oamadmin and the password for oamadmin.

Click **Authenticate**. If the authentication is successful, integration has been completed successfully.

Perform the same validation on OAMHOST2.

Setting OAAM properties for Access Manager

Set the OAAM properties for Access manager by editing the oaam_cli.properties file.

To set the OAAM properties on OAMHOST1:

1. Copy *IAD_ORACLE_HOME/oaam/cli* to a temporary location. For example:
`cp -r IAD_ORACLE_HOME/oaam/cli /u01/oracle/config/oaam`
2. Edit the file oaam_cli.properties, which is located in the directory:
/u01/oracle/config/oaam/conf/bharosa_properties.

Set the following property values in the file:

TABLE 7: OAAM PROPERTIES

Parameter	Value
oaam.adminserver.hostname	IADADMINVHN.example.com
oaam.adminserver.port	7001
oaam.adminserver.username	weblogic
oaam.adminserver.password	Password for the weblogic user
oaam.db.url	The DBC URL for the OAAM Database. Format:



	jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=IAMDBSCAN)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=oaamedg.example.com)))
<code>oaam.uio.oam.tap.keystoreFile</code>	The location of the keystore that was created in Section, "Registering OAAM as a Third Party Application." For example: IAD_ASERVER_HOME/keystores/oaam_keystore.jks
<code>oaam.uio.oam.tap.partnername</code>	OAAMTAPPartner
<code>oaam.uio.oam.host</code>	OAMHOST1
<code>oaam.uio.oam.port</code>	The Access Manager Server proxy port OAM_PROXY_PORT. For example: 5575.
<code>oaam.uio.oam.webgate_id</code>	IAMSuiteAgent
<code>oaam.uio.oam.secondary.host</code>	OAMHOST2
<code>oaam.uio.oam.secondary.host.port</code>	The Access Manager Server proxy port, OAM_PROXY_PORT, on the second Access Manager Server. For example: 5575.
<code>oaam.uio.oam.security.mode</code>	This depends on the Access Manager security transport mode in use. If this is an AIX build, then the value will be 1 (Open) otherwise it will be 2 (Simple).
<code>oam.uio.oam.rootcertificate.keystore.filepath</code>	The location of the Keystore file generated for the root certificate: IAD_ASERVER_HOME/output/webgate-ssl/oamclient-truststore.jks This is required only for security modes 2 (Simple) and 3 (Cert).
<code>oam.uio.oam.privatekeycertificate.keystore.filepath</code>	The location of the Keystore file generated for private key: IAD_ASERVER_HOME/output/webgate-ssl/oamclient-keystore.jks This is required for security modes 2 (Simple) and 3 (Cert).

Save the file

- Execute the OAAM CLI tool by issuing the command `setupOAMTapIntegration.sh`, which is located in the directory:

`/u01/oracle/config/oaam`

as follows:

Set `ORACLE_MW_HOME` to `IAD_MW_HOME`

Set `JAVA_HOME` to `JAVA_HOME`

Set `WLS_HOME` to `IAD_MW_HOME/wlserver_10.3`

Set `APP_SERVER_TYPE` to `weblogic`

Run the commands:

```
chmod +x /u01/oracle/config/oaam/setupOAMTapIntegration.sh
/u01/oracle/config/oaam/setupOAMTapIntegration.sh \
/u01/oracle/config/oaam/conf/bharosa_properties/oaam_cli.properties
```

When the command runs, it prompts you for the following information:

- » OAAM AdminServer User Name: weblogic_idm
- » OAAM AdminServer Password: Password for weblogic_idm account
- » OAAM DB username: EDG_OAAM.
- » OAAM DB password: Password for the OAAM database user.
- » OAM Webgate Credentials to be stored in CSF: Enter WebGate password (COMMON_IDM_PASSWORD).
- » OAM TAP Key store file password: The password you assigned when you registered OAAM as a 3rd party application in Section, "[Registering OAAM as a Third Party Application](#)" (COMMON_IDM_PASSWORD).
- » OAM Private Key certificate Key store file password: The Access Manager global passphrase obtained in Section, "[Retrieving the Global Passphrase for Simple Mode.](#)"
- » OAM Global Pass phrase: If you are using the OAAM Simple security model then this is the value retrieved in Section, "[Retrieving the Global Passphrase for Simple Mode.](#)"

Creating a Test Resource

To perform this validation, first create a test resource.

Note: Where Oracle Traffic Director is used, you can skip the step of creating a static HTML page. Unlike Oracle HTTP Server, displaying static HTML pages can be difficult. However, the purpose of creating this resource is to test OAAM.

Create a test page called oaam_sso.html on WEBHOST1 and WEBHOST2. The easiest way to do this is to create a file called oaam_sso.html in the directory WEB_ORACLE_INSTANCE/config/OHS/component/htdocs with the following:

```
<html>
<body>
<center>
<p>
<h2>
OAAM Protected Resource
</h2>
</p>
</center>
</body>
```



</html>

Creating Oracle Adaptive Access Manager Policies

Create a group for OAAM Protected resources in the IAMSuite Application Domain.

1. Log in to the Access Management Console, using the oamadmin account created previously
2. Click **Application Domains**.
3. Click **Search**.
4. Click **IAM Suite**. The IAM Suite Domain page is displayed.
5. Click the **Authentication Policies** tab.
6. Click **Create Authentication Policy** and enter the following information:
Name: OAAM Protected Resources
Description: Resources protected by OAAM
Authentication Scheme: TAPScheme
Click **Apply**.
7. Repeat Steps 1 through 7, but enter the following values after clicking Create Authentication Policy:
Name: LDAP Protected Resource
Description: Resources protected by LDAPScheme
Authentication Scheme: LDAPScheme


Creating a Resource in Access Manager

Now that you have something to protect, you must create a resource in Access Manager and assign it to one of the policy groups you just created.

1. Log in to the Access Management Console.
2. Click **Application Domains**.
3. Click **Search**.
4. Click **IAM Suite**.
5. Click the **Resources** tab.
6. Click **Create** and enter the following information:
Type: http
Description: OAAM Test Page
Host Identifier: IAMSuiteAgent
Resource URL: /oaam_sso.html
Protection Level: Protected
Authentication Policy: OAAM Protected Resources
Authorization Policy: Protected Resource Policy
Click **Apply**.

Validating Oracle Adaptive Access Manager

Access your protected resource using the URL: https://login.example.com:443/oaam_sso.html. You are redirected to OAAM for registration and challenge. The OAAM login page is shown instead of the Access Manager login page.



Log in using an authorized Access Manager user such as oamadmin. Once you are logged in, the oaam protected resource is displayed.

Note:

Where Oracle Traffic Director is used, once you have been through the OAAM authentication, an error appears showing "page not found." This is expected, you have not created the oaam_sso.html page merely created a policy to test authentication.

If you have an Oracle HTTP Server, you can easily create a simple HTML page. This is possible in Oracle Traffic Director, but is complicated. If you are presented with an OAAM challenge when trying to access the resource, and you pass that validation, that is sufficient to validate OAAM. Whether or not a simple HTML page is displayed at the end is not relevant and does not invalidate the test.

Moving TAP Resource to LDAP Policy

1. Log in to the Access Management Console, using the oamadmin account created previously.
2. Click on **Application Domains** under the Access Manager section.
3. The **Application Domains** Search screen appears.
4. Click **Search**.
5. Click on **IAM Suite** to bring up the IAM Suite Domain page.
6. Click on the **Authentication Policies** subtab.
7. Click **Protected Higher Level Policy**.
8. Click on the **Resources** subtab.
9. In the Resources window click **/oamTAPAuthenticate**.
10. Click **Delete**.
11. Click **Apply**.
12. Click on **Application Domains** under the Access Manager section.
13. The Application Domains Search screen appears.
Click **Search**.
14. Click on **IAM Suite** to bring up the IAM Suite Domain page.
Click on the Authentication Policies subtab.
15. Click LDAP Protected Resources.
Click **Open** on the tool bar below the Browse tab.
16. In the Resources window, click **Add**.
When the Search box appears enter:
Resource URL: /oamTAPAuthenticate
Click **Search**.
17. Click on /oamTAPAuthenticate from the search results.
18. Click **Add Selected**.
19. Select the resource /oamTAPAuthenticate.
20. Click **Apply**.

Integrating Oracle Adaptive Access Manager with Oracle Identity Manager

OAAM provides a comprehensive set of challenge questions. Its functionality includes:

- » Challenging the user before and after authentication, as required, with a series of questions.
- » Presenting the questions as images and seeking answers through various input devices.
- » Asking questions one after another, revealing subsequent questions only if correct answers are provided.

Oracle Identity Manager also has basic challenge question functionality. It enables users to answer a set of configurable questions and reset their password if they forgot the password. Unlike OAAM, Oracle Identity Manager also has a rich set of password validation capabilities, and it enables policies to be set based on the accounts owned, in addition to simple attributes.

In an Identity and Access Management deployment, best practice is to register only a single set of challenge questions, and to use a single set of password policies. OAAM can be integrated with Oracle Identity Manager so that OAAM provides the challenge questions and Oracle Identity Manager provides password validation, storage and propagation. This enables you to use OAAM fraud prevention at the same time you use Oracle Identity Manager for password validation. When OAAM is integrated with Oracle Identity Manager, Oracle Identity Manager is used to help users who have forgotten their username or password.

Configuring Oracle Identity Manager Encryption Keys in CSF

1. Go to Oracle Enterprise Manager Fusion Middleware Control for the domain IAMAccessDomain
2. Log in using the WebLogic administrator account, for example weblogic_idm.
Expand the WebLogic Domain icon in the navigation tree in the left pane.
3. Select the **IAMAccessDomain**, right click, and select the menu option **Security** and then the option **Credentials** in the sub menu.
4. Click **oaam** to select the map and then click **Create Key**.

In the pop-up window, ensure Select Map is **oaam**.

Enter:

Key Name: oim.credentials

Type: Password

UserName: xelsysadm

Password: Password for xelsysadm account, COMMON_IDM_PASSWORD

Click **OK** to save the secret key to the Credential Store Framework.

Configuring Cross Domain Trust Between Oracle Identity Manager and Oracle Adaptive Access Manager

When you are deploying Oracle Adaptive Access Manager, and Oracle Identity Manager and Oracle Adaptive Access Manager are in separate domains, you must configure cross-domain trust.

Configure cross-domain trust in the domain IAMAccessDomain, as follows:

1. Log in to WebLogic Administration Console in IAMAccessDomain.
2. Click **Lock and Edit**.

3. Click **IAMAccessDomain** in Domain Structure and select the **Security** tab.
4. Expand the **Advanced** section.
5. Select **Cross domain security enabled**.
6. Choose a password to be used to confirm cross domain trust and type it in the **Credential** and **Confirm Credential** fields.
7. Click **Save**.
8. Click **Activate Changes**.

Configure Cross-Domain Trust in the domain IAMGovernanceDomain, as follows:

1. Log in to WebLogic Administration Console in IAMGovernanceDomain.
2. Click **Lock and Edit**.
3. Click **IAMGovernanceDomain** in Domain Structure and select the **Security** tab.
4. Expand the **Advanced** section.
5. Select **Cross domain security enabled**.
6. Enter the password you entered into the credential fields of the IAMAccessDomain in the **Credential** and **Confirm Credential** fields.
7. Click **Save**.
8. Click **Activate Changes**.

Setting Oracle Adaptive Access Manager Properties for Oracle Identity Manager

Go to the OAAM Administration Console

Log in using the oaamadmin account you created in Section, "[Creating OAAM Users and Groups in LDAP](#)."

Then proceed as follows:

1. In the navigation tree, click **Properties** under the Environment heading and then click **Open**. The properties search page is displayed.
2. To set a property value, enter its name in the **Name** field and click **Search**. The current value is shown in the search results window.
3. Click the entry. The Value field is displayed. Enter the new value and click **Save**.
4. Set the following properties to enable Oracle Adaptive Access Manager to integrate with Oracle Identity Manager:
 - **bharosa.uio.default.user.management.provider.classname:**
com.bharosa.vcrypt.services.OAAMUserMgmtOIM
 - **bharosa.uio.default.signon.links.enum.selfregistration.url:**
https://login.example.com:443/identity/faces/register?&backUrl=https://login.example.com:443/identity
 - **bharosa.uio.default.signon.links.enum.trackregistration.enabled:** true
 - **bharosa.uio.default.signon.links.enum.selfregistration.enabled:** true
 - **bharosa.uio.default.signon.links.enum.trackregistration.url:**
https://login.example.com:443/identity/faces/trackregistration?&backUrl=https://login.example.com:443/identity
 - **oaam.oim.url:** t3://oimhost1vhn.example.com:14000,oimhost2vhn.example.com:14000

Setting Oracle Identity Manager Properties for OAAM

1. Log in to the Oracle Identity Manager System Administration Console
2. Click **Configuration Properties** under the System Configuration heading. The Configuration Properties window opens.
3. Click **Search** in Search System Properties.
4. Click each of the properties shown, then select Edit. Set the value of each property as shown and click **Save** to save the value.

Note:

The property name appears in the keyword column.

- **OIM.DisableChallengeQuestions**: TRUE
- **OIM.ChangePasswordURL**: https://login.example.com:443/oaam_server/oimChangePassword.jsp
- **OIM.ChallengeQuestionModificationURL**:
https://login.example.com:443/oaam_server/oimResetChallengeQuestions.jsp

Restarting IAMAccessDomain and IAMGovernanceDomain

Restart the following Administration servers and managed servers

- » WebLogic Administration Servers
- » wls_oam1 and wls_oam2
- » wls_oim1 and wls_oim2
- » wls_oaam1 and wls_oaam2


Changing Domain to Oracle Adaptive Access Manager Protection

If you want to protect certain resources with OAAM, you can do so by adding the OAAM Protected Resources Authentication Policy created in Section , "[Creating a Resource in Access Manager](#)."

TO use OAAM authentication for everything:

1. Log in to the Access Management Console.
2. Click **Application Domains**.
3. Click **Search**.
4. Click **IAM Suite**.
5. Click the **Authentication Policies** tab.
6. Click on the policy **Protected HigherLevel Policy**.
7. Change the value of **Authentication Scheme** to TAPScheme.
8. Click **Apply**.

Validating OAAM - Oracle Identity Manager Integration



Access the test page you created above, for example: https://login.example.com/oaam_sso.html. You will be presented with the OAAM login page. Click on the links Registration or Track Registration. If integration is working you will be directed to OIM.

Note: Due to a bug, the OAAM Authentication image is not rendered properly if both OAAM servers are running. To work-around the issue, only one OAAM managed server should be running. The issue occurs only when the MW_HOME is shared by managed servers.

Validating Oracle Identity Manager-OAAM Integration

Validate that Oracle Identity Manager is integrated with OAAM as follows:

Log in to the Oracle Identity Manager Self Service Console as the xelsysadm user.

You are prompted to set up challenge questions and OAAM-specific security pictures.

Backing Up the Application Tier Configuration

Conclusion

Having followed the above configuration steps, you will have built an identity management application suitable for use in a typical enterprise.







Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615

White Paper Extending Identity and Access Management Enterprise Deployment with Oracle Adaptive Access Manager
July 2016
Author: Michael Rhys
Contributing Authors: Firdaus Fraz