Oracle® Fusion Middleware
Installing WebGates for Oracle Access Manager
Contents

Preface

Audience v
Documentation Accessibility v
Related Documents v
Conventions vi

1 About WebGates for Oracle Access Manager

2 Configuring Oracle HTTP Server WebGate for Oracle Access Manager

About Oracle HTTP Server Webgate 2-1
General Prerequisites for Configuring Oracle HTTP Server Webgate 2-1
Configuring Oracle HTTP Server WebGate 2-2
Registering the Oracle HTTP Server 12c WebGate with Oracle Access Manager 2-3
  Locating and Preparing the RREG Tool 2-3
  Updating the Standard Properties in the OAM11gRequest.xml File 2-4
Running the RREG Tool 2-7
  About RREG In-Band and Out-of-Band Mode 2-7
  Running the RREG Tool in In-Band Mode 2-8
  Running the RREG Tool in Out-Of-Band Mode 2-9
Files and Artifacts Generated by RREG 2-10
Copying Generated Artifacts to the Oracle HTTP Server WebGate Instance Location 2-11
Restarting the Oracle HTTP Server Instance 2-14

3 Configuring Oracle Traffic Director WebGate for Oracle Access Manager

Prerequisites for Configuring Webgate 3-1
Configuring Oracle Traffic Director 12c WebGate 3-2
Verifying the Configuration of Oracle Traffic Director 12c WebGate 3-4
Getting Started with a New Oracle Traffic Director 12c WebGate 3-4
Registering the New Oracle Traffic Director 12c WebGate 3-5
   Setting Up the RREG Tool 3-5
   Updating the OAM11gRequest.xml File 3-6
Using the In-Band Mode 3-7
Using the Out-Of-Band Mode 3-7
Files and Artifacts Generated by RREG 3-9
Copying Generated Files and Artifacts to the Oracle Traffic Director WebGate Instance Location 3-10
   Generating a New Certificate 3-10
   Migrating an Existing Certificate 3-11
Restarting the Oracle Traffic Director Instance 3-11

4   Adding Trusted Certificate for SIMPLE and CERT Mode communication

5   Upgrading to OHS/OTD 12c WebGate
Preface

This Preface provides supporting information for Oracle Fusion Middleware Installing WebGates for Oracle Access Manager and includes the following topics:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions
- Audience
- Documentation Accessibility
- Related Documents
- Conventions

**Audience**

The Oracle Fusion Middleware Installing WebGates for Oracle Access Manager guide is intended for administrators that are responsible for installing 12c WebGates for Oracle Access Manager. This document assumes you have experience installing enterprise components. Basic knowledge about Oracle Access Manager, WebGates, and Oracle Application Server is recommended.

**Documentation Accessibility**

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

**Access to Oracle Support**

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

**Related Documents**

For more information, see the following documents in the Oracle Identity and Access Management 11g Release 2 (11.1.2) documentation library:

- Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management
Conventions

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><em>monospace</em></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
1

About WebGates for Oracle Access Manager

A WebGate is a web-server plug-in for Oracle Access Manager (OAM) that intercepts HTTP requests and forwards them to the Access Server for authentication and authorization.

For information about the typical workflow in an environment with a WebGate and Oracle Access Manager, see About SSO Log In Processing with OAM Agents in Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service.

This document contains the following chapters:

• Configuring Oracle HTTP Server WebGate for Oracle Access Manager
• Configuring Oracle Traffic Director WebGate for Oracle Access Manager
• Adding Trusted Certificate for SIMPLE and CERT Mode communication
• Upgrading to OHS/OTD 12c WebGate

ORACLE
Configuring Oracle HTTP Server WebGate for Oracle Access Manager

Configuring Oracle HTTP Server WebGate for Oracle Access Manager involves several steps.

The chapter contains the following sections:

- About Oracle HTTP Server Webgate
- General Prerequisites for Configuring Oracle HTTP Server Webgate
- Configuring Oracle HTTP Server WebGate
- Registering the Oracle HTTP Server 12c WebGate with Oracle Access Manager

About Oracle HTTP Server Webgate

Oracle HTTP Server WebGate is a Web server plug-in that intercepts HTTP requests and forwards them to an existing Oracle Access Manager instance for authentication and authorization.

General Prerequisites for Configuring Oracle HTTP Server Webgate

Before you can configure Oracle HTTP Server WebGate, you must have installed and configured a certified version of Oracle Access Manager.

At the time this document was published, the supported version was Oracle Access Manager 12c Release 2 (12.2.1.1). For the most up-to-date information, see the certification document for your release on the Oracle Fusion Middleware Supported System Configurations page.
Configuring Oracle HTTP Server WebGate

Configuring Oracle HTTP Server WebGate for Oracle Access Manager requires several steps.

In the following examples:

- Replace `OHS_ORACLE_HOME` with the complete path to the Oracle home where you installed the Oracle HTTP Server software.
- Replace `OHS_CONFIG_DIR` with the path to the following location in the Oracle HTTP Server domain home:
  
  \`DOMAIN_HOME/config/fmwconfig/components/OHS/ohs_instance_name\`

1. Navigate to the `deployWebGate` directory in the Oracle HTTP Server Oracle home:
   
   (UNIX) cd `OHS_ORACLE_HOME/webgate/ohs/tools/deployWebGate`
   
   (Windows) cd `OHS_ORACLE_HOME/webgate/ohs\tools\deployWebGate`

2. Run the following command to create the WebGate Instance directory and enable WebGate logging on OHS Instance:
   
   (UNIX) `./deployWebGateInstance.sh -w OHS_CONFIG_DIR -oh OHS_ORACLE_HOME`
   
   (Windows) `deployWebGateInstance.bat -w OHS_CONFIG_DIR -oh OHS_ORACLE_HOME`

3. Verify that a `webgate` directory and subdirectories was created by the `deployWebGateInstance` command:
   
   For example, on UNIX:
   
   ```
   ls -lart OHS_CONFIG_DIR/webgate/
   total 6
   drwxr-x---+ 8 orcl oinstall 20 Oct  2 07:14 ..
   drwxr-xr-x+ 4 orcl oinstall  4 Oct  2 07:14 .
   drwxr-xr-x+ 3 orcl oinstall  3 Oct  2 07:14 tools
   drwxr-xr-x+ 3 orcl oinstall  4 Oct  2 07:14 config
   ```

4. Run the following command to set the path environment variable:
   
   (UNIX) `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:OHS_ORACLE_HOME/lib`
   
   (Windows) `set PATH=%PATH%;OHS_ORACLE_HOME\bin`

5. Navigate to the `EditHttpConf` directory:
(UNIX) cd OHS_ORACLE_HOME/webgate/ohs/tools/setup/InstallTools/EditHttpConf
(Windows) cd OHS_ORACLE_HOME\webgate\ohs\tools\InstallTools/EditHttpConf

6. Run the following command:

(UNIX) ./EditHttpConf -w OHS_CONFIG_DIR [-oh OHS_ORACLE_HOME] [-o output_file_name] [-dcc custom_dcc_scripts/pages_location]
(Windows) EditHttpConf -w OHS_CONFIG_DIR [-oh OHS_ORACLE_HOME] [-o output_file_name] [-dcc custom_dcc_scripts\pages_location]

This command does the following:

- Copies the apache_webgate.template file from the Oracle HTTP Server Oracle home to a new webgate.conf file in the Oracle HTTP Server configuration directory.
- Updates the httpd.conf file to add one line, so it includes the webgate.conf.
- Generates a WebGate configuration file. The default name of the file is webgate.conf, but you can use a custom name by using the output_file argument to the command.

If you want to customize Detached Credential Collector (DCC) scripts or pages, such as the oamsso/logout.html, oamsso-bin/login.p, or logout.pll scripts), then you can copy these scripts from the following location to the custom location identified by the -dcc parameter to EditHttpConf utility:

ORACLE_HOME/webgate/ohs/

Registering the Oracle HTTP Server 12c WebGate with Oracle Access Manager

You can register the WebGate agent with Oracle Access Manager using the Oracle Access Manager Administration console.

See Registering an OAM Agent Using the Console in Administrator’s Guide for Oracle Access Management.

- Locating and Preparing the RREG Tool
- Updating the Standard Properties in the OAM11gRequest.xml File
- Running the RREG Tool
- Files and Artifacts Generated by RREG
- Copying Generated Artifacts to the Oracle HTTP Server WebGate Instance Location
- Restarting the Oracle HTTP Server Instance

Locating and Preparing the RREG Tool

To set up the RREG tool, complete the following steps:

1. Log in to one of the Oracle Access Manager hosts in the Application tier.
2. Change directory to the following directory in the Oracle Access Manager Oracle home:
The location is required only for the out-of-band mode.

OAM_ORACLE_HOME/oam/server/rreg/client

In this example, OAM_ORACLE_HOME refers to the Oracle home on the system where the Oracle Access Manager software was installed.

If the Oracle Enterprise Deployment Guide for IDM was used, OAM_ORACLE_HOME may be /u01/oracle/products/access/iam.

If you do not have privileges or access to the Oracle Access Manager server, then you can use out-of-band mode to generate the required files and register the WebGate with Oracle Access Manager. See About RREG In-Band and Out-of-Band Mode.

3. Unzip the RREG.tar.gz file to the required directory.

4. From the unzipped directory, open the oamreg.sh file and set the following environment variables in the file, as follows:
   - Set OAM_REG_HOME to the absolute path to the directory in which you extracted the contents of RREG archive.
   - Set JAVA_HOME to the absolute path of the directory in which a supported JDK is installed on your machine.

Updating the Standard Properties in the OAM11gRequest.xml File

Before you can register the Webgate agent with Oracle Access Manager, you must update some required properties in the OAM11gRequest.xml file.

If you plan to use the default values for most of the parameters in the provided XML file, then you can use the shorter version (OAM11gRequest_short.xml, in which all non-listed fields will take a default value.)
To perform this task:

1. If you are using in-band mode, then change directory to the following location on one of the OAM Servers:
   
   `OAM_ORACLE_HOME/oam/server/rreg/input`

   If you are using out-of-band mode, then change directory to the location where you unpacked the RREG archive on the WEBHOST1 server.

2. Make a copy of the OAM11GRequest.xml file template with an environment-specific name.
   
   `cp OAM11GRequest.xml OAM11GRequest_edg.xml`

3. Review the properties listed in the file, and then update your copy of the OAM11GRequest.xml file to make sure the properties reference the host names and other values specific to your environment.

<table>
<thead>
<tr>
<th>OAM11gRequest.xml Property</th>
<th>Set to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>serverAddress</td>
<td>The host and the port of the Administration Server for the Oracle Access Manager domain.</td>
</tr>
<tr>
<td>agentName</td>
<td>Any custom name for the agent. Typically, you use a name that identifies the Fusion Middleware product you are configuring for single sign-on.</td>
</tr>
<tr>
<td>applicationDomain</td>
<td>A value that identifies the Web tier host and the FMW component you are configuring for single sign-on.</td>
</tr>
</tbody>
</table>
**OAM11gRequest.xml Property** | **Set to...**
--- | ---
security | Must be set to the security mode configured on the Oracle Access Management server. This will be one of three modes: open, simple, or certificate.

Note:

For an enterprise deployment, Oracle recommends simple mode, unless additional requirements exist to implement custom security certificates for the encryption of authentication and authorization traffic.

In most cases, avoid using open mode, because in open mode, traffic to and from the Oracle Access Manager server is not encrypted.

For more information using certificate mode or about Oracle Access Manager supported security modes in general, see Securing Communication Between OAM Servers and WebGates in the *Administrator's Guide for Oracle Access Management*.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cachePragmaHeader</td>
<td>private</td>
</tr>
<tr>
<td>cacheControlHeader</td>
<td>private</td>
</tr>
<tr>
<td>ipValidation</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>&lt;ipValidation&gt;0&lt;/ipValidation&gt;</td>
</tr>
<tr>
<td>ipValidationExceptions</td>
<td>The IP address of the front-end load balancer. For example: &lt;ipValidationExceptions&gt; &lt;ipAddress&gt;130.35.165.42&lt;/ipAddress&gt; &lt;/ipValidationExceptions&gt;</td>
</tr>
<tr>
<td>agentBaseUrl</td>
<td>Fully-qualified URL with the host and the port of the front-end Load Balancer VIP in front of the WEBHOSTn machines on which Oracle HTTP 12c WebGates are installed. For example: &lt;agentBaseUrl&gt; <a href="https://soa.example.com:443">https://soa.example.com:443</a> &lt;/agentBaseUrl&gt;</td>
</tr>
<tr>
<td><strong>OAM11gRequest.xml Property</strong></td>
<td><strong>Set to</strong>...</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>virtualHost</td>
<td>Set to true when protecting more than the agentBaseUrl, such as SSO protection for the administrative VIP.</td>
</tr>
<tr>
<td>hostPortVariationsList</td>
<td>Add hostPortVariation host and port elements for each of the load-balancer URLs that will be protected by the WebGates. For example:</td>
</tr>
</tbody>
</table>

```xml
<hostPortVariationsList>
  <hostPortVariations>
    <host>soainternal.example.com</host>
    <port>80</port>
  </hostPortVariations>
  <hostPortVariations>
    <host>admin.example.com</host>
    <port>80</port>
  </hostPortVariations>
  <hostPortVariations>
    <host>osb.example.com</host>
    <port>443</port>
  </hostPortVariations>
</hostPortVariationsList>
```

## Running the RREG Tool

The following topics provide information about running the RREG tool to register your Oracle HTTP Server Webgate with Oracle Access Manager.

- About RREG In-Band and Out-of-Band Mode
- Running the RREG Tool in In-Band Mode
- Running the RREG Tool in Out-Of-Band Mode

### About RREG In-Band and Out-of-Band Mode

You can run the RREG Tool in one of two modes: in-band and out-of-band.

**Use in-band** mode when you have the privileges to access the Oracle Access Manager server and run the RREG tool yourself from the Oracle Access Manager Oracle home. You can then copy the generated artifacts and files to the Web server configuration directory after you run the RREG Tool.

**Use out-of-band** mode if you do not have privileges or access to the Oracle Access Manager server. For example, in some organizations, only the Oracle Access Manager server administrators have privileges access the server directories and perform administration tasks on the server. In out-of-band mode, the process can work as follows:

1. The Oracle Access Manager server administrator provides you with a copy of the RREG archive file (RREG.tar.gz).
   The server administrator can find it in the location described in **Updating the Standard Properties in the OAM11gRequest.xml File**.
2. Untar the RREG.tar.gz file that was provided to you by the server administrator.
   
   For example:
   
   ```bash
gunzip RREG.tar.gz
   tar -xvf RREG.tar
   ```
   
   After you unpack the RREG archive, you can find the tool for registering the agent in the following location:
   
   ```bash
RREG_HOME/bin/oamreg.sh
   ```
   
   In this example, RREG_HOME is the directory in which you extracted the contents of RREG archive.

3. Use the instructions in Updating the Standard Properties in the OAM11GRequest.xml File to update the OAM11GRequest.xml file, and send the completed OAM11GRequest.xml file to the Oracle Access Manager server administrator.

4. The Oracle Access Manager server administrator then uses the instructions in Running the RREG Tool in Out-Of-Band Mode to run the RREG Tool and generate the AgentID_response.xml file.

5. The Oracle Access Manager server administrator sends the AgentID_response.xml file to you.

6. Use the instructions in Running the RREG Tool in Out-Of-Band Mode to run the RREG Tool with the AgentID_response.xml file and generate the required artifacts and files on the client system.

### Running the RREG Tool in In-Band Mode

To run the RREG Tool in in-band mode:

1. Navigate to the RREG home directory.
   
   If you are using in-band mode, the RREG directory is inside the Oracle Access Manager Oracle home:
   
   ```bash
OAM_ORACLE_HOME/oam/server/rreg
   ```
   
   If you are using out-of-band mode, then the RREG home directory is the location where you unpacked the RREG archive.

2. In the RREG home directory, navigate to the bin directory:
   
   ```bash
cd RREG_HOME/bin/
   ```

3. Set the permissions of the oamreg.sh command so you can execute the file:
   
   ```bash
chmod +x oamreg.sh
   ```

4. Run the following command:
   
   ```bash
./oamreg.sh inband RREG_HOME/input/OAM11GRequest_edg.xml
   ```
   
   In this example:
   
   - It is assumed the edited OAM11GRequest.xml file is located in the RREG_HOME/input directory.
   - The output from this command will be saved to the following directory:
     ```bash
RREG_HOME/output/
     ```
The following example shows a sample RREG session:

Welcome to OAM Remote Registration Tool!
Parameters passed to the registration tool are:
Mode: inband
Filename: /u01/oracle/products/fmw/iam_home/oam/server/rreg/client/rreg/input/OAM11GRequest_edg.xml
Enter admin username: weblogic_idm
Username: weblogic_idm
Enter admin password:
Do you want to enter a Webgate password?(y/n):
  n
Do you want to import an URIs file?(y/n):
  n

----------------------------------------
Request summary:
OAM11G Agent Name: SOA12213_EDG_AGENT
Base URL: https://soa.example.com:443
URL String: null
Registering in Mode: inband
Your registration request is being sent to the Admin server at: http://host1.example.com:7001
----------------------------------------

Jul 08, 2015 7:18:13 PM oracle.security.jps.util.JpsUtil disableAudit
INFO: JpsUtil: isAuditDisabled set to true
Jul 08, 2015 7:18:14 PM oracle.security.jps.util.JpsUtil disableAudit
INFO: JpsUtil: isAuditDisabled set to true
Inband registration process completed successfully! Output artifacts are created in the output folder.

Running the RREG Tool in Out-Of-Band Mode

To run the RREG Tool in out-of-band mode on the WEBHOST server, the administrator uses the following command:

```
RREG_HOME/bin/oamreg.sh outofband input/OAM11GRequest.xml
```

In this example:

- Replace `RREG_HOME` with the location where the RREG archive file was unpacked on the server.
- The edited `OAM11GRequest.xml` file is located in the `RREG_HOME/input` directory.
- The RREG Tool saves the output from this command (the `AgentID_response.xml` file) to the following directory:

```
RREG_HOME/output/
```

The Oracle Access Manager server administrator can then send the `AgentID_response.xml` to the user who provided the `OAM11GRequest.xml` file.

To run the RREG Tool in out-of-band mode on the Web server client machine, use the following command:

```
RREG_HOME/bin/oamreg.sh outofband input/AgentID_response.xml
```

In this example:
Replace `RREG_HOME` with the location where you unpacked the RREG archive file on the client system.

The `AgentID_response.xml` file, which was provided by the Oracle Access Manager server administrator, is located in the `RREG_HOME/input` directory.

The RREG Tool saves the output from this command (the artifacts and files required to register the Webgate software) to the following directory on the client machine:

```
RREG_HOME/output/
```

### Files and Artifacts Generated by RREG

The files that get generated by the RREG Tool vary, depending on the security level you are using for communications between the WebGate and the Oracle Access Manager server. See Securing Communication Between OAM Servers and WebGates in *Administrator's Guide for Oracle Access Management*.

Note that in this topic any references to `RREG_HOME` should be replaced with the path to the directory where you ran the RREG tool. This is typically the following directory on the Oracle Access Manager server, or (if you are using out-of-band mode) the directory where you unpacked the RREG archive:

```
OAM_ORACLE_HOME/oam/server/rreg/client
```

The following table lists the artifacts that are always generated by the RREG Tool, regardless of the Oracle Access Manager security level.

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
</tr>
</thead>
</table>
| `cwallet.sso`   | • `RREG_HOME/output/Agent_ID/` - For WebGate 12c  
|                 | • `RREG_HOME/output/Agent_ID/wallet` - For WebGate 12c and OHS 12c |
| `ObAccessClient.xml` | `RREG_HOME/output/Agent_ID/` |

The following table lists the additional files that are created if you are using the SIMPLE or CERT security level for Oracle Access Manager:

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa_key.pem</code></td>
<td><code>RREG_HOME/output/Agent_ID/</code></td>
</tr>
<tr>
<td><code>aaa_cert.pem</code></td>
<td><code>RREG_HOME/output/Agent_ID/</code></td>
</tr>
<tr>
<td><code>password.xml</code></td>
<td><code>RREG_HOME/output/Agent_ID/</code></td>
</tr>
</tbody>
</table>

Note that the `password.xml` file contains the obfuscated global passphrase to encrypt the private key used in SSL. This passphrase can be different than the passphrase used on the server.

You can use the files generated by RREG to generate a certificate request and get it signed by a third-party Certification Authority. To install an existing certificate, you must use the existing `aaa_cert.pem` and `aaa_chain.pem` files along with `password.xml` and `aaa_key.pem`.  

Copying Generated Artifacts to the Oracle HTTP Server WebGate Instance Location

After the RREG Tool generates the required artifacts, manually copy the artifacts from the `RREG_Home/output/agent_ID` directory to the Oracle HTTP Server configuration directory on the Web tier host.

The location of the files in the Oracle HTTP Server configuration directory depends upon the Oracle Access Manager security mode setting (OPEN, SIMPLE, or CERT).

The following table lists the required location of each generated artifact in the Oracle HTTP Server configuration directory, based on the security mode setting for Oracle Access Manager. In some cases, you might have to create the directories if they do not exist already. For example, the wallet directory might not exist in the configuration directory.

---

**Note:**

For an enterprise deployment, Oracle recommends simple mode, unless additional requirements exist to implement custom security certificates for the encryption of authentication and authorization traffic. The information about using open or certification mode is provided here as a convenience.

Avoid using open mode, because in open mode, traffic to and from the Oracle Access Manager server is not encrypted.

For more information using certificate mode or about Oracle Access Manager supported security modes in general, see Securing Communication Between OAM Servers and WebGates in *Administrator’s Guide for Oracle Access Management*. 

---
<table>
<thead>
<tr>
<th>File</th>
<th>Location When Using OPEN Mode</th>
<th>Location When Using SIMPLE Mode</th>
<th>Location When Using CERT Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>wallet/cwallet.sso</td>
<td>OHS_CONFIG_DIR/webgate/config/wallet</td>
<td>OHS_CONFIG_DIR/webgate/config/wallet</td>
<td>OHS_CONFIG_DIR/webgate/config/wallet</td>
</tr>
</tbody>
</table>

**Note:**
By default, the wallet folder is not available.
<table>
<thead>
<tr>
<th>File</th>
<th>Location When Using OPEN Mode</th>
<th>Location When Using SIMPLE Mode</th>
<th>Location When Using CERT Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File</td>
<td>Location When Using OPEN Mode</td>
<td>Location When Using SIMPLE Mode</td>
<td>Location When Using CERT Mode</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>ObAccessClient.xml</td>
<td>OHS_CONFIG_DIR/webgate/config</td>
<td>OHS_CONFIG_DIR/webgate/config</td>
<td>OHS_CONFIG_DIR/webgate/config</td>
</tr>
<tr>
<td>password.xml</td>
<td>N/A</td>
<td>OHS_CONFIG_DIR/webgate/config</td>
<td>OHS_CONFIG_DIR/webgate/config</td>
</tr>
<tr>
<td>aaa_key.pem</td>
<td>N/A</td>
<td>OHS_CONFIG_DIR/webgate/config/simple</td>
<td>OHS_CONFIG_DIR/webgate/config</td>
</tr>
<tr>
<td>aaa_cert.pem</td>
<td>N/A</td>
<td>OHS_CONFIG_DIR/webgate/config/simple</td>
<td>OHS_CONFIG_DIR/webgate/config</td>
</tr>
<tr>
<td>aaa_chain.pem</td>
<td>N/A</td>
<td>N/A</td>
<td>OHS_CONFIG_DIR/webgate/config</td>
</tr>
</tbody>
</table>

**Note:**

If you need to redeploy the `ObAccessClient.xml` to WEBHOST1 and WEBHOST2, delete the cached copy of `ObAccessClient.xml` and its lock file, `ObAccessClient.xml.lck` from the servers. The cache location on WEBHOST1 is:

```
OHS_DOMAIN_HOME/servers/ohs1/cache/
```

And you must perform the similar step for the second Oracle HTTP Server instance on WEBHOST2:

```
OHS_DOMAIN_HOME/servers/ohs2/cache/
```

**Note:**

`aaa_chain.pem` is generated when certificates are created for CERT mode.

### Restarting the Oracle HTTP Server Instance

For information about restarting the Oracle HTTP Server instance, see Restarting Oracle HTTP Server Instances by Using WLST in *Administrator’s Guide for Oracle HTTP Server*.

If you have configured Oracle HTTP Server in a WebLogic Server domain, you can also use Oracle Fusion Middleware Control to restart the Oracle HTTP Server instances. See Restarting Oracle HTTP Server Instances by Using Fusion Middleware Control in *Administrator’s Guide for Oracle HTTP Server*. 
Configuring Oracle Traffic Director WebGate for Oracle Access Manager

WebGate is installed by default along with Oracle Traffic Director. However, you still need to configure it. A WebGate intercepts HTTP requests and forwards them to the Oracle Access Manager for authentication and authorization. WebGate gets installed by default when you install Oracle Traffic Director.

This appendix contains the following sections:

- Prerequisites for Configuring Webgate
- Configuring Oracle Traffic Director 12c WebGate
- Verifying the Configuration of Oracle Traffic Director 12c WebGate
- Getting Started with a New Oracle Traffic Director 12c WebGate
- Prerequisites for Configuring Webgate

Note:
It is highly recommended that Oracle Access Manager is installed in its own environment and not on the same machine as WebLogic Server. Oracle Access Manager and WebLogic Server can be installed on the same machine if they are both 11g versions.

- Oracle Fusion Middleware 12c Release 1(12.2.1.2)
- Oracle Fusion Middleware 12c Release 2(12.1.3)
Configuring Oracle Traffic Director 12c WebGate

Complete the following steps after installing Oracle Traffic Director to configure Oracle Traffic Director 12c WebGate for Oracle Access Manager:

- **On UNIX**
  1. Go to the $(Oracle_Home)/webgate/otd/tools/deployWebGate directory (Please note that $(Oracle_Home) is the location set as the OracleHome when installing Oracle Traffic Director) by running the following command:

     ```
     cd $(Oracle_Home)/webgate/otd/tools/deployWebGate
     ```

  2. Run the following command to create the OTD WebGate Instance Directory from $(Oracle_Home)/webgate/otd/tools/deployWebGate:

     ```
     ./deployWebGateInstance -w webgate_instanceDirectory -oh $(Oracle_Home) -ws otd
     ```

     In this command:

     - $(Oracle_Home) is the path to where Oracle Traffic Director has been installed.
     
       Example: /home/oracle

     - webgate_instanceDirectory is the location of the directory where you will copy the WebGate profile.
     
       Example: $(Domain_Home)/config/fmwconfig/components/OTD/instances/Instance_Name

       (Please note that $(Domain_Home) is the path to the directory which contains the OTD domain.)

  3. Set the environment variable LD_LIBRARY_PATH to WebGate_$(Oracle_Home)/lib

     For example:

     For Linux 64

     ```
     export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$(Oracle_Home)/lib
     ```

     For Windows

     ```
     set PATH=%(Oracle_Home)%\bin;%path%
     ```

  4. Go to the following directory:

     For Unix-based platforms

     ```
     $(Oracle_Home)/webgate/otd/tools/setup/InstallTools
     ```

     For Windows

     ```
     $(Oracle_Home)/webgate/otd/tools/EditObjConf
     ```

  5. On the command line, run the following command for updating OTD conf files, such as magnus.conf and obj.conf.

     For a standalone Oracle Traffic Director installation:
For a collocated Oracle Traffic Director installation:

`./EditObjConf -f Domain_Home/config/fmwconfig/components/OTD/instances/Instance_Name/config/Instance_Name-obj.conf -w webgate_instanceDirectory [-oh Oracle_Home] -ws otd`

In this command:
- Oracle_Home is the path to the parent directory of a valid WebLogic Server installation, or to where Oracle Traffic Director is installed.
  
  Example:
  `/home/oracle`

- webgate_instanceDirectory is the location of the directory where you will copy the WebGate profile.
  
  Example:
  `Domain_Home/config/fmwconfig/components/OTD/instances/Instance_Name`

- On Windows

  1. Go to the `$Oracle_Home\webgate\otd\tools\deployWebGate` directory by running the following command:

     `cd $Oracle_Home\webgate\otd\tools\deployWebGate`

  2. Run the following command to copy the required bits of agent from the `$Oracle_Home\` directory to the `webgate_instanceDirectory` location:

     `deployWebGateInstance.bat -w webgate_instanceDirectory [-oh Oracle_Home] -ws otd`

     In this command:

     - Oracle_Home is the directory in which you have installed Oracle Traffic Director WebGate.

       Example:
       `
       \home\oracle`

     - webgate_instanceDirectory is the location of the directory where you will copy the WebGate profile.

       Example:
       `
       Domain_Home/config/fmwconfig/components/OTD/instances/Instance_Name`

  3. Run the following command to set the `PATH` environment variable:

     `set %PATH%=%PATH%;$Oracle_Home\webgate\otd\lib;$Oracle_Home\bin`

  4. Go to the following directory:

     `$Oracle_Home\webgate\otd\tools\EditObjConf`

  5. On the command line, run the following command for updating OTD conf files, such as `magnus.conf` and `obj.conf`.

      For a standalone Oracle Traffic Director installation:
Verifying the Configuration of Oracle Traffic Director 12c WebGate

After installing Oracle Traffic Director 12c WebGate for Oracle Access Manager and completing the configuration steps, you can examine the `installDATE-TIME_STAMP.out` log file to verify the installation. The default location of the log are as follows:

- **On UNIX**
  
  `{Oracle_Home}/oraInst.loc`

- **On Windows**
  
  `C:\Program Files\Oracle\Inventory\logs`

Getting Started with a New Oracle Traffic Director 12c WebGate

Before you can use the new Oracle Traffic Director 12c WebGate agent for Oracle Access Manager, you must complete the following tasks:

1. **Registering the New Oracle Traffic Director 12c WebGate**
2. **Copying Generated Files and Artifacts to the Oracle Traffic Director WebGate Instance Location**
3. **Restarting the Oracle Traffic Director Instance**
   - Registering the New Oracle Traffic Director 12c WebGate
   - Copying Generated Files and Artifacts to the Oracle Traffic Director WebGate Instance Location
   - Restarting the Oracle Traffic Director Instance
Registering the New Oracle Traffic Director 12c WebGate

You can register the new WebGate agent with Oracle Access Manager by using the Oracle Access Manager Administration console. For more information, see Registering an OAM Agent Using the Console in the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.

Alternatively, you can use the RREG command-line tool to register a new WebGate agent. You can use the tool to run in two modes: **In-Band** and **Out-Of-Band**.

This section contains the following topics:

- Setting Up the RREG Tool
- Updating the OAM11gRequest.xml File
- Using the In-Band Mode
- Using the Out-Of-Band Mode
- Files and Artifacts Generated by RREG
- Setting Up the RREG Tool
- Updating the OAM11gRequest.xml File
- Using the In-Band Mode
- Using the Out-Of-Band Mode
- Files and Artifacts Generated by RREG

Setting Up the RREG Tool

To set up the RREG tool, complete the following steps:

- **On UNIX**
  1. After installing and configuring Oracle Access Manager, go to the following directory:
     
     $Oracle_IDM2/oam/server/rreg/client
  2. Untar the `RREG.tar.gz` file.
     
     Example:
     
     ```
     gunzip RREG.tar.gz
     tar -xvf RREG.tar
     ```
     
     The tool for registering the agent is located at:
     
     ```
     RREG_Home/bin/oamreg.sh
     ```

    **Note:**

    *RREG_Home* is the directory in which you extracted the contents of `RREG.tar.gz/rreg`.

- **On Windows**
1. After installing and configuring Oracle Access Manager, go to the following location:
   Oracle_IDM2\oam\server\rreg\client

2. Extract the contents of the RREG.tar.zip file to a destination of your choice.

   The tool for registering the agent is located at:
   RREG_Home\bin\oamreg.bat

   **Note:**
   RREG_Home is the directory in which you extracted the contents of RREG.tar.gz/rreg.

Set the following environment variables in the oamreg.sh script, on UNIX, and oamreg.bat script, on Windows:

- **OAM_REG_HOME**
  Set this variable to the absolute path to the directory in which you extracted the contents of RREG.tar/rreg.

- **JDK_HOME**
  Set this variable to the absolute path to the directory in which Java or JDK is installed on your machine.

### Updating the OAM11gRequest.xml File

You must update the agent parameters, such as `agentName`, in the OAM11GRequest.xml file in the RREG_Home\input directory on Windows. On UNIX, the file is in the RREG_Home/input directory.

   **Note:**
   The OAM11GRequest.xml file or the short version OAM11GRequest_short.xml is used as a template. You can copy this template file and use it.

Modify the following required parameters in the OAM11GRequest.xml file or in the OAM11GRequest_short.xml file:

- **serverAddress**
  Specify the host and the port of the OAM Administration Server.

- **agentName**
  Specify any custom name for the agent.

- **agentBaseUrl**
  Specify the host and the port of the machine on which Oracle Traffic Director 12c WebGate is installed.
• **preferredHost**
  Specify the host and the port of the machine on which Oracle Traffic Director 12c WebGate is installed.

• **security**
  Specify the security mode, such as open, based on the WebGate installed.

• **primaryServerList**
  Specify the host and the port of Managed Server for the Oracle Access Manager proxy, under a Server container element.

After modifying the file, save and close it.

**Using the In-Band Mode**

If you run the RREG tool once after updating the WebGate parameters in the OAM11GRequest.xml file, the files and artifacts required by WebGate are generated in the following directory:

**On UNIX:**

```
RREG_Home/output/agent_name
```

**On Windows:**

```
RREG_Home\output\agent_name
```

**Note:**

You can run RREG either on a client machine or on the server. If you are running it on the server, you must manually copy the artifacts back to the client.

Complete the following steps:

1. Open the OAM11GRequest.xml file, which is in RREG_Home/input/on UNIX and RREG_Home\input on Windows. RREG_Home is the directory on which you extracted the contents of RREG.tar.gz/rreg.

   Edit the XML file and specify parameters for the new Oracle Traffic Director WebGate for Oracle Access Manager.

2. Run the following command:

   **On UNIX:**
   
   ```
   ./RREG_Home/bin/oamreg.sh inband input/OAM11GRequest.xml
   ```

   **On Windows:**
   
   ```
   RREG_Home\bin\oamreg.bat inband input\OAM11GRequest.xml
   ```

**Using the Out-Of-Band Mode**

If you are an end user with no access to the server, you can e-mail your updated OAM11GRequest.xml file to the system administrator, who can run RREG in the out-of-
band mode. You can collect the generated AgentID_Response.xml file from the system administrator and run RREG on this file to obtain the WebGate files and artifacts you require.

After you receive the generated AgentID_Response.xml file from the administrator, you must manually copy the file to the input directory on your machine.

• **On UNIX**

  Complete the following steps:

  1. If you are an end user with no access to the server, open the OAM11GRequest.xml file, which is in RREG_Home/input/.
     
     RREG_Home is the directory on which you extracted the contents of RREG.tar.gz/rreg. Edit this XML file and specify parameters for the new Oracle Traffic Director WebGate for Oracle Access Manager. Send the updated file to your system administrator.

  2. If you are an administrator, copy the updated OAM11GRequest.xml file, which is in RREG_Home/input/ directory.
     
     This is the file that you received from the end user. Go to your (administrator's) RREG_Home directory and run the following command:

     ./RREG_Home/bin/oamreg.sh outofband input/OAM11GRequest.xml

     An Agent_ID_Response.xml file is generated in the output directory on the administrator's machine, in the RREG_Home/output/ directory. Send this file to the end user who sent you the updated OAM11GRequest.xml file.

  3. If you are an end user, copy the generated Agent_ID_Response.xml file, which is in RREG_Home/input/.
     
     This is the file that you received from the administrator. Go to your (client's) RREG home directory and run the following command on the command line:

     ./RREG_Home/bin/oamreg.sh outofband input/Agent_ID_Response.xml

  **Note:**

  If you register the WebGate agent by using the Oracle Access Manager Administration Console, as described in "Registering an OAM Agent Using the Console in the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management", you must manually copy the files and artifacts generated after the registration from the server (the machine on which the Oracle Access Manager Administration Console is running) to the client machine. The files and artifacts are generated in the $Oracle_Home/user_projects/domains/name_of_the_WebLogic_domain_for_OAM/output/Agent_ID directory.

• **On Windows**

  Complete the following steps:

  1. If you are an end user with no access to the server, open the OAM11GRequest.xml file, which is in RREG_HOME\input\ directory.
     
     RREG_HOME is the directory in which you extracted the contents of RREG.tar.gz/rreg. Edit this XML file, specify parameters for the new Oracle Traffic Director
WebGate for Oracle Access Manager, and send the updated file to your system administrator.

2. If you are an administrator, copy the updated OAM11GRequest.xml file, which is in RREG_Home\input\. This is the file you received from the end user. Go to your (administrator's) RREG_Home directory and run the following command:

```
RREG_Home\bin\oamreg.bat outofband input\OAM11GRequest.xml
```

An Agent_ID_Response.xml file is generated on the administrator's machine in the RREG_Home\output\ directory. Send this file to the end user who sent you the updated OAM11GRequest.xml file.

3. If you are an end user, copy the generated Agent_ID_Response.xml file, which is in RREG_Home\input\. This is the file you received from the administrator. Go to your (client's) RREG home directory and run the following command:

```
RREG_Home\bin\oamreg.bat outofband input\Agent_ID_Response.xml
```

---

**Note:**

If you register the WebGate agent by using the Oracle Access Manager Administration Console, as described in "Registering an OAM Agent Using the Console in the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management," you must manually copy the files and artifacts generated after the registration from the server (the machine on which the Oracle Access Manager Administration Console is running) to the client machine. The files and artifacts are generated in the $(Oracle_Home)/user_projects/domains/name_of_the_WebLogic_domain_for_OAM/output/Agent_ID directory.

---

**Files and Artifacts Generated by RREG**

Regardless of the method or mode you use to register the new WebGate agent, the following files and artifacts are generated in the RREG_Home/output/Agent_ID directory:

- wallet/cwallet.sso
- cwallet.sso
- ObAccessClient.xml

- In the **SIMPLE** mode, RREG generates:
  - password.xml, which contains the obfuscated global passphrase to encrypt the private key used in SSL. This passphrase can be the same as the passphrase used on the server.
  - aaa_key.pem
  - aaa_cert.pem

- In the **CERT** mode, RREG generates password.xml, which contains the obfuscated global passphrase to encrypt the private key used in SSL. This passphrase can be different than the passphrase used on the server.
Note:

You can use these files generated by RREG to generate a certificate request and get it signed by a third-party Certification Authority. To install an existing certificate, you must use the existing `aaa_cert.pem` and `aaa_chain.pem` files along with `password.xml` and `aaa_key.pem`.

Copying Generated Files and Artifacts to the Oracle Traffic Director WebGate Instance Location

After RREG generates these files and artifacts, you must manually copy them, based on the security mode you are using, from the `RREG_Home/output/Agent_ID` directory to the `webgate_instanceDirectory` directory.

Do the following according to the security mode you are using:

- **In OPEN mode**, copy the following files from the `RREG_Home/output/Agent_ID` directory to the `webgate_instanceDirectory/webgate/config` directory:
  - wallet/cwallet.sso
  - ObAccessClient.xml
  - cwallet.sso

- **In SIMPLE mode**, copy the following files from the `RREG_Home/output/Agent_ID` directory to the `webgate_instanceDirectory/webgate/config` directory:
  - ObAccessClient.xml
  - cwallet.sso
  - password.xml

  In addition, copy the following files from the `RREG_Home/output/Agent_ID` directory to the `webgate_instanceDirectory/webgate/config/simple` directory:
  - aaa_key.pem
  - aaa_cert.pem

- **In CERT mode**, copy the following files from the `RREG_Home/output/Agent_ID` directory to the `webgate_instanceDirectory/webgate/config` directory:
  - ObAccessClient.xml
  - cwallet.sso
  - password.xml

- **Generating a New Certificate**

- **Migrating an Existing Certificate**

**Generating a New Certificate**

You can generate a new certificate as follows:

1. Go to the `${Oracle_Home}/webgate/otd/tools/openssl` directory.
2. Create a certificate request as follows:

```
./openssl req -utf8 -new -nodes -config openssl_silent_otd11g.cnf -keyout aaa_key.pem -out aaa_req.pem -rand $(Oracle_Home)/webgate/otd/config/random-seed/
```

3. Self-sign the certificate as follows:

```
./openssl ca -config openssl_silent_otd11g.cnf -policy policy_anything -batch -out aaa_cert.pem -infiles aaa_req.pem
```

4. Copy the following generated certificates to the `webgate_instanceDirectory/webgate/config` directory:

- `aaa_key.pem`
- `aaa_cert.pem`
- `cacert.pem` located in the `simpleCA` directory

---

**Note:**

After copying the `cacert.pem` file, you must rename the file to `aaa_chain.pem`.

---

### Migrating an Existing Certificate

If you want to migrate an existing certificate (`aaa_key.pem`, `aaa_cert.pem`, and `aaa_chain.pem`), ensure that you use the same passphrase that you used to encrypt `aaa_key.pem`. You must enter the same passphrase during the RREG registration process. If you do not use the same passphrase, the `password.xml` file generated by RREG does not match the passphrase used to encrypt the key.

If you enter the same passphrase, you can copy these certificates as follows:

1. Go to the `webgate_instanceDirectory/webgate/config` directory.
2. Copy the following certificates to the `webgate_instanceDirectory/webgate/config` directory:
   - `aaa_key.pem`
   - `aaa_cert.pem`
   - `aaa_chain.pem`

### Restarting the Oracle Traffic Director Instance

For information about restarting the Oracle Traffic Director instance, see "Starting, Stopping, and Restarting Oracle Traffic Director Instances by Using WLST" in *Administering Oracle Traffic Director*.

If you have configured Oracle Traffic Director in a WebLogic Server domain, you can also use Oracle Fusion Middleware Control to restart the Oracle Traffic Director Instances. For more information, see "Starting, Stopping, and Restarting Oracle Traffic Director Instances Using Fusion Middleware Control" in *Administering Oracle Traffic Director*.
For a standalone instance, you can restart from `Domain_Home/config/fmwconfig/components/OTD/instances/Instance_Name/bin` using the `.restart` command.
4

Adding Trusted Certificate for SIMPLE and CERT Mode communication

To add a trusted certificate for SIMPLE and CERT mode communication, you must perform following steps for a new WebGate profile created:

Note:
The orapki utility is used for adding trusted certificate in wallet.

1. Go to `webgate_instanceDirectory/webgate/config/wallet` directory.
2. Set `JAVA_HOME` variable to the absolute path of the directory in which Java or JDK is installed.
3. Run the following command to display the wallet content before adding the certificate:
   ```bash
   <MW_HOME>/oracle_common/bin/orapki wallet display -wallet ./
   ``
4. Perform the following steps to add the trusted certificate in wallet:
   - Run the following command to add the trusted certificate in SIMPLE mode:
     ```bash
     <MW_HOME>/oracle_common/bin/orapki wallet -wallet ./ -trusted_cert -cert webgate_installDirectory/tools/openssl/simpleCA/cacert.pem -auto_login_only
     ``
   - Run the following command to add the trusted certificate in CERT mode:
     ```bash
     <MW_HOME>/oracle_common/bin/orapki wallet -wallet ./ -trusted_cert -cert webgate_instanceDirectory/webgate/config/aaa_chain.pem -auto_login_only
     ``
5. Run the following command to verify the certificate added:
   ```bash
   <MW_HOME>/oracle_common/bin/orapki wallet display -wallet ./
   ```
Upgrading to OHS/OTD 12c WebGate

After upgrading from OHS 11g WebGate to OHS 12c WebGate or OTD 11g WebGate to OTD 12c WebGate, you must perform either of the following steps:

• Create a new WebGate profile and copy the new WebGate artifacts to WebGate.
  OR
• Manually add SHA256 certificate to the existing WebGate cwallet.sso after deleting md5 cert.