ORACLE®
Instantis

EnterpriseTrack

EnterpriseTrack OAM Configuration Guide
Version 17

June 2018

Contents

About Configuring Oracle Access Manager

Oracle Access Manager (OAM) is used as the SAML Service Provider for EnterpriseTrack and enables you to use single sign-on (SSO).

Prerequisites

You must do the following before configuring Instantis EnterpriseTrack for SSO:

- Install Oracle HTTP Server (OHS). For more information, see http://docs.oracle.com/middleware/1213/core/WTINS/toc.htm
- Install Oracle Access Manager (OAM) For more information, see ***http://docs.oracle.com/cd/E52734_01/core/INOAM/toc.htm http://docs.oracle.com/cd/E52734_01/core/INOAM/toc.htm***
- Install Oracle HTTP Server 11g WebGate for OAM, see http://docs.oracle.com/cd/E40329_01/doc.1112/e49451/webgate_ohs.htm#CACEAEIE

In This Section

Configuring Oracle HTTP Server WebGate

After installing WebGate, you must configure the Oracle HTTP Server WebGate as follows:

1) Ensure that <Webgate_Home> is under the Oracle Home for Oracle Web Tier <MW_HOME>.
   Where: <Webgate_Home> is the Webgate Home directory. For example, /u01/app/Oracle/Middleware/Oracle_OAMWebGate1.
   <MW_HOME> is oracle middleware home directory, For example, /u01/app/Oracle/Middleware
2) Go to `<Webgate_Home>/webgate/ohs/tools/deployWebGate`.
3) Run the following:
   `deployWebgateInstance.sh -w <Webgate_Instance_Directory> -oh <Webgate_Oracle_Home>`
   where:<Webgate_Instance_Directory> is the location of Webgate Instance Home
   <Webgate_Oracle_Home> is the directory where Oracle HTTP Server Webgate is installed and created as the Oracle Home for Webgate.
   For example, run the following: deployWebgateInstance.sh -w <MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1 -oh <MW_HOME>/Oracle_OAMWebGate1
4) Ensure that the `LD_LIBRARY_PATH` variable contains `<Oracle_Home_for_Oracle_HTTP_Server>/lib`.

If not set, run the following command:

```
export LD_LIBRARY_PATH=<Oracle_Home_for_Oracle_HTTP_Server>/lib
```

For example, `export LD_LIBRARY_PATH=<MW_Home>/Oracle_WT1/lib`

5) Go to `<Webgate_Home>/webgate/ohs/tools/EditHttpConf`.
6) Run the following:

   ```
   ./EditHttpConf -w <Webgate_Instance_Directory> [-oh
   <Webgate_Oracle_Home>] [-o<output_file>]
   ```

   For example, run the following: `./EditHttpConf.sh -w <MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1 -oh <MW_HOME>/Oracle_OAMWebGate1 -o Edithttpconf.log`

Registering Agents for Oracle Access Manager Server

Note: Ensure that you register the OAM server with a fully qualified hostname (for example, OAM_Server.us.oracle.com).

To register agents for OAM:

1) Log in to the **Oracle Access Manager Administration** Console.
2) Click the **Launch Pad** tab.
3) On the **Welcome to Oracle Access Managemen**t page, under **Access Manager**, click **SSO Agent**.
4) On the **Search SSO Agents** page, click **Create 11g Webgate**.
5) On the **Create OAM 11g Webgate** screen:
   a. In the **Name** field, enter a unique name to identify this server. Oracle recommends that this name matches the WebLogic Domain Name.
   b. In the **Base URL** field, enter the URL for the Oracle HTTP Server. You must use a fully qualified host name. You can confirm this in the Installation Summary text file that was saved when the OHS server was created.
   c. In the **Host Identifier** field, enter the host name of the server running Oracle HTTP Server.
   d. Click **Apply**. A detailed page is displayed after the OAM 11g Webgate is created.
6) On the detailed page for OAM 11g Webgate:
   a. Note the location where the artifacts are generated. This is displayed in the confirmation message.
   b. In the field **Cache Control Header**, remove the default value **no-cache**.
   c. Click **Apply**.
7) Copy the files generated by the OAM console to the OHS domain:

a. On the Oracle Access Management Server (OAM), navigate to: `<MW_HOME>/user_projects/domains/<OAM Domain>/output/<name>/` (This is the path from step 6.)

b. Copy the files into the OHS configuration stage location on the OHS Server. For example: `<OHS_DOMAINHOME>/config/fmwconfig/components/OHS/ohs1/`

8) Restart the OHS Server (Application Server).

a. Navigate to the OHS Server's Domain Home/bin folder: `<OHS_DOMAINHOME>/bin`

b. Stop and Start the services with the following commands:

```
./stopComponent.sh ohs1
./stopNodeManager.sh
./startNodeManager.sh
./startComponent.sh ohs1
```

Enabling the Oracle Identify Federation Services

In This Section

Enabling Identity Federation Service

To manage the Identity Federation Services with Access Manager:

1) From the **Oracle Access Management Console**, click the **Configuration** tab.
2) Click to **Enable** next to **Identity Federation**. Confirm that a green status check mark ✓ is displayed.
3) Click **Enable** next to **Access Manager**. Confirm that a green status check mark ✓ is displayed.

Configure Federation Settings

To set or modify the general settings for Federation:

1) From the **Oracle Access Management Console**, click the **Configuration** tab.
2) From the **Settings** drop-down list, select **Federation**.
3) On the **Federation Settings** page, complete the **General** section with settings values for your environment.
4) Click **Apply**.

Exporting Metadata

After configuring the general settings, you can export the metadata for use by federation partners.

In This Section

Exporting SAML 2.0 Metadata

To export the metadata:

1) From the **Oracle Access Management Console**, click the **Configuration** tab.
2) From the **Settings** drop-down list, select **Federation**.
3) On the **Federation Settings** page, click **Export SAML 2.0 Metadata**.
4) In the dialog box, specify the file for the exported metadata.
5) Click **Save** to save your new metadata file.

Creating a New Identity Provider and Configuring the Authentication Scheme

Use the **New Identity Provider** page to define an identity provider partner record for Access Manager. You can specify service details manually or load them from a metadata file.

To define a new SAML 2.0 identity provider (IdP):

1) From the **Oracle Access Management** console, click the **Federation** tab.
2) From the **Identity Federation** section, click **Service Provider Administration**.
3) On the **Service Provider Administration** page, click **Create Identity Provider Partner**.
4) On the **Create Identity Provider Partne**r page, under the **Service Information** section, enter the following:
   a. For the **Service Details** field, check the radio button **Load from provider metadata**.
   b. For the **Metadata File** field, click **Browse** and select the metadata file of the IdP.
   c. Click **Save** to create the Identity Provider definition.
5) Click **Create Authentication Scheme and Module** to create a new federation scheme associated with the IdP for use with Instantis EnterpriseTrack application.

Registering the Instantis Application SSO Agent

Register the Instantis EnterpriseTrack application domains and policies that protect resources.

Register SSO Agent

To register the SSO agent:

1) From the **Oracle Access Management** console, click the **Application Security** tab.
2) From the **SSO Agent Registration** page, under **Agent Type**, choose **Webgate**.
3) Click **Next**.
4) From the **Version** drop-down menu, select **11g**.
5) Enter a unique name for the webgate agent.
6) In the **Protected Resource List** field, add the relative SSO URL to be protected, for example: `/SiteWand/Submission/etrack/SSOLogin` for Instantis EnterpriseTrack
7) In the **Public Resource List** field, add the relative URL `/SiteWand/**` as unprotected resource.
8) Click **Finish**.
9) Click **Apply**.

Creating an Authentication Policy

To create an authentication policy:

1) From the **Oracle Access Management** console, click the **Application Security** tab.
2) From the **Access Manager** section, click **Application Domains**.
3) Click **Search**. The search displays an application domain with the same name as the SSO agent created in the previous section.
4) From the **Authentication Policies** tab, select the generated domain name.
5) Click on the **Protected Resources Policy** link.
    a. From the **Authentication Scheme** drop-down list, select the scheme you created when creating the Identity Provider Partner. See topic *Creating a New Identity Provider and Configuring the Authentication Scheme*.
    b. Click **Apply**.
6) From the **Protected Resource Policy** page, click the **Responses** tab:
    a. Click ✚ to add a new entry.
    b. In the **Type** field, select **Header**.
    c. In the **Name** field, enter **REMOTE_USER**.
    d. In the **Value** field, enter **$user.userid**.
    e. Click **Add**.
    f. Click **Apply**.

Creating an Authorization Policy

To create an authorization policy:

1) From the same **Application Domains** page, click on the **Authorization Policies** tab.
2) Click the **Protected Policies** link.
3) From the **Protected Resource** page, click the **Responses** tab:
    a. Click ✚ to add a new entry.
    b. In the **Type** field, select **Header**.
    c. In the **Name** field, enter **REMOTE_USER**.

   d. In the **Value** field, enter **$user.userid**.
   e. Click **Add**.

4) Click **Apply**.

Enabling/Disabling User Provisioning

To enable or disable user provisioning in the OAM/Service Provider's embedded local IdP server:

1) To enter the WLST environment, execute the following command:
   `$IAM_ORACLE_HOME/common/bin/wlst.sh`
2) To connect to the WLS Admin server, enter:
   `connect()`
3) To navigate to the Domain Runtime branch, enter:
   `domainRuntime()`
4) Update the **userprovisioningenabled** property:
   - To enable User Provisioning in OIF/SP, enter:

     ```
     putBooleanProperty("/fedserverconfig/userprovisioningenabled",
     "true")
     ```

   - To disable User Provisioning in OIF/SP, enter:

     ```
     putBooleanProperty("/fedserverconfig/userprovisioningenabled",
     "false")
     ```

5) To exit the WLST environment, enter:

   ```
   exit()
   ```

Configuring the Default User Authentication Mode

Use the *Default User Authentication Mode* page to set SSO as the default authentication mode for all users. The user authentication mode describes how users will log into the system and how user credentials are authenticated. If you select **SSO**, administrators can still configure some users to use a password.

To set the default user authentication mode:

1) Click the **Deployment Options** tab.
2) Click the **Default User Authentication Mode** link.
3) Click **Edit Authentication Mode**.
4) From the **Value** drop-down menu, select the default **SSO** as the user authentication mode.
5) Click **Update**.
6) When changing modes, select how you want existing user accounts to be handled and click **Update**.
7) If you selected SSO:

a. Enter the **SSO Login URL** in the following format:
`https://hostname/SiteWand/Submission/<account name>/SSOLogin`
For example:
`https://example.company.com/SiteWand/Submission/etrack/SSOLogin`

b. Enter the **SSO Logout URL** in the following format:
`https://hostname/SiteWand/Submission/<account name>/SSOLogout`
For example:
`https://example.company.com/SiteWand/Submission/<etrack/SSOLogout`

c. Use the default value for **SSO Public Key for RSA.**

d. Us the default value for **SSO Authentication Token Name**.

e. Enter the **Authentication Host** in the following format: `https://hostname`

f. Enter the **Authentication Type**. Leave this field blank if you are using OAM as your SAML service provider. Contact Oracle Support for more information on the authentication type if you use other SAML service provider software.

g. Click **Update**.

> **Note:** You must configure the default user authentication mode for sys_admin and tmp_admin to use User Password and not SSO.

Legal Notices

Oracle Instantis EnterpriseTrack EnterpriseTrack OAM Configuration Guide

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information on content, products and services from third-parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.