## Contents

**Preface**

- Audience vi
- Documentation Accessibility vi
- Related Documents vi
- Conventions vii

### 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 WebGate with Oracle Access Manager 2-3
  - Locating and Preparing the RREG Tool 2-4
  - Updating the Standard Properties in the OAM12cRequest.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
- Deleting the previous version files 2-13
- Restarting the Oracle HTTP Server Instance 2-13

### 3 Configuring Oracle Traffic Director WebGate for Oracle Access Manager

- Prerequisites for Configuring Webgate 3-1
- Configuring the Domain 3-1
Starting the Configuration Wizard 3-2
Navigating the Configuration Wizard Screens to Create and Configure the Domain 3-2
  Selecting the Domain Type and Domain Home Location 3-4
  Selecting the Configuration Templates 3-4
  Selecting the Application Home Location 3-5
  Configuring the Administrator Account 3-6
  Specifying the Domain Mode and JDK 3-7
  Specifying the Database Configuration Type 3-7
  Specifying JDBC Component Schema Information 3-8
  Testing the JDBC Connections 3-8
  Selecting Advanced Configuration 3-8
  Configuring the Administration Server Listen Address 3-9
  Configuring Node Manager 3-9
  Configuring Managed Servers for Oracle Access Management 3-9
  Configuring a Cluster for Webgate 3-11
  Defining Server Templates 3-11
  Configuring Dynamic Servers 3-11
  Assigning Webgate Managed Servers to the Cluster 3-12
  Configuring Coherence Clusters 3-12
  Creating a New Webgate Machine 3-13
  Assigning Servers to Webgate Machines 3-13
  Virtual Targets 3-14
  Partitions 3-14
  Configuring Domain Frontend Host 3-14
  Targeting the Deployments 3-14
  Targeting the Services 3-14
  Reviewing Your Configuration Specifications and Configuring the Domain 3-14
  Writing Down Your Domain Home and Administration Server URL 3-15
  Updating the System Properties for SSL Enabled Servers 3-15
Configuring Oracle Traffic Director WebGate 3-15
Verifying the Configuration of Oracle Traffic Director WebGate 3-18
Getting Started with a New Oracle Traffic Director WebGate 3-18
  Registering the New Oracle Traffic Director 12c (12.2.1.4.0) WebGate 3-18
    Setting Up the RREG Tool 3-18
    Updating the OAM12cRequest.xml File 3-19
    Using the In-Band Mode 3-20
    Using the Out-Of-Band Mode 3-21
    Files and Artifacts Generated by RREG 3-23
  Copying Generated Files and Artifacts to the Oracle Traffic Director WebGate Instance Location 3-23
    Generating a New Certificate 3-24
4  Adding Trusted Certificate for SIMPLE and CERT Mode communication

5  Upgrading to OHS/OTD 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 (12.2.1.4.0) 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 12c (12.2.1.4.0) documentation library:

- Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management
• Oracle Fusion Middleware Administrator’s Guide for Oracle Access Management
• Oracle Fusion Middleware Planning an Installation of Oracle Fusion Middleware
• Release Notes for Oracle Fusion Middleware Infrastructure

You can also access Oracle documentation online from the Oracle Technology Network (OTN) Web site at the following URL:

http://docs.oracle.com/

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>monospace</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 WebGate
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**
  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 configure Oracle HTTP Server WebGate, you must have installed and configured a certified version of Oracle Access Manager.

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

• **Registering the Oracle HTTP Server WebGate with Oracle Access Manager**
  You can register the WebGate agent with Oracle Access Manager using the Oracle Access Manager Administration console.

### 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 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.
Note:
For production environments, it is highly recommended that you install Oracle Access Manager in its own environment and not on the machines that are hosting the enterprise deployment.

For more information about Oracle Access Manager, see the latest Oracle Identity and Access Management documentation, which you can find in the Middleware documentation on the Oracle Help Center.

For Oracle Fusion Middleware 12c (12.2.1.4.0), the WebGate software is installed as part of the Oracle HTTP Server 12c (12.2.1.4.0) software installation. See Registering and Managing OAM Agents in Administrator’s Guide for Oracle Access Management.

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-x-x+ 4 orcl oinstall 4 Oct 2 07:14 .
   drwxr-x-x+ 3 orcl oinstall 3 Oct 2 07:14 tools
   drwxr-x-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`
5. **Navigate to the EditHttpConf directory:**

   (UNIX) cd OHS_ORACLE_HOME/webgate/ohs/tools/setup/InstallTools

   (Windows) cd OHS_ORACLE_HOME\webgate\ohs\tools\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.pl, or logout.pl 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 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 OAM12cRequest.xml File
- Running the RREG Tool
- Files and Artifacts Generated by RREG
- Copying Generated Artifacts to the Oracle HTTP Server WebGate Instance Location
- Deleting the previous version files
  After installing the newer version of Oracle HTTP Server Webgate, you must manually delete the older files in the configuration folder.
- 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:

   ![Note]
   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.

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

   ![Note]
   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 OAM12cRequest.xml File

Before you can register the Webgate agent with Oracle Access Manager, you must update some required properties in the `OAM12cRequest.xml` file.
Note:

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 (OAM12cRequest_short.xml, in which all non-listed fields will take a default value.

Note:

In the primary server list, the default names are mentioned as OAM_SERVER1 and OAM_SERVER2 for OAM servers. Rename these names in the list if the server names are changed in your environment.

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 OAM12cRequest.xml file template with an environment-specific name.

   cp OAM12cRequest.xml OAM12cRequest_edg.xml

3. Review the properties listed in the file, and then update your copy of the OAM12cRequest.xml file to make sure the properties reference the host names and other values specific to your environment.

<table>
<thead>
<tr>
<th>OAM12cRequest.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>
**OAM12cRequest.xml Property**

<table>
<thead>
<tr>
<th>Property</th>
<th>Set to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>security</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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>ipValidationExceptions</td>
<td>&lt;ipValidation&gt;0&lt;/ipValidation&gt;</td>
</tr>
<tr>
<td>ipValidationExceptions</td>
<td>&lt;ipValidationExceptions&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;ipAddress&gt;130.35.165.42&lt;/ipAddress&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/ipValidationExceptions&gt;</td>
</tr>
</tbody>
</table>
### OAM12cRequest.xml Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Set to...</th>
</tr>
</thead>
</table>
| agentBaseUrl              | 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 (12.2.1.4.0) WebGates are installed. For example:  
|                           | `<agentBaseUrl>`  
|                           |     https://soa.example.com:443  
|                           |   </agentBaseUrl> |
| virtualHost               | Set to **true** when protecting more than the agentBaseUrl, such as SSO protection for the administrative VIP. |
| hostPortVariationsList    | Add `hostPortVariation` host and port elements for each of the load-balancer URLs that will be protected by the WebGates. For example:  
|                           | `<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 OAM12cRequest.xml File*.

2. Untar the RREG.tar.gz file that was provided to you by the server administrator.
   
   For example:
   
   ```
   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:

   `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 OAM12cRequest.xml File* to update the `OAM12cRequest.xml` file, and send the completed `OAM12cRequest.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:

   `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/OAM12cRequest_edg.xml
   ```

   **In this example:**
   
   - It is assumed the edited `OAM12cRequest.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/OAM12cRequest_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:
   OAM12c Agent Name:SOA12214_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:

```bash
RREG_HOME/bin/oamreg.sh outofband input/OAM12cRequest.xml
```
In this example:

- Replace `RREG_HOME` with the location where the RREG archive file was unpacked on the server.
- The edited `OAM12cRequest.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 `OAM12cRequest.xml` file.

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

```bash
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>
<tbody>
<tr>
<td><code>cwallet.sso</code></td>
<td><code>RREG_HOME/output/Agent_ID/</code> - For WebGate</td>
</tr>
<tr>
<td></td>
<td>12c (12.2.1.4.0).</td>
</tr>
<tr>
<td></td>
<td><code>RREG_HOME/output/Agent_ID/wallet</code> - For WebGate 12c (12.2.1.4.0) and OHS 12c (12.2.1.4.0).</td>
</tr>
<tr>
<td><code>ObAccessClient.xml</code></td>
<td><code>RREG_HOME/output/Agent_ID/</code></td>
</tr>
</tbody>
</table>
The following table lists the additional files that are created if you are using the SIMPLE security level for Oracle Access Manager:

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

Note:
- The `password.xml` file is a common file for both the SIMPLE and CERT security levels, which is generated by the RREG tool.
- 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`.

The following table lists the additional files that an administrator has to generate, if you are using the CERT security level for Oracle Access Manager:

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

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>
<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/
Deleting the previous version files

After installing the newer version of Oracle HTTP Server Webgate, you must manually delete the older files in the configuration folder.

Complete the following steps:

1. Go to the `{Oracle_OAMWebGate1}/webgate/ohs/config` directory.
2. Delete the `np{previous_rel}_wg.txt` file.

   Where, `{previous_rel}` is the version number of the previous release from which you have upgraded from.

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 Oracle Fusion Middleware Administering 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 Oracle Fusion Middleware Administering Oracle HTTP Server.
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**
  You need to install Oracle Access Manager (OAM) before configuring Oracle Traffic Director. Also, there are version and environment related limitations for installing OAM.

- **Configuring the Domain**
  Use the Configuration Wizard to create and configure a domain.

- **Configuring Oracle Traffic Director WebGate**

- **Verifying the Configuration of Oracle Traffic Director WebGate**

- **Getting Started with a New Oracle Traffic Director WebGate**

### Prerequisites for Configuring Webgate

You need to install Oracle Access Manager (OAM) before configuring Oracle Traffic Director. Also, there are version and environment related limitations for installing OAM.

Before you can configure Oracle Traffic Director 12c (12.2.1.4.0) WebGate, you must install one of the following versions of Oracle Access Manager.

> **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 12c versions.

### Configuring the Domain

Use the Configuration Wizard to create and configure a domain.

For information on other methods to create domains, see Additional Tools for Creating, Extending, and Managing WebLogic Domains in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.
• **Starting the Configuration Wizard**  
  Start the Configuration Wizard to begin configuring a domain.

• **Navigating the Configuration Wizard Screens to Create and Configure the Domain**  
  Enter required information in the Configuration Wizard screens to create and configure the domain for the topology.

• **Updating the System Properties for SSL Enabled Servers**  
  For SSL enabled servers, you must set the required properties in the `setDomainEnv` file in the domain home.

---

**Starting the Configuration Wizard**

Start the Configuration Wizard to begin configuring a domain.

To start the Configuration Wizard:

1. Change to the following directory:  
   (UNIX) `ORACLE_HOME/oracle_common/common/bin`  
   (Windows) `ORACLE_HOME\oracle_common\common\bin`  
   where `ORACLE_HOME` is your 12c (12.2.1.4.0) Oracle home.

2. Enter the following command:  
   (UNIX) `.config.sh`  
   (Windows) `config.cmd`

---

**Navigating the Configuration Wizard Screens to Create and Configure the Domain**

Enter required information in the Configuration Wizard screens to create and configure the domain for the topology.

---

**Note:**

You can use this procedure to extend an existing domain. If your needs do not match the instructions in the procedure, be sure to make your selections accordingly, or see the supporting documentation for more details.

---

• **Selecting the Domain Type and Domain Home Location**  
  Use the Configuration Type screen to select a Domain home directory location, optimally outside the Oracle home directory.

• **Selecting the Configuration Templates**

• **Selecting the Application Home Location**  
  Use the Application Location screen to select the location to store applications associated with your domain, also known as the `Application home` directory.

• **Configuring the Administrator Account**  
  Use the Administrator Account screen to specify the user name and password for the default WebLogic Administrator account for the domain.
- **Specifying the Domain Mode and JDK**
  Use the Domain Mode and JDK screen to specify the domain mode and Java Development Kit (JDK).

- **Specifying the Database Configuration Type**
  Use the Database Configuration type screen to specify details about the database and database schema.

- **Specifying JDBC Component Schema Information**
  Use the JDBC Component Schema screen to verify or specify details about the database schemas.

- **Testing the JDBC Connections**
  Use the JDBC Component Schema Test screen to test the data source connections.

- **Selecting Advanced Configuration**
  Use the Advanced Configuration screen to complete the domain configuration.

- **Configuring the Administration Server Listen Address**
  Use the Administration Server screen to select the IP address of the host.

- **Configuring Node Manager**
  Use the Node Manager screen to select the type of Node Manager you want to configure, along with the Node Manager credentials.

- **Configuring Managed Servers for Oracle Access Management**

- **Configuring a Cluster for Webgate**
  Use the Clusters screen to create a new cluster.

- **Defining Server Templates**
  If you are creating dynamic clusters for a high availability setup, use the Server Templates screen to define one or more server templates for domain.

- **Configuring Dynamic Servers**
  You can skip this screen for Oracle Access Management configuration.

- **Assigning Webgate Managed Servers to the Cluster**
  Use the Assign Servers to Clusters screen to assign Managed Servers to a new configured cluster. A configured cluster is a cluster you configure manually. You do not use this screen if you are configuring a dynamic cluster, a cluster that contains one or more generated server instances that are based on a server template.

- **Configuring Coherence Clusters**
  Use the Coherence Clusters screen to configure the Coherence cluster.

- **Creating a New Webgate Machine**
  Use the Machines screen to create new machines in the domain. A machine is required so that Node Manager can start and stop servers.

- **Assigning Servers to Webgate Machines**
  Use the Assign Servers to Machines screen to assign the Administration Server and Managed Servers to the new machine you just created.

- **Virtual Targets**
  You can skip this screen for Oracle Access Management configuration.

- **Partitions**
  The Partitions screen is used to configure partitions for virtual targets in WebLogic Server Multitenant (MT) environments. Select **Next** without selecting any options.
Selecting the Domain Type and Domain Home Location

Use the Configuration Type screen to select a Domain home directory location, optimally outside the Oracle home directory.

Oracle recommends that you locate your Domain home in accordance with the directory structure in What Are the Key Oracle Fusion Middleware Directories? in Oracle Fusion Middleware Understanding Oracle Fusion Middleware, where the Domain home is located outside the Oracle home directory. This directory structure helps avoid issues when you need to upgrade or reinstall software.

To specify the Domain type and Domain home directory:

1. On the Configuration Type screen, select Create a new domain.
2. In the Domain Location field, specify your Domain home directory.

Note:

For more details about this screen, see Configuration Type in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard.

Selecting the Configuration Templates

On the Templates screen, make sure Create Domain Using Product Templates is selected, then select the Webgate template.

Selecting this template automatically selects the following as dependencies:

- Oracle Enterprise Manager
- Oracle JRF
- WebLogic Coherence Cluster Extension
Selecting the Application Home Location

Use the Application Location screen to select the location to store applications associated with your domain, also known as the Application home directory.

Oracle recommends that you locate your Application home in accordance with the directory structure in What Are the Key Oracle Fusion Middleware Directories? in Oracle Fusion Middleware Understanding Oracle Fusion Middleware, where the Application home is located outside the Oracle home directory. This directory structure helps avoid issues when you need to upgrade or re-install your software.

For more about the Application home directory, see About the Application Home Directory.

For more information about this screen, see Application Location in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard.

• About the Application Home Directory
  The Application home is the directory where applications for domains you configure are created.

• About the Recommended Directory Structure
  Oracle recommends specific locations for the Oracle Home, Domain Home, and Application Home.

About the Application Home Directory

The Application home is the directory where applications for domains you configure are created.

The default Application home location is $ORACLE_HOME/user_projects/applications/domain_name. However, Oracle strongly recommends that you locate your Application home outside of the Oracle home directory; if you upgrade your product to another major release, you must create a new Oracle home for binaries.

See About the Recommended Directory Structure for more on the recommended directory structure and locating your Application home.

Fusion Middleware documentation refers to the Application home directory as $APPLICATION_HOME and includes all folders up to and including the domain name. For example, if you name your domain exampledomain and you locate your application data in the $HOME/oracle/config/applications directory, the documentation uses $APPLICATION_HOME to refer to $HOME/oracle/config/applications/exampledomain.

About the Recommended Directory Structure

Oracle recommends specific locations for the Oracle Home, Domain Home, and Application Home.
Oracle recommends a directory structure similar to the one shown in Figure 3-1.

**Figure 3-1  Recommended Oracle Fusion Middleware Directory Structure**

A base location (Oracle base) should be established on your system (for example, `/home/oracle`). From this base location, create two separate branches, namely, the `product` directory and the `config` directory. The `product` directory should contain the product binary files and all the Oracle home directories. The `config` directory should contain your domain and application data.

Oracle recommends that you do not keep your configuration data in the Oracle home directory; if you upgrade your product to another major release, are required to create a new Oracle home for binaries. You must also make sure that your configuration data exists in a location where the binaries in the Oracle home have access.

The `/home/oracle/product` (for the Oracle home) and `/home/oracle/config` (for the application and configuration data) directories are used in the examples throughout the documentation; be sure to replace these directories with the actual directories on your system.

**Configuring the Administrator Account**

Use the Administrator Account screen to specify the user name and password for the default WebLogic Administrator account for the domain.

Oracle recommends that you make a note of the user name and password that you enter on this screen; you need these credentials later to boot and connect to the domain's Administration Server.

For more information about this screen, see Administrator Account in *Creating WebLogic Domains Using the Configuration Wizard*. 
Specifying the Domain Mode and JDK

Use the Domain Mode and JDK screen to specify the domain mode and Java Development Kit (JDK).

On the Domain Mode and JDK screen:

- Select **Production** in the **Domain Mode** field.
- Select the **Oracle HotSpot JDK** in the **JDK** field.

For more information about this screen, see Domain Mode and JDK in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Specifying the Database Configuration Type

Use the Database Configuration type screen to specify details about the database and database schema.

On the Database Configuration type screen, select **RCU Data**. This option instructs the Configuration Wizard to connect to the database and Service Table (STB) schema to automatically retrieve schema information for schemas needed to configure the domain.

Note:

If you select **Manual Configuration** on this screen, you must manually fill in parameters for your schema on the next screen.

After selecting **RCU Data**, specify details in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBMS/Service</td>
<td>Enter the database DBMS name, or service name if you selected a service type driver. Example: orcl.exampledomain.com</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the server hosting the database. Example: examplehost.exampledomain.com</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number on which the database listens. Example: 1521</td>
</tr>
<tr>
<td>Schema Owner</td>
<td>Enter the username and password for connecting to the database's Service Table schema. This is the schema username and password entered for the Service Table component on the Schema Passwords screen in the RCU. The default username is <code>prefix_STB</code>, where <code>prefix</code> is the custom prefix that you defined in the RCU.</td>
</tr>
<tr>
<td>Schema Password</td>
<td></td>
</tr>
</tbody>
</table>

Click **Get RCU Configuration** when you finish specifying the database connection information. The following output in the Connection Result Log indicates that the operation succeeded:
For more information about the schema installed when the RCU is run, see About the Service Table Schema in Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility. See Database Configuration Type in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard.

Specifying JDBC Component Schema Information

Use the JDBC Component Schema screen to verify or specify details about the database schemas.

Verify that the values populated on the JDBC Component Schema screen are correct for all schemas. If you selected RCU Data on the previous screen, the schema table should already be populated appropriately. If you selected Manual configuration on the Database Configuration screen, you must configure the schemas listed in the table manually, before you proceed.

For high availability environments, see the following sections in Oracle Fusion Middleware High Availability Guide for additional information on configuring data sources for Oracle RAC databases:

- Configuring Active GridLink Data Sources with Oracle RAC
- Configuring Multi Data Sources

See JDBC Component Schema in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard for more details about this screen.

Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections.

A green check mark in the Status column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

By default, the schema password for each schema component is the password you specified while creating your schemas. If you want different passwords for different schema components, manually edit them in the previous screen (JDBC Component Schema) by entering the password you want in the Schema Password column, against each row. After specifying the passwords, select the check box corresponding to the schemas that you changed the password in and test the connection again.

For more information about this screen, see JDBC Component Schema Test in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard.

Selecting Advanced Configuration

Use the Advanced Configuration screen to complete the domain configuration.

On the Advanced Configuration screen, select:
• Administration Server
  Required to properly configure the listen address of the Administration Server.

• Node Manager
  Required to configure Node Manager.

• Topology
  Required to configure the Webgate Managed Server.

Optionally, select other available options as required for your desired installation environment. The steps in this guide describe a standard installation topology, but you may choose to follow a different path. If your installation requirements extend to additional options outside the scope of this guide, you may be presented with additional screens to configure those options. For information about all Configuration Wizard screens, see Configuration Wizard Screens in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard.

Configuring the Administration Server Listen Address

Use the Administration Server screen to select the IP address of the host.

Select the drop-down list next to **Listen Address** and select the IP address of the host where the Administration Server will reside, or use the system name or DNS name that maps to a single IP address. Do **not** use All Local Addresses.

Do **not** specify any server groups for the Administration Server.

---

**Note:**

Use the Mozilla Firefox browser to access Internet Protocol Version 6 (IPv6) URLs. You must enter the Global IPv6 address to create a domain and access URLs. (You should not use the local IPv6 address.)

---

Configuring Node Manager

Use the Node Manager screen to select the type of Node Manager you want to configure, along with the Node Manager credentials.

Select **Per Domain Default Location** as the Node Manager type, then specify Node Manager credentials.

For more information about this screen, see Node Manager in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard.

For more about Node Manager types, see Node Manager Overview in Oracle Fusion Middleware Administering Node Manager for Oracle WebLogic Server.

Configuring Managed Servers for Oracle Access Management

On the Managed Servers screen, the new Managed Servers named **otd_server_1** and **otd_policy_mgr1** are displayed:
1. In the Listen Address drop-down list, select the IP address of the host on which
the Managed Server will reside or use the system name or DNS name that maps
to a single IP address. Do not use "All Local Addresses."

2. In the Server Groups drop-down list, select the server group for your managed
server. By default, OTD-MGD-SVRS is selected for otd_server1 and OTD-
POLICY-MANAGED-SERVER is selected for otd_policy_mgr1.

Server groups target Fusion Middleware applications and services to one or more
servers by mapping defined application service groups to each defined server
group. A given application service group may be mapped to multiple server groups
if needed. Any application services that are mapped to a given server group are
automatically targeted to all servers that are assigned to that group. For more
information, see Application Service Groups, Server Groups, and Application
Service Mappings in Oracle Fusion Middleware Domain Template Reference.

3. Configuring a second Managed Server is one of the steps needed to configure the
standard topology for high availability. If you are not creating a highly available
environment, then this step is optional.

Click Clone and repeat this process to create a second Managed Server named
otd_policy_mgr2.

Note:

If you wish to configure additional Managed Servers, use the Clone
option and add the Managed Server. For example, if we want to
configure otd_server2, click Clone and select oam_server1 to clone
this server. Do not use the add option to add a new Managed Server.

Configuring a second Managed Server is one of the steps needed to configure the
standard topology for high availability. If you are not creating a highly available
environment, then this step is optional.

For more information about the high availability standard topology, see
Understanding the Fusion Middleware Standard HA Topology in Oracle Fusion
Middleware High Availability Guide.

For more information about the next steps to prepare for high availability after your
domain is configured, see Preparing Your Environment for High Availability.

These server names and will be referenced throughout this document; if you choose
different names be sure to replace them as needed.

Tip:

More information about the options on this screen can be found in Managed
Servers in Oracle Fusion Middleware Creating WebLogic Domains Using the
Configuration Wizard.
Configuring a Cluster for Webgate

Use the Clusters screen to create a new cluster.

**Note:**
If you are configuring a non-clustered setup on a single node, skip this screen.

On the Clusters screen:

1. Click **Add**.
2. Specify `otd_cluster_1` in the Cluster Name field for `oam_server`. For `oam_policy_mgr` server, you must create another cluster, for example, `oam_policy_cluster`.
3. For the Cluster Address field, specify the `ipaddress/hostname:port`. For example: `ip_address_machine1:portnumber`, `ip_address_machine2:portnumber`

Repeat the preceding steps to create three more clusters: `cpt_cluster1`, `ibr_cluster1`, and `wccui_cluster1`.

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, see Considerations for Choosing Unicast or Multicast in Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server.

You can also create clusters using Fusion Middleware Control. In this case, you can configure cluster communication (unicast or multicast) when you create the new cluster. See Create and configure clusters in Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help.

For more information about this screen, see Clusters in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard.

Defining Server Templates

If you are creating dynamic clusters for a high availability setup, use the Server Templates screen to define one or more server templates for domain.

To continue configuring the domain, click **Next**.

For steps to create a dynamic cluster for a high availability setup, see Using Dynamic Clusters in Oracle Fusion Middleware High Availability Guide.

Configuring Dynamic Servers

You can skip this screen for Oracle Access Management configuration.

Click **Next** and proceed.
Assigning Webgate Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign Managed Servers to a new configured cluster. A configured cluster is a cluster you configure manually. You do not use this screen if you are configuring a dynamic cluster, a cluster that contains one or more generated server instances that are based on a server template.

Note:

All Managed Servers of a component type in the domain must belong to that cluster. For example, Webgate domains support only a single Webgate cluster inside each domain.

For more on configured cluster and dynamic cluster terms, see About Dynamic Clusters in Oracle Fusion Middleware Understanding Oracle WebLogic Server.

On the Assign Servers to Clusters screen:

1. In the Clusters pane, select the cluster to which you want to assign the Managed Servers; in this case, otd_cluster_1.
2. In the Servers pane, assign oam_server_1 to oam_cluster_1 by doing one of the following:
   - Click once on oam_server_1 to select it, then click the right arrow to move it beneath the selected cluster (oam_cluster_1) in the Clusters pane.
   - Double-click on oam_server_1 to move it beneath the selected cluster (oam_cluster_1) in the Clusters pane.
3. Repeat to assign oam_policy_mgr to oam_policy_cluster.

For more information about this screen, see Assign Servers to Clusters in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard.

Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster.

Leave the default port number as the Coherence cluster listen port. After configuration, the Coherence cluster is automatically added to the domain.

Note:

Setting the unicast listen port to 0 creates an offset for the Managed Server port numbers. The offset is 5000, meaning the maximum allowed value that you can assign to a Managed Server port number is 60535, instead of 65535.

See Table 5-2 for more information and next steps for configuring Coherence.

For Coherence licensing information, see Oracle Coherence Products in Oracle Fusion Middleware Licensing Information User Manual.
Creating a New Webgate Machine

Use the Machines screen to create new machines in the domain. A machine is required so that Node Manager can start and stop servers.

If you plan to create a high availability environment and know the list of machines your target topology requires, you can follow the instructions in this section to create all the machines at this time. For more about scale out steps, see Optional Scale Out Procedure in Oracle Fusion Middleware High Availability Guide.

To create a new Webgate machine so that Node Manager can start and stop servers:

1. Select the Machine tab (for Windows) or the UNIX Machine tab (for UNIX), then click Add to create a new machine.
2. In the Name field, specify a machine name, such as otd_machine_1.
3. In the Node Manager Listen Address field, select the IP address of the machine in which the Managed Servers are being configured.
   You must select a specific interface and not localhost. This allows Coherence cluster addresses to be dynamically calculated.
4. Verify the port in the Node Manager Listen Port field.
5. Repeat these steps to add more machines, if required.

Note:
If you are extending an existing domain, you can assign servers to any existing machine. It is not necessary to create a new machine unless your situation requires it.

For more information about this screen, see Machines in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard.

Assigning Servers to Webgate Machines

Use the Assign Servers to Machines screen to assign the Administration Server and Managed Servers to the new machine you just created.

On the Assign Servers to Machines screen:

1. In the Machines pane, select the machine to which you want to assign the servers; in this case, otd_machine_1.
2. In the Servers pane, assign AdminServer to otd_machine_1 by doing one of the following:
   • Click once on AdminServer to select it, then click the right arrow to move it beneath the selected machine (otd_machine_1) in the Machines pane.
   • Double-click on AdminServer to move it beneath the selected machine (otd_machine_1) in the Machines pane.
3. Repeat these steps to assign all Managed Servers to their respective machines.
For more information about this screen, see Assign Servers to Machines in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

### Virtual Targets

You can skip this screen for Oracle Access Management configuration.

Click **Next** and proceed.

### Partitions

The Partitions screen is used to configure partitions for virtual targets in WebLogic Server Multitenant (MT) environments. Select **Next** without selecting any options.

For details about options on this screen, see Partitions in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

**Note:**

WebLogic Server Multitenant domain partitions are deprecated in WebLogic Server 12.2.1.4.0 and will be removed in the next release.

### Configuring Domain Frontend Host

The Domain Frontend Host screen can be used to configure the frontend host for the domain.

Select **Plain** or **SSL** and specify the respective host value.

Click **Next**.

### Targeting the Deployments

The Deployments Targeting screen can be used to target the available deployments to the servers.

Make the required modifications, and click **Next**.

### Targeting the Services

The Services Targeting screen can be used to target the available services to the Servers.

Make necessary modifications, and click **Next**.

### Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen shows detailed configuration information for the domain you are about to create.

Review each item on the screen and verify that the information is correct. To make any changes, go back to a screen by clicking the **Back** button or selecting the screen in the navigation pane. Domain creation does not start until you click **Create**.
Writing Down Your Domain Home and Administration Server URL

The End of Configuration screen shows information about the domain you just configured.

Make a note of the following items because you need them later:

• Domain Location
• Administration Server URL

You need the domain location to access scripts that start Node Manager and Administration Server, and you need the URL to access the Administration Server.

Click Finish to dismiss the Configuration Wizard.

Updating the System Properties for SSL Enabled Servers

For SSL enabled servers, you must set the required properties in the setDomainEnv file in the domain home.

Set the following properties in the DOMAIN_HOME/bin/setDomainEnv.sh (for UNIX) or DOMAIN_HOME/bin/setDomainEnv.cmd (for Windows) file before you start the servers:

• -Dweblogic.security.SSL.ignoreHostnameVerification=true
• -Dweblogic.security.TrustKeyStore=DemoTrust

Configuring Oracle Traffic Director WebGate

Complete the following steps after installing Oracle Traffic Director to configure Oracle Traffic Director 12c (12.2.1.4.0) 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:
   
   ./EditObjConf -f Domain_Home/config/fmwconfig/components/OTD/instances/Instance_Name/config/Instance_Name-obj.conf -w webgate_instanceDirectory [-oh Oracle_Home] -ws otd

   For a collocated Oracle Traffic Director installation:
   
   ./EditObjConf -f Domain_Home/config/fmwconfig/components/OTD/Instance_Name/config/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:
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:

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

For a collocated Oracle Traffic Director installation:

./EditObjConf -f Domain_Home/config/fmwconfig/components/OTD/Instance_Name/config/Instance_Name.obj.conf -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 for Oracle Access Manager.

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
Verifying the Configuration of Oracle Traffic Director WebGate

After installing Oracle Traffic Director 12c (12.2.1.4.0) 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 WebGate

Before you can use the new Oracle Traffic Director 12c (12.2.1.4.0) WebGate agent for Oracle Access Manager, you must complete the following tasks:

- Registering the New Oracle Traffic Director 12c (12.2.1.4.0) 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 (12.2.1.4.0) 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 OAM12cRequest.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:
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 OAM12cRequest.xml File**

You must update the agent parameters, such as `agentName`, in the `OAM12cRequest.xml` file in the `RREG_Home\input` directory on Windows. On UNIX, the file is in the `RREG_Home/input` directory.
Note:

The OAM12cRequest.xml file or the short version OAM12cRequest_short.xml is used as a template. You can copy this template file and use it.

Modify the following required parameters in the OAM12cRequest.xml file or in the OAM12cRequest_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 (12.2.1.4.0) WebGate is installed.

- preferredHost
  Specify the host and the port of the machine on which Oracle Traffic Director 12c (12.2.1.4.0) 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 OAM12cRequest.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 OAM12cRequest.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/OAM12cRequest.xml
   ```

   **On Windows:**
   
   ```
   RREG_Home\bin\oamreg.bat inband input\OAM12cRequest.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 OAM12cRequest.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 OAM12cRequest.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 OAM12cRequest.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/OAM12cRequest.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 OAM12cRequest.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 $\text{(Oracle\_Home)}/user\_projects/domains/name\_of\_the\_WebLogic\_domain\_for\_OAM/output/Agent\_ID$ directory.

- On Windows

Complete the following steps:

1. If you are an end user with no access to the server, open the OAM12cRequest.xml file, which is in $\text{RREG\_Home/input}$ directory. $\text{RREG\_Home}$ 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 OAM12cRequest.xml file, which is in $\text{RREG\_Home/input}$. This is the file you received from the end user. Go to your (administrator's) $\text{RREG\_Home}$ directory and run the following command:

   $\text{RREG\_Home/bin/oamreg.bat outofband input/OAM12cRequest.xml}$

   An Agent_ID_Response.xml file is generated on the administrator's machine in the $\text{RREG\_Home/output}$ directory. Send this file to the end user who sent you the updated OAM12cRequest.xml file.

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

   $\text{RREG\_Home/bin/oamreg.bat outofband input/Agent\_ID\_Response.xml}$

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 $\text{(Oracle\_Home)}/user\_projects/domains/name\_of\_the\_WebLogic\_domain\_for\_OAM/output/Agent\_ID$ 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 \texttt{RREG\_Home/output/Agent\_ID} directory:

- \texttt{wallet/cwallet.sso}
- \texttt{cwallet.sso}
- \texttt{ObAccessClient.xml}
- In the \texttt{SIMPLE} mode, RREG generates:
  - \texttt{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.
  - \texttt{aaa\_key.pem}
  - \texttt{aaa\_cert.pem}
- In the \texttt{CERT} mode, RREG generates \texttt{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.

\begin{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 \texttt{aaa\_cert.pem} and \texttt{aaa\_chain.pem} files along with \texttt{password.xml} and \texttt{aaa\_key.pem}.
\end{note}

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 \texttt{RREG\_Home/output/Agent\_ID} directory to the \texttt{webgate\_instanceDirectory} directory.

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

- In \texttt{OPEN} mode, copy the following files from the \texttt{RREG\_Home/output/Agent\_ID} directory to the \texttt{webgate\_instanceDirectory/webgate/config} directory:
  - \texttt{wallet}
  - \texttt{ObAccessClient.xml}
  - \texttt{cwallet.sso}

- In \texttt{SIMPLE} mode, copy the following files from the \texttt{RREG\_Home/output/Agent\_ID} directory to the \texttt{webgate\_instanceDirectory/webgate/config} directory:
  - \texttt{wallet}
  - \texttt{ObAccessClient.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:

  - wallet
  - 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_otd12c.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_otd12c.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.
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:
   ```
   <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:
     ```
     <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:
     ```
     <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:
   ```
   <MW_HOME>/oracle_common/bin/orapki wallet display -wallet ./
   ```
Upgrading to OHS/OTD WebGate

After upgrading from OHS 12c (12.2.1.3.0) WebGate to OHS 12c (12.2.1.4.0) WebGate or OTD 12c (12.2.1.3.0) WebGate to OTD 12c (12.2.1.4.0) 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.