Oracle® Fusion Middleware

Installing WebGates for Oracle Access Manager

12c (12.2.1.4.0)
E95114-08
August 2022

Oracle Fusion Middleware Installing WebGates for Oracle Access Manager, 12c (12.2.1.4.0)

E95114-08

Primary Author: Oracle Corporation

Contents

4 Installing and Configuring Apache 12c WebGate for OAM

6 Installing and Configuring Apache HTTP 2.4 Server WebGate on Windows 64

7 Configuring Oracle Traffic Director WebGate for Oracle Access Manager

Preface

This document provides supporting information for *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*.

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

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:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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:

2

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 12*c* 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 *Adminstrator'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-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

   (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
- 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.

OAM12cRequest.xml Property	Set to...
`serverAddress`	The host and the port of the Administration Server for the Oracle Access Manager domain.
`agentName`	Any custom name for the agent. Typically, you use a name that identifies the Fusion Middleware product you are configuring for single sign-on.
`applicationDomain`	A value that identifies the Web tier host and the FMW component you are configuring for single sign-on.
`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*.
`cachePragmaHeader`	private
`cacheControlHeader`	private

OAM12cRequest.xml Property	Set to...
`ipValidation`	0 `<ipValidation>0</ipValidation>`

`ipValidationExceptions`	The IP address of the front-end load balancer. For example:
	
	`<ipValidationExceptions>`
	`<ipAddress>130.35.165.42</ipAddress>`
	`</ipValidationExceptions>`

`agentBaseUrl`	Fully-qualified URL with the host and the port of the front-end Load Balancer VIP in front of the WEBHOST*n* 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:

   cd *RREG_HOME*/bin/

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

   ```
   chmod +x oamreg.sh
   ```

4. Run the following command:

   ```
   ./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:

  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:

```
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:

```
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.

File	Location
`cwallet.sso`	• *RREG_HOME*`/output/Agent_ID/` - For WebGate 12c (12.2.1.4.0) . • *RREG_HOME*`/output/Agent_ID/wallet` - For WebGate 12c (12.2.1.4.0) and OHS 12c (12.2.1.4.0).
`ObAccessClient.xml`	*RREG_HOME*`/output/Agent_ID/`

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

File	Location
`aaa_key.pem`	*RREG_HOME*`/output/Agent_ID/`
`aaa_cert.pem`	*RREG_HOME*`/output/Agent_ID/`
`password.xml`	*RREG_HOME*`/output/Agent_ID/`

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:

File	Location
`aaa_key.pem`	*RREG_HOME*`/output/Agent_ID/`
`aaa_cert.pem`	*RREG_HOME*`/output/Agent_ID/`
`aaa_chain.pem`	*RREG_HOME*`/output/Agent_ID/`

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*.

File	Location When Using OPEN Mode	Location When Using SIMPLE Mode	Location When Using CERT Mode
`wallet/cwallet.sso`	*`OHS_CONFIG_DIR`*`/webgate/config/wallet`	*`OHS_CONFIG_DIR`*`/webgate/config/wallet/`	*`OHS_CONFIG_DIR`*`/webgate/config/wallet/`
`ObAccessClient.xml`	*`OHS_CONFIG_DIR`*`/webgate/config`	*`OHS_CONFIG_DIR`*`/webgate/config/`	*`OHS_CONFIG_DIR`*`/webgate/config/`
`password.xml`	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/`	*`OHS_CONFIG_DIR`*`/webgate/config/`
`aaa_key.pem`	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/simple/`	*`OHS_CONFIG_DIR`*`/webgate/config/`
`aaa_cert.pem`	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/simple/`	*`OHS_CONFIG_DIR`*`/webgate/config/`
`aaa_chain.pem`	N/A	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/`

> **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.

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*.

3

Installing and Configuring IIS 12*c* WebGate for OAM

This chapter describes how to install and configure Internet Information Services (IIS) 12*c* WebGate for Oracle Access Manager.
This chapter contains the following sections:

Installation Overview of IIS 12*c* WebGate

Installing IIS 12*c* WebGate for Oracle Access Manager involves the following steps:

1. Installing the IIS web server
2. Installing IIS 12*c* WebGate for Oracle Access Manager
3. Completing the post-installation configuration steps
4. Verifying the IIS 12*c* WebGate installation
5. Registering the new WebGate agent

Prerequisites for Installing IIS 12*c* WebGate

This section discusses the following topics:

Oracle Fusion Middleware Certification

The *Oracle Fusion Middleware Supported System Configurations* document provides certification information for Oracle Fusion Middleware, including supported installation types, platforms, operating systems, databases, JDKs, and third-party products related to Oracle Identity and Access Management 12*c*.

You can access the *Oracle Fusion Middleware Supported System Configurations* document by searching the Oracle Technology Network (OTN) web site:

`http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html`

Installing JRE

You must have a 64-bit Java runtime environment (JRE) 11 or higher installed.

Installing Visual C++ Redistributable for Visual Studio 2010 and 2012

You must install Visual C++ Redistributable for Visual Studio 2010 and Visual Studio 2012 Update 4, `vcredist_x64.exe`.

> **WARNING:**
>
> During IIS 12*c* WebGate installation, you might encounter *Supported MS Visual C++ version is not available in this machine* warning if have not installed Visual C++ Redistributable for Visual Studio 2010 and 2012.

For information about downloading, installing, and configuring, see the Microsoft download page and product documentation.

Installing and Configuring IIS

For information about installing and configuring IIS, see the Microsoft HTTP Server product documentation.

Installing and Configuring OAM 12*c*

For information about installing Oracle Access Manager (OAM), see Installing and Configuring Oracle Identity and Access Management Software in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

For information about configuring Oracle Access Manager in a new or existing WebLogic administration domain, see Configuring Oracle Access Management in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

For information about configuring Oracle Access Manager in Open, Simple, or Cert mode, see Securing Communication in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager* .

Installing IIS 12*c* WebGate

This section contains the following topics:

Obtaining the Software

For information about obtaining the IIS 12*c* software, see Oracle Fusion Middleware Download, Installation, and Configuration ReadMe.

Starting the IIS 12*c* WebGate Installer

To start the installation wizard, do the following:

1. Go to the `Disk1` directory under the `WebGate` folder
2. Run the following command:

```
setup_fmw_12.2.1.4.0_iiswebgate_win64.exe
```

After the Installer starts, the **Welcome** screen is displayed. Proceed with the installation by referring to Installation Flow and Procedure of IIS 12*c* WebGate.

Installation Flow and Procedure of IIS 12*c* WebGate

To install IIS 12*c* WebGate for Oracle Access Manager, follow the instructions in Table 3-1.

If you need additional help with any of the installation screens, click **Help** to access the online help.

Table 3-1 Installation Flow of IIS WebGate

No.	Screen	Description and Action Required
1	Welcome Screen	Click **Next** to continue.
2	Prerequisite Checks Screen	Click **Next** to continue.
3	Specify Installation Location Screen	Specify the Middleware home and Oracle home locations. For more information about these directories, see Understanding Your Installation Starting Point in *Planning an Installation of Oracle Fusion Middleware*. Oracle home in case of IIS WebGate is any valid directory, not necessarily in the Middleware home. So, if you do not provide a Middleware home or if you provide an invalid Middleware home, the Installer proceeds without any error. Click **Next** to continue.
4	Installation Summary Screen	Verify the information on this screen. Click **Install** to begin the installation.
5	Installation Progress Screen	Click **Next** to continue.

Table 3-1 (Cont.) Installation Flow of IIS WebGate

No.	Screen	Description and Action Required
6	Installation Complete Screen	Click **Finish** to dismiss the Installer.

Post-Installation Steps for IIS 12c WebGate

This section includes the following topics:

- Deploying the IIS WebGate Instance
- Running the ConfigureIISWebGate.bat Tool

Deploying the IIS WebGate Instance

Create an IIS WebGate instance by using the `deployWebGateInstance.sh` tool from the WebGate Oracle home directory. The WebGate instance directory that you are creating or have provided must be empty.

To deploy the WebGate instance, do the following:

1. Go to the *WebGate_Oracle_Home*`/webgate/IIS/tools/deployWebGate` directory by running the following command:

   ```
   cd WebGate_Oracle_Home/webgate/IIS/tools/deployWebGate
   ```

2. Run the following command:

   ```
   deployWebGateInstance.bat -w WebGate_Instancedir -oh
   WebGate_Oracle_Home -ws WebServer
   ```

   In the preceding command:

   - `WebGate_Instancedir` is the directory in which the new WebGate instances should be created.
   - `WebGate_Oracle_Home` is the WebGate Oracle home directory you specified while installing IIS 12*c* WebGate.
   - `WebServer` is IIS.

   Example:

   ```
   deployWebGateInstance.bat -w /home/wg_instance4iis/ -oh /home/
   Oracle_OAMWebGate1/ -ws IIS
   ```

Running the ConfigureIISWebGate.bat Tool

To run the `ConfigureIISWebGate.bat` tool, do the following:

1. Go to the following directory:

   ```
   cd WebGate_Home\webgate\iis\tools\ConfigureIISConf
   ```

2. Run the following command:

   ```
   ConfigureIISWebGate.bat -oh <WebGateHome> -w <Webgate Instance> -site
   <Web Site Name> [-o <output file>]
   ```

In the preceding command:

- `WebGate_Home` is the full path to the WebGate Oracle home.
- `WebGate_Instancedir` is the directory in which the new WebGate instances are created. This is the same instance directory that you have provided while running the deployWebGateInstance.bat command.
- `SiteName` is the IIS WebServer site name.

Example:

```
ConfigureIISWebGate.bat -oh c:\WGHome -w c:\WGInstance -site "Default Web
Site
```

> **Note:**
>
> Running the `ConfigureIISWebGate.bat` command also updates the WebGate_Oracle_Home\webgate\iis\lib\webgate.ini file with IIS Site ID and WebGate Instance Directory.

Verifying the Installation and Configuration of IIS 12*c* WebGate

After installing IIS 12*c* WebGate for Oracle Access Manager, you can examine the `installDATE-TIME_STAMP.out` log file to verify the installation. The default location of the log is in the following file:

`WebGate_Home``/oraInst.loc`

Getting Started with a New IIS 12*c* WebGate

Before you can use the new IIS 12*C* WebGate agent for Oracle Access Manager, you must complete the following tasks:

- Registering the New IIS 12c WebGate
- Copying Generated Files and Artifacts to the IIS WebGate Instance Location

Registering the New IIS 12*c* WebGate

You can register the new IIS WebGate with Oracle Access Manager by using the Oracle Access Manager Administration Console.

This section includes the following topics:

- Locating and Preparing the RREG Tool
- Updating the OAM12cRequest.xml File
- Running the RREG Tool
- Files and Artifacts Generated by RREG
- Deleting the previous version files
  After installing the newer version of the IIS Webgate, you must manually delete the older files in the configuration folder.

- Restarting the IIS 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 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.

Running the RREG Tool

The following topics provide information about running the RREG tool to register your IIS 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:

   ```
   cd RREG_HOME/bin/
   ```

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

   ```
   chmod +x oamreg.sh
   ```

4. Run the following command:

```
./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:

  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:

```
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:

```
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

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:

- cwallet.sso
- ObAccessClient.xml
- In **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 **CERT** mode, RREG generates password.xml file, 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.

Deleting the previous version files

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

Complete the following steps:

1. Go to the *{Oracle_OAMWebGate1}*/webgate/IIS/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 IIS Instance

Use the startserv command to start or stopserv command to stop your Apache instance.

To stop the server, run the following command:

```
/home/bin/stopserv
```

To start the server, run the following command:

```
export LD_LIBRARY_PATH=/WebGate_Home/lib
```

```
/home/bin/startserv
```

To restart the IIS instance, stop all running instances, and then run the start command.

Copying Generated Files and Artifacts to the IIS 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_Instance_Home* 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_Instance_Home*/webgate/config directory:
  - ObAccessClient.xml
  - cwallet.sso
- In **SIMPLE** mode, copy the following files from the *RREG_Home*/output/*Agent_ID* directory to the *WebGate_Instance_Home*/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_Instance_Home*/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_Instance_Home*/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. Create a certificate request as follows:

   ```
   openssl.exe req -utf8 -new -nodes -config openssl_silent_IIS12c.cnf -
   keyout aaa_key.pem -out aaa_req.pem -rand WebGate_Home/webgate/IIS/
   config/random-seed
   ```

2. Self-sign the certificate as follows:

   ```
   openssl.exe ca -config openssl_silent_IIS12c.cnf -policy
   policy_anything -batch -out aaa_cert.pem -infiles aaa_req.pem
   ```

3. Copy the following generated certificates to the *WebGate_Instance_Home*/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`

Starting the IIS Web Server and Accessing the IIS Resource

To start the IIS web server:

1. From the **Start** menu, select **run**, and type `inetmgr`.
2. Select the **IIS Site** and select **Start** to start the IIS Site.

After you start the IIS Web Server, log in to it by using the following URL:

`http://machine_name.my.company.com:port`

WebGate intercepts the request and redirects you to the Oracle Access Manager console. Enter the username and password, and you are redirected to the Microsoft HTTP Server.

Deinstalling IIS 12*c* WebGate

You should always use the instructions provided in this section for removing the IIS 12*c* WebGate. If you try to remove the software manually, thne you may experience problems when you try to reinstall the software again at a later time. Following the procedures in this chapter will ensure that the software is properly removed.

To deinstall the IIS WebGate, do the following:

1. Go to the *MW_HOME/Webgate_Home*`/oui/bin` directory
2. Run the following command:

   ```
   deinstall.cmd
   ```

After the Installer starts, the **Welcome** screen is displayed. Proceed with the deinstallation by referring to Deinstallation Screens and Instructions.

Deinstallation Screens and Instructions

Follow the instructions in Table 4-2 to complete the deinstallation.

If you need additional help with any of the deinstallation screens, click **Help** to access the online help.

Table 3-2 Deinstallation Flow

Sl. No.	Screen	Description	Action Required
1.	Welcome	Each time the deinstaller starts, the **Welcome** screen is displayed.	Click **Next**.

Table 3-2 (Cont.) Deinstallation Flow

Sl. No.	Screen	Description	Action Required
2.	Deinstall Oracle Home	The **Deinstall Oracle Home** screen shows the Oracle home you are about to deinstall.	Verify the Oracle home you are about to deinstall. Click **Deinstall**. On the Warning screen, select whether or not you want the deinstaller to remove the Oracle home directory in addition to removing the software. Click **Yes** to have the deinstaller remove the software and Oracle home, **No** to remove only the software, or **Cancel** to return to the previous screen. If you select **No**, go to Manually Removing the Oracle Home Directory for instructions on how to manually remove your Oracle home directory.
3.	Deinstallation progress	The **Deinstallation Progress** screen shows the progress and status of the deinstallation.	Wait until the **Deinstallation Complete** screen appears.
4.	Deinstallation Complete	The **Deinstallation Complete** screen appears when the deinstallation is complete.	Click **Finish** to dismiss the screen.

Navigating the Uninstall Wizard Screens

The Uninstall Wizard shows a series of screens to confirm the removal of the software. See, Navigating the Uninstall Wizard Screens.

Manually Removing the Oracle Home Directory

If you have selected **No** on the warning screen during deinstallation, then you must manually remove your *Webgate_Home* directory and any sub-directories.

For example:

On UNIX, if your Oracle WebGate home directory was `/home/Oracle/Middleware/Oracle_OAMWebGate1`, run the following command:

```
cd /home/Oracle/Middleware/

rm -rf Oracle_OAMWebGate1
```

Silent Installation for IIS 12*c*WebGate

To run the IIS 12*c* WebGate in silent mode, complete the following steps:

1. Set the contents of the `silent.rsp` file. For example:

```
[ENGINE]
#DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0
[GENERIC]
ORACLE_HOME=/home/MW_HOME/iis_WebGate_home
MIDDLEWARE_HOME=/home/MW_HOME
[SYSTEM]
[APPLICATIONS]
[RELATIONSHIPS]
```

   In the preceding file, the parameters are as follows:

   - `ORACLE_HOME`: Provide the Oracle home location. This is the directory in which you want to install the new IIS WebGate. The location must be an immediate child folder under the specified Middleware home location. The Oracle home directory name can contain only alphanumeric, hyphen (-), dot (.), and underscore (_) characters, and must begin with an alphanumeric character. The total length must be less than or equal to 128 characters. For example, `home/middleware/iis_webgate`.
   - `MIDDLEWARE_HOME`: Specify the full path to your Middleware home directory.

2. Extract the contents of the installer to a directory.
3. Run the following command:

```
setup_fmw_12.2.1.4.0_iiswebgate_win64.exe -invPtrLoc
Absolute_Path_Of_the_oraInst.loc_file -silent -response
Absolute_Path_Of_the_silent.rsp_file
```

   In the preceding command:

   - `Absolute_Path_Of_the_oraInst.loc_file` is the absolute path to the `oraInst.loc` file.
   - `Absolute_Path_Of_the_ silent.rsp_file` is the absolute path to the `silent.rsp` file you created.

4

Installing and Configuring Apache 12*c* WebGate for OAM

This chapter describes how to install and configure Apache 12*c* WebGate for Oracle Access Manager. For an introduction to WebGates and an overview of installing WebGates, see About WebGates for Oracle Access Manager.
This chapter contains the following sections:

Installation Overview of Apache 12*c* WebGate

Installing Apache 12*c* WebGate for Oracle Access Manager includes the following steps:

1. Installing the Apache web server
2. Installing Apache 12*c* WebGate for Oracle Access Manager
3. Completing the post-installation configuration steps
4. Verifying the Apache 12*c* WebGate installation
5. Registering the new WebGate agent

Prerequisites for Apache 12*c* WebGate

This section discusses the following topics:

Oracle Fusion Middleware Certification

The *Oracle Fusion Middleware Supported System Configurations* document provides certification information for Oracle Fusion Middleware, including supported installation types,

platforms, operating systems, databases, JDKs, and third-party products related to Oracle Identity and Access Management 12*c*.

See *Oracle Fusion Middleware Supported System Configurations* document at http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html.

Installing JRE

You must have a 64-bit Java runtime environment (JRE) 11 or higher installed.

Installing and Configuring Apache 2.4

For information about installing and configuring Apache 2.4, see the Apache product documentation.

Installing and Configuring OAM 12*c*

For information about installing Oracle Access Manager (OAM), see Installing and Configuring Oracle Identity and Access Management Software in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

For information about configuring Oracle Access Manager in a new or existing WebLogic administration domain, see Configuring Oracle Access Management in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

For information about configuring Oracle Access Manager in Open, Simple, or Cert mode, see Securing Communication in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager* .

Installing Apache 12*c* WebGate

This section includes the following topics:

- Obtaining the Software
- Starting the Apache 12c WebGate Installer
- Installation Flow and Procedure of Apache 12c WebGate

Obtaining the Software

For information about obtaining the Apache 12*c* software, see Oracle Fusion Middleware Download, Installation, and Configuration ReadMe.

Starting the Apache 12*c* WebGate Installer

To start the installation wizard, do the following:

1. Go to the directory in which you extracted the contents of the Installer.
2. Run the following command:

   On UNIX:

```
./fmw_12.2.1.4.0_apachewebgate_linux64.bin
```

After the Installer starts, the Welcome screen appears. Continue by referring to the section Installation Flow and Procedure of Apache 12*c* WebGate for installing Apache 12*c* WebGate for Oracle Access Manager.

Installation Flow and Procedure of Apache 12*c* WebGate

To install Apache 12*c* WebGate for Oracle Access Manager, follow the instructions in Table 4-1.

If you need additional help with any of the installation screens, click **Help** to access the online help.

Table 4-1 Installation Flow of Apache WebGate

No.	Screen	Description and Action Required
1	Welcome Screen	Click **Next** to continue.
2	Specify Installation Location Screen	Specify the Middleware home and Oracle home locations. For more information about these directories, see Understanding Your Installation Starting Point in *Planning an Installation of Oracle Fusion Middleware*. Oracle home in case of Apache WebGate is any valid directory, not necessarily in the Middleware home. So, if you do not provide a Middleware home or if you provide an invalid Middleware home, the Installer proceeds without any error. Click **Next** to continue.
3	Prerequisite Checks Screen	Click **Next** to continue.
4	Installation Summary Screen	Verify the information on this screen. Click **Install** to begin the installation.
5	Installation Progress Screen	Click **Next** to continue.
6	Installation Complete Screen	Click **Finish** to dismiss the Installer.

Post-Installation Steps for Apache 12*c* WebGate

This section includes the following topics:

- Deploying the Apache WebGate Instance
- Setting the Environment Variable
- Running the EditHttpConf Tool

Deploying the Apache WebGate Instance

Create an Apache instance by using the `deployWebGateInstance.sh` tool from the Webgate Oracle home directory.

To deploy the WebGate instance, do the following:

1. Go to the *`WebGate_Oracle_Home`*`/webgate/apache/tools/deployWebGate` directory by running the following command:

```
cd WebGate_Oracle_Home/webgate/apache/tools/deployWebGate
```

2. Run the following command:

   ```
   ./deployWebGateInstance -w WebGate_Instancedir -oh WebGate_Oracle_Home
   -ws apache
   ```

   In this command:

   - `WebGate_Instancedir` is the directory in which the new WebGate instances should be created.
   - `WebGate_Oracle_Home` is the WebGate Oracle home directory you specified while installing Apache 12*c* WebGate.
   - Web server is Apache.

Setting the Environment Variable

For Apache webgate, set the environment variable:

- **On Linux**:

  ```
  export LD_LIBRARY_PATH=<Apache24_install_dir>/lib:<webgate_oracle_home>/
  Oracle_OAMWebGate1/webgate/apache/lib
  ```

Running the EditHttpConf Tool

To run the `EditHttpConf` tool, do the following:

1. Go to the *WebGate_Oracle_Home*`/webgate/apache/tools/setup/InstallTools` directory by running the following command:

   ```
   cd WebGate_Oracle_Home/webgate/apache/tools/setup/InstallTools
   ```

2. Run the following command:

   On UNIX:

   ```
   ./EditHttpConf -f /home/webserver-apache24/conf/httpd.conf -oh /home/
   Webgate_Oracle_Home/ -w /home/webserver-apache24/
   webgate_instanceApache/ -ws apache24
   ```

   In the preceding command:

   - `path_to_httpd.conf_file` is the full path of the Apache instance `httpd.conf` file.
   - `WebGate_Instance_Dir` is the directory in which new WebGate instances are created.
   - `WebGate_Oracle_Home` is the full path to the WebGate Oracle home.
   - The name of the webserver is `WebServer`. For Apache 2.4, use `apache24`.

   For example:

   On Apache 2.4:

   ```
   cd /home/OAMWebGate1/webgate/apache/tools/setup/InstallTools/
   ```

   ```
   ./EditHttpConf -f /home/webserver-apache24/conf/httpd.conf -oh /home/
   Webgate_Oracle_Home/ -w /home/webgate_instance4Apache/ -ws apache24
   ```

Verifying the Installation and Configuration of Apache 12*c* WebGate

After installing Apache 12*c* WebGate for Oracle Access Manager, you can examine the `installDATE-TIME_STAMP.out` log file to verify the installation. The default location of the log is in the following file:

WebGate_Home`/oraInst.loc`

Getting Started with a New Apache 12*c* WebGate

Before you can use the new Apache 12*c* WebGate for Oracle Access Manager, you must complete the following tasks:

- Registering the New WebGate Agent for Apache 12c WebGate
- Copying Generated Artifacts to the Apache 12c WebGate Instance Location
- Deleting the previous version files
  After installing the newer version of the Apache Webgate, you must manually delete the older files in the configuration folder.
- Restarting the Apache Instance

Registering the New WebGate Agent for Apache 12*c* WebGate

You can register the new WebGate with Oracle Access Manager by using the Oracle Access Manager Administration Console.

This section includes the following topics:

- 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

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.

OAM12cRequest.xml Property	Set to...
`serverAddress`	The host and the port of the Administration Server for the Oracle Access Manager domain.
`agentName`	Any custom name for the agent. Typically, you use a name that identifies the Fusion Middleware product you are configuring for single sign-on.
`applicationDomain`	A value that identifies the Web tier host and the FMW component you are configuring for single sign-on.
`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*.
`cachePragmaHeader`	private
`cacheControlHeader`	private

OAM12cRequest.xml Property	Set to...
ipValidation	0 <ipValidation>0</ipValidation>
ipValidationExceptions	The IP address of the front-end load balancer. For example: <ipValidationExceptions> <ipAddress>130.35.165.42</ipAddress> </ipValidationExceptions>
agentBaseUrl	Fully-qualified URL with the host and the port of the front-end Load Balancer VIP in front of the WEBHOST*n* 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:

   cd *RREG_HOME*/bin/

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

   ```
   chmod +x oamreg.sh
   ```

4. Run the following command:

   ./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:

  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:

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:

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.

File	Location
cwallet.sso	• *RREG_HOME*/output/Agent_ID/ - For WebGate 12c (12.2.1.4.0) . • *RREG_HOME*/output/Agent_ID/wallet - For WebGate 12c (12.2.1.4.0) and OHS 12c (12.2.1.4.0).
ObAccessClient.xml	*RREG_HOME*/output/Agent_ID/

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

File	Location
aaa_key.pem	*RREG_HOME*/output/Agent_ID/
aaa_cert.pem	*RREG_HOME*/output/Agent_ID/
password.xml	*RREG_HOME*/output/Agent_ID/

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:

File	Location
aaa_key.pem	*RREG_HOME*/output/Agent_ID/
aaa_cert.pem	*RREG_HOME*/output/Agent_ID/
aaa_chain.pem	*RREG_HOME*/output/Agent_ID/

Copying Generated Artifacts to the Apache 12c 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 Apache configuration directory on the Web tier host.

The location of the files in the Apache 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 Apache 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*.

File	Location When Using OPEN Mode	Location When Using SIMPLE Mode	Location When Using CERT Mode
`wallet/cwallet.sso`	*`OHS_CONFIG_DIR`*`/webgate/config/wallet`	*`OHS_CONFIG_DIR`*`/webgate/config/wallet/`	*`OHS_CONFIG_DIR`*`/webgate/config/wallet/`
`ObAccessClient.xml`	*`OHS_CONFIG_DIR`*`/webgate/config`	*`OHS_CONFIG_DIR`*`/webgate/config/`	*`OHS_CONFIG_DIR`*`/webgate/config/`
`password.xml`	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/`	*`OHS_CONFIG_DIR`*`/webgate/config/`
`aaa_key.pem`	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/simple/`	*`OHS_CONFIG_DIR`*`/webgate/config/`
`aaa_cert.pem`	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/simple/`	*`OHS_CONFIG_DIR`*`/webgate/config/`
`aaa_chain.pem`	N/A	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/`

> **Note:**
>
> `aaa_chain.pem` is generated when certificates are created for CERT mode.

- Generating a New Certificate
- Migrating an Existing Certificate

Generating a New Certificate

You can generate a new certificate as follows:

1. Create a certificate request as follows:

   ```
   openssl req -utf8 -new -nodes -config openssl_silent_ohs12c.cnf -
   keyout aaa_key.pem -out aaa_req.pem -rand WebGate_Home/webgate/ohs/
   config/random-seed
   ```

2. Self-sign the certificate as follows:

   ```
   openssl ca -config openssl_silent_ohs12c.cnf -policy policy_anything -
   batch -out aaa_cert.pem -infiles aaa_req.pem
   ```

3. Copy the following generated certificates to the *WebGate_Instance_Home*/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

Deleting the previous version files

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

Complete the following steps:

1. Go to the *{Oracle_OAMWebGate1}*/webgate/apache/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 Apache Instance

Use the startserv command to start or stopserv command to stop your Apache instance.

To stop the server, run the following command:

/home/bin/stopserv

To start the server, run the following command:

export LD_LIBRARY_PATH=*/WebGate_Home*/lib

/home/bin/startserv

To restart the Apache instance, stop all running instances, and then run the start command.

Deinstalling Apache 12*c* WebGate

You should always use the instructions provided in this section for removing the Apache 12*c* WebGate for Oracle Access Manager. If you try to remove the software manually, then you may experience problems when you try to reinstall the software again at a later time. Following the procedures in this section will ensure that the software is properly removed.

To deinstall the WebGate agent, do the following:

1. Go to the *MW_HOME/Webgate_Home*/oui/bin directory on UNIX.
2. Run the following command:

   On UNIX: ./runInstaller -deinstall

   Ensure that you specify the absolute path to your *JRE_LOCATION*; relative paths are not supported.

After the deinstaller starts, the **Welcome** screen is displayed. Proceed with the deinstallation by referring to Deinstallation Screens and Instructions.

- Deinstallation Screens and Instructions
- Manually Removing the Oracle Home Directory

Deinstallation Screens and Instructions

Follow the instructions in Table 4-2 to complete the deinstallation.

If you need additional help with any of the deinstallation screens, click **Help** to access the online help.

Table 4-2 Deinstallation Flow

Sl. No.	Screen	Description	Action Required
1.	Welcome	Each time the deinstaller starts, the **Welcome** screen is displayed.	Click **Next**.
2.	Deinstall Oracle Home	The **Deinstall Oracle Home** screen shows the Oracle home you are about to deinstall.	Verify the Oracle home you are about to deinstall. Click **Deinstall**. On the Warning screen, select whether or not you want the deinstaller to remove the Oracle home directory in addition to removing the software. Click **Yes** to have the deinstaller remove the software and Oracle home, **No** to remove only the software, or **Cancel** to return to the previous screen. If you select **No**, go to Manually Removing the Oracle Home Directory for instructions on how to manually remove your Oracle home directory.
3.	Deinstallation progress	The **Deinstallation Progress** screen shows the progress and status of the deinstallation.	Wait until the **Deinstallation Complete** screen appears.
4.	Deinstallation Complete	The **Deinstallation Complete** screen appears when the deinstallation is complete.	Click **Finish** to dismiss the screen.

Manually Removing the Oracle Home Directory

If you have selected **No** on the warning screen during deinstallation, then you must manually remove your *Webgate_Home* directory and any sub-directories.

For example:

On UNIX, if your Oracle WebGate home directory was `/home/Oracle/Middleware/Oracle_OAMWebGate1`, run the following command:

```
cd /home/Oracle/Middleware/

rm -rf Oracle_OAMWebGate1
```

Silent Installation for Apache 12*c* WebGate

To run the Apache 12*c* WebGate in silent mode, complete the following steps:

1. Set the contents of the `silent.rsp` file. For example:

```
[ENGINE]
#DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0
[GENERIC]
ORACLE_HOME=/home/MW_HOME/apache_WebGate_home
#Set this variable value to the Installation Type selected. to ApacheWebgate.
INSTALL_TYPE=ApacheWebgate
[SYSTEM]
[APPLICATIONS]
[RELATIONSHIPS]
```

In the preceding file, the parameters are as follows:

- `ORACLE_HOME`: Provide the Oracle home location. This is the directory in which you want to install the new Apache WebGate. The location must be an immediate child folder under the specified Middleware home location. The Oracle home directory name can contain only alphanumeric, hyphen (-), dot (.), and underscore (_) characters, and must begin with an alphanumeric character. The total length has to be less than or equal to 128 characters. For example, `home/middleware/apache_webgate`.

2. Set the contents of the `oraInst.loc` file. For example:

```
#Oracle Installer Location File Location
inst_group=<group_name (like dba/root/oracle etc.)>
inventory_loc=<location of oraInventory like (/home/testuser/oraInventory)>
```

3. Run the following command:

```
WebGate_Installer_Directory/fmw_12.2.1.4.0_apachewebgate_linux64.bin -invPtrLoc
Absolute_Path_Of_the_oraInst.loc_file -silent -responseFile
Absolute_Path_Of_the_silent.rsp_file
```

In the preceding command:

- `WebGate_Installer_Directory` is the absolute path to the directory in which you have extracted the contents of the WebGate installer.
- `Absolute_Path_Of_the_oraInst.loc_file` is the absolute path to the `oraInst.loc` file like `/home/testuser/oraInst.loc`.
- `Absolute_Path_Of_the_ silent.rsp_file` is the absolute path to the `silent.rsp` file you created like /home/testuser/silent.rsp.

5

Installing and Configuring IHS 12*c* WebGate for OAM

This chapter describes how to install and configure IBM HTTP Server (IHS) 12*c* WebGate for Oracle Access Manager (OAM).
This chapter contains the following sections:

Installation Overview of IHS 12*c* WebGate

Installing IHS 12*c* WebGate for Oracle Access Manager involves the following steps:

1. Installing IHS 12*c* WebGate for Oracle Access Manager
2. Completing the post-installation configuration steps
3. Verifying the IHS 12*c* WebGate installation
4. Registering the new IHS 12cWebGate agent

Prerequisites for Installing IHS 12*c* WebGate

This section discusses the following topics:

Oracle Fusion Middleware Certification

The *Oracle Fusion Middleware Supported System Configurations* document provides certification information for Oracle Fusion Middleware, including supported installation types,

platforms, operating systems, databases, JDKs, and third-party products related to Oracle Identity and Access Management 12*c* .

You can access the *Oracle Fusion Middleware Supported System Configurations* document at:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

Installing JRE

You must have a 64-bit Java runtime environment (JRE), 11 or higher installed.

Installing and Configuring IHS

For information about installing and configuring IHS, see the IBM HTTP Server product documentation.

> **Note:**
>
> IHS 12*c* WebGate is supported on IHS Web Server version 9.x only.

Installing and Configuring OAM 12*c*

For information about installing Oracle Access Manager (OAM), see Installing and Configuring Oracle Identity and Access Management Software in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

For information about configuring Oracle Access Manager in a new or existing WebLogic administration domain, see Configuring Oracle Access Management in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

For information about configuring Oracle Access Manager in Open, Simple, or Cert mode, see Securing Communication in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager* .

Installing IHS 12*c* WebGate

This section contains the following topics:

Obtaining the Software

For information about obtaining the IHS 12*c* software, see Oracle Fusion Middleware Download, Installation, and Configuration ReadMe.

Starting the IHS 12*c* WebGate Installer

To start the installation wizard, do the following:

1. Go to the directory in which you extracted the contents of the Installer.
2. Run the following command:

   On Linux: `./fmw_12.2.1.4.0_ihswebgate_linux64.bin`

> **Note:**
>
> Follow silent mode installation for OEL 8. GUI mode installation is not supported.

After the Installer starts, the Welcome screen appears. Continue by referring to the section Installation Flow and Procedure of IHS 12*c* WebGate for installing IHS 12*c* WebGate for Oracle Access Manager.

Installation Flow and Procedure of IHS 12*c* WebGate

To install IHS 12*c* WebGate for Oracle Access Manager, follow the instructions in Table 5-1.

If you need additional help with any of the installation screens, then click **Help** to access the online help.

Table 5-1 Installation Flow of IHS 12*c* WebGate

No.	Screen	Description and Action Required
1.	Welcome Screen	Click **Next** to continue.
2.	Prerequisite Checks Screen	Click **Next** to continue.
3.	Specify Installation Location Screen	Specify the Middleware home and Oracle home locations. For more information about these directories, see Understanding Your Installation Starting Point in *Planning an Installation of Oracle Fusion Middleware*. Click **Next** to continue.
4.	Installation Summary Screen	Verify the information on this screen. Click **Install** to begin the installation.
5.	Installation Progress Screen	Click **Next** to continue.
6.	Installation Complete Screen	Click **Finish** to dismiss the Installer.

Post-Installation Steps for IHS 12*c* WebGate

This section includes the following topics:

- Deploying the IHS WebGate Instance
- Setting the Environment Variables
- Running the EditHttpConf Tool

Deploying the IHS WebGate Instance

Create an IHS WebGate instance by using the `deployWebGateInstance.sh` tool from the WebGate Oracle home directory. The WebGate instance directory that you are creating or have provided must be empty.

To deploy the WebGate instance, do the following:

1. Go to the *WebGate_Oracle_Home*`/webgate/ihs/tools/deployWebGate` directory by running the following command:

   `cd` *WebGate_Oracle_Home*`/webgate/ihs/tools/deployWebGate`

2. Run the following command:

   `./deployWebGateInstance.sh -w` *WebGate_Instancedir* `-oh` *WebGate_Oracle_Home* `-ws` *WebServer*

   In the preceding command:

   - `WebGate_Instancedir` is the directory in which the new WebGate instances should be created.
   - `WebGate_Oracle_Home` is the WebGate Oracle home directory you specified while installing IHS 12*c* WebGate.
   - `WebServer` is ihs24.

   Example:

   ```
   ./deployWebGateInstance.sh -w /home/wg_instance4ihs/ -oh /home/
   Oracle_OAMWebGate1/ -ws ihs24
   ```

Setting the Environment Variables

Set the environment variable `LD_LIBRARY_PATH` on Linux, and `LIBPATH` on AIX, to *WebGate_Oracle_Home*`/webgate/ihs/lib`.

Example:

On Linux

```
export LD_LIBRARY_PATH=/home/Oracle_OAMWebGate1/webgate/ihs/lib
```

On AIX

```
export LIBPATH=/home/Oracle_OAMWebGate1/webgate/ihs/lib
```

```
export LDR_PRELOAD64=libclntsh.so
```

Running the EditHttpConf Tool

To run the `EditHttpConf` tool, do the following:

1. Go to the *WebGate_Oracle_Home*`/webgate/ihs/tools/setup/InstallTools` directory, by running the following command:

   `cd` *WebGate_Oracle_Home*`/webgate/ihs/tools/setup/InstallTools`

2. Run the following command:

```
./EditHttpConf -f path_to_webserver_config_file -w WebGate_Instance_Dir -oh
WebGate_Oracle_Home -ws WebServer
```

In the preceding command:

- `path_to_webserver_config_file` is the full path of the IHS instance `httpd.conf` file.
- `WebGate_Instance_Dir` is the directory in which the new WebGate instance is created.
- `WebGate_Oracle_Home` is the full path to the WebGate Oracle home.
- `WebServer` is ihs24.

> **Note:**
>
> The `-oh` parameter is optional and the command runs without any error, even if you do not specify it.

Example:

```
cd /home/OAMWebGate1/webgate/ihs/tools/setup/InstallTools/

./EditHttpConf -f /home/instanceHome1/net-test_ihs1/config/test_httpd.conf -
oh /home/Oracle_OAMWebGate1/ -w /home/Oracle_OAMWebGate1/wg_instance4ihs/ -
ws ihs24
```

Verifying the Installation and Configuration of IHS 12*c* WebGate

After installing IHS 12*c* WebGate for Oracle Access Manager, you can examine the `installDATE-TIME_STAMP.out` log file to verify the installation. The default location of the log is in the following file:

WebGate_Home`/oraInst.loc`

Getting Started with a New IHS 12*c* WebGate

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

- Registering the New IHS 12c WebGate
- Copying Generated Files and Artifacts to the IHS 12c WebGate Instance Location
- Restarting the IHS Instance

Registering the New IHS 12*c* WebGate

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

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

- Locating and Preparing the RREG Tool
- Running the RREG Tool

- Updating the Standard Properties in the OAM12cRequest.xml File

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.

Running the RREG Tool

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

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

```
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/`

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:

   `cd` *RREG_HOME*`/bin/`

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

   ```
   chmod +x oamreg.sh
   ```

4. Run the following command:

   `./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:

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.
```

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.

OAM12cRequest.xml Property	Set to...
`serverAddress`	The host and the port of the Administration Server for the Oracle Access Manager domain.
`agentName`	Any custom name for the agent. Typically, you use a name that identifies the Fusion Middleware product you are configuring for single sign-on.
`applicationDomain`	A value that identifies the Web tier host and the FMW component you are configuring for single sign-on.
`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*.

OAM12cRequest.xml Property	Set to...
`cachePragmaHeader`	private
`cacheControlHeader`	private
`ipValidation`	0 `<ipValidation>0</ipValidation>`

`ipValidationExceptions`	The IP address of the front-end load balancer. For example:
	
	`<ipValidationExceptions>`
	`<ipAddress>130.35.165.42</ipAddress>`
	`</ipValidationExceptions>`

`agentBaseUrl`	Fully-qualified URL with the host and the port of the front-end Load Balancer VIP in front of the WEBHOST*n* 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.

OAM12cRequest.xml Property	Set to...

`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>`

Copying Generated Files and Artifacts to the IHS 12*c* 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_Instance_Home* 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_Instance_Home*/webgate/config directory:
  - ObAccessClient.xml
  - cwallet.sso
- In **SIMPLE** mode, copy the following files from the *RREG_Home*/output/*Agent_ID* directory to the *WebGate_Instance_Home*/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_Instance_Home*/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_Instance_Home*/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 *WebGate_Home*/webgate/ihs/tools/openssl directory.
2. Create a certificate request as follows:

   ```
   ./openssl req -utf8 -new -nodes -config openssl_silent_ihs12c.cnf -keyout aaa_key.pem -out aaa_req.pem -rand WebGate_Home/webgate/ihs/config/random-seed
   ```

3. Self-sign the certificate as follows:

   ```
   ./openssl ca -config openssl_silent_ihs12c.cnf -policy policy_anything -batch -out aaa_cert.pem -infiles aaa_req.pem
   ```

4. Copy the following generated certificates to the *WebGate_Instance_Home*/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), then ensure that you use the same passphrase which 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, then the password.xml file generated by RREG will not match the passphrase used to encrypt the key.

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

1. Go to the *WebGate_Instance_Home*/webgate/config directory.
2. Copy the following certificates to the *WebGate_Instance_Home*/webgate/config directory:
   - aaa_key.pem

- `aaa_cert.pem`
- `aaa_chain.pem`

Restarting the IHS Instance

Use the `startserv` command to start or `stopserv` command to stop your Apache instance.

To stop the server, run the following command:

`/home/bin/stopserv`

To start the server, run the following command:

On Linux

```
export LD_LIBRARY_PATH=/WebGate_Home/lib
/home/bin/startserv
```

On AIX

```
export LIBPATH=/home/Oracle_OAMWebGate1/webgate/ihs/lib
export LDR_PRELOAD64=libclntsh.so
/home/bin/startserv
```

To restart the IHS instance, stop all running instances, and then run the start command.

Starting the IHS Web Server and Accessing the IHS Resource

To start the IHS web server:

- **On Linux**

  Run the following command:

  ```
  /IBM/HTTPServer/bin/apachectl -k start
  ```

- **On AIX**

  1. Go to the `httpd.conf` file at `/IHS/HTTPServer/conf/httpd.conf`, open it in a text editor, and add the following:

     ```
     ThreadStackSize 2097152
     ```

  2. Run the following command:

     ```
     /IBM/HTTPServer/bin/apachectl -k start
     ```

After you start the IHS Web Server, log in to it by using the following URL:

`http://machine_name.my.company.com:port`

WebGate intercepts the request and redirects you to the Oracle Access Manager console. Enter the username and password, and you are redirected to the IBM HTTP Server.

Deinstalling IHS 12*c* WebGate

You should always use the instructions provided in this section for removing the IHS 12c WebGate. If you try to remove the software manually, thne you may experience problems when you try to reinstall the software again at a later time. Following the procedures in this chapter will ensure that the software is properly removed.

To deinstall the IHS WebGate, do the following:

1. Go to the *MW_HOME/Webgate_Home*`/oui/bin` directory
2. Run the following command:

```
./deinstall.sh
```

After the Installer starts, the **Welcome** screen is displayed, proceed with deinstallation.

- Deinstallation Screens and Instructions
- Manually Removing the Oracle Home Directory

Deinstallation Screens and Instructions

Follow the instructions in Table 5-2 to complete the deinstallation.

If you need additional help with any of the deinstallation screens, then click **Help** to access the online help.

Table 5-2 Deinstallation Flow

Sl. No.	Screen	Description	Action Required
1.	Welcome	Each time the deinstaller starts, the **Welcome** screen is displayed.	Click **Next**.
2.	Deinstall Oracle Home	The **Deinstall Oracle Home** screen shows the Oracle home you are about to deinstall.	Verify the Oracle home you are about to deinstall. Click **Deinstall**. On the Warning screen, select whether or not you want the deinstaller to remove the Oracle home directory in addition to removing the software. Click **Yes** to have the deinstaller remove the software and Oracle home, **No** to remove only the software, or **Cancel** to return to the previous screen. If you select **No**, go to Manually Removing the Oracle Home Directory for instructions on how to manually remove your Oracle home directory.

Table 5-2 (Cont.) Deinstallation Flow

Sl. No.	Screen	Description	Action Required
3.	Deinstallation progress	The **Deinstallation Progress** screen shows the progress and status of the deinstallation.	Wait until the **Deinstallation Complete** screen appears.
4.	Deinstallation Complete	The **Deinstallation Complete** screen appears when the deinstallation is complete.	Click **Finish** to dismiss the screen.

Manually Removing the Oracle Home Directory

If you have selected **No** on the warning screen during deinstallation, then you must manually remove your *WebGate_Home* directory and any sub-directories. For example: if your Oracle WebGate home directory was `/home/Oracle/Middleware/Oracle_OAMWebGate1`, run the following command:

```
cd /home/Oracle/Middleware/

rm -rf Oracle_OAMWebGate1
```

On Windows, if your Oracle Common home directory was `C:\Oracle\Middleware\Oracle_OAMWebGate1`, then use a file manager window, go to the `C:\Oracle\Middleware` directory, right-click on the `Oracle_OAMWebGate1` folder, and then select **Delete**.

Silent Installation for IHS 12*c* WebGate

To run the IHS 12*c* WebGate in silent mode, complete the following steps:

1. Set the contents of the `silent.rsp` file. For example:

```
[ENGINE]
#DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0
[GENERIC]
ORACLE_HOME=/home/MW_HOME/ihs_WebGate_home
MIDDLEWARE_HOME=/home/MW_HOME
[SYSTEM]
[APPLICATIONS]
[RELATIONSHIPS]
```

   In the preceding file, the parameters are as follows:

   - `ORACLE_HOME`: Provide the Oracle home location. This is the directory in which you want to install the new IHS WebGate. The location must be an immediate child folder under the specified Middleware home location. The Oracle home directory name can contain only alphanumeric, hyphen (-), dot (.), and underscore (_) characters, and must begin with an alphanumeric character. The total length must be less than or equal to 128 characters. For example, `home/middleware/ihs_webgate`.

- `MIDDLEWARE_HOME`: Specify the full path to your Middleware home directory.

2. Extract the contents of the installer to a directory.
3. Run the following command:

   `fmw_12.2.1.4.0_ihswebgate_linux64.bin` `-invPtrLoc` *`Absolute_Path_Of_the_oraInst.loc_file`* `-silent -response` *`Absolute_Path_Of_the_silent.rsp_file`*

   In the preceding command:

   - `Absolute_Path_Of_the_oraInst.loc_file` is the absolute path to the `oraInst.loc` file.
   - `Absolute_Path_Of_the_ silent.rsp_file` is the absolute path to the `silent.rsp` file you created.

6

Installing and Configuring Apache HTTP 2.4 Server WebGate on Windows 64

This chapter describes how to install and configure Apache HTTP 2.4 Server WebGate on Windows 64.
This chapter contains the following sections:

Installation Overview of Apache HTTP 2.4 Server WebGate

Installing Apache HTTP 2.4 Server WebGate for Windows 64 includes the following steps:

1. Installing the Apache Web Server.
2. Installing Apache HTTP 2.4 Server WebGate for Windows.
3. Completing the post-installation configuration steps.
4. Verifying the Apache HTTP 2.4 Server WebGate installation.
5. Registering the new WebGate agent.

Prerequisites for Apache HTTP 2.4 Server WebGate

This section discusses the following topics:

Oracle Fusion Middleware Certification

The *Oracle Fusion Middleware Supported System Configurations* document provides certification information for Oracle Fusion Middleware, including supported installation types, platforms, operating systems, databases, JDKs, and third-party products related to Oracle Identity and Access Management 12*c*.

See *Oracle Fusion Middleware Supported System Configurations* document at http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html.

Installing JRE

You must have a 64-bit Java runtime environment (JRE) 11 or higher installed.

Installing Visual C++ Redistributable for Visual Studio 2010 and 2012

You must install Visual C++ Redistributable for Visual Studio 2010 and Visual Studio 2012 Update 4, `vcredist_x64.exe`.

> **WARNING:**
>
> During Apache HTTP 2.4 Server WebGate installation, you might encounter *Supported MS Visual C++ version is not available in this machine* warning if have not installed Visual C++ Redistributable for Visual Studio 2010 and 2012.

For information about downloading, installing, and configuring, see the Microsoft download page and product documentation.

Installing and Configuring Apache 2.4

For information about installing and configuring Apache 2.4, see the Apache product documentation.

Installing and Configuring OAM 12*c*

For information about installing Oracle Access Manager (OAM), see Installing and Configuring Oracle Identity and Access Management Software in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

For information about configuring Oracle Access Manager in a new or existing WebLogic administration domain, see Configuring Oracle Access Management in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

For information about configuring Oracle Access Manager in Open, Simple, or Cert mode, see Securing Communication in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager* .

Installing Apache HTTP 2.4 Server WebGate

This section includes the following topics:

Obtaining the Software

For information about obtaining the Apache HTTP 2.4 Server WebGate software, see Oracle Fusion Middleware Download, Installation, and Configuration ReadMe.

Starting the Apache HTTP 2.4 Server WebGate Installer

To start the installation wizard, do the following:

1. Go to the directory in which you extracted the contents of the Installer.
2. Run the following file:

```
setup_fmw_12.2.1.4.0_apache24webgate_win64.exe
```

After the Installer starts, the Welcome screen appears. Continue by referring to the section Installation Flow and Procedure of Apache HTTP 2.4 Server WebGate for installing Apache HTTP 2.4 Server WebGate for Oracle Access Manager.

Installation Flow and Procedure of Apache HTTP 2.4 Server WebGate

To install Apache HTTP 2.4 Server WebGate for Oracle Access Manager, follow the instructions in Table 6-1.

If you need additional help with any of the installation screens, click **Help** to access the online help.

Table 6-1 Installation Flow of Apache HTTP 2.4 Server WebGate

No.	Screen	Description and Action Required
1	Welcome Screen	Click **Next** to continue.
2	Specify Installation Location Screen	Specify the Middleware home and Oracle home locations. For more information about these directories, see Understanding Your Installation Starting Point in *Planning an Installation of Oracle Fusion Middleware*. Oracle home in case of Apache WebGate is any valid directory, not necessarily in the Middleware home. So, if you do not provide a Middleware home or if you provide an invalid Middleware home, the Installer proceeds without any error. Click **Next** to continue.

Table 6-1 (Cont.) Installation Flow of Apache HTTP 2.4 Server WebGate

No.	Screen	Description and Action Required

3	Prerequisite Checks Screen	Ignore if you encounter the following error:
		`Expected result: 0.0`
		`Actual result: 11.0, 12.0`
		`Check complete. The overall result of this check is: Failed`
		`Problem: Supported MS Visual C++ version is not available in this machine`
		`Recommendation: Install expected MS Visual C++ version`
		Click **Next** to continue.

4	Installation Summary Screen	Verify the information on this screen. Click **Install** to begin the installation.
5	Installation Progress Screen	Click **Next** to continue.
6	Installation Complete Screen	Click **Finish** to dismiss the Installer.

Post-Installation Steps for Apache HTTP 2.4 Server WebGate

This section includes the following topics:

- Deploying the Apache HTTP 2.4 Server WebGate Instance
- Setting the Environment Variable
- Running the EditHttpConf Tool

Deploying the Apache HTTP 2.4 Server WebGate Instance

Create an Apache instance by using the `$WEBGATE_HOME\webgate\apache\tools\deployWebGate` tool from the Webgate Oracle home directory.

To deploy the WebGate instance, do the following:

1. Go to the *`WebGate_Oracle_Home`*`\webgate\apache\tools\deployWebGate` directory by running the following command:

   ```
   cd WebGate_Oracle_Home\webgate\apache\tools\deployWebGate
   ```

2. Run the following command:

   ```
   deployWebGateInstance.bat -w c:\Apachewg -oh C:\WebgateHome -ws apache
   ```

   In this command:

   - `WebGate_Instancedir` is the directory in which the new WebGate instances should be created.
   - `WebGate_Oracle_Home` is the WebGate Oracle home directory you specified while installing Apache HTTP 2.4 Server WebGate.

- `-ws apache` is the Web Server that is used to pass as an argument in Apache.

Setting the Environment Variable

For Apache HTTP 2.4 Server WebGate, set the environment variable:

```
PATH=$WEBGATE_HOME\webgate\apache\lib;%PATH%
```

Running the EditHttpConf Tool

To run the `EditHttpConf` tool, do the following:

1. Go to the *$WebGate_Oracle_Home*`\webgate\apache\tools\EditHttpConf` directory by running the following command:

   ```
   cd WebGate_Oracle_Home\webgate\apache\tools\EditHttpConf
   ```

2. Run the following command:

   ```
   EditHttpConf.exe -w c:\Apachewg -f c:\Apache24\conf\httpd.conf -ws apache24
   -oh C:\WebgateHome
   ```

   In the preceding command:

   - `path_to_httpd.conf_file` is the full path of the Apache instance `httpd.conf` file.
   - `WebGate_Instance_Dir` is the directory in which new WebGate instances are created.
   - `WebgateHome` is the full path to the WebGate Oracle home.
   - The name of the webserver is `WebServer`. For Apache 2.4, use `apache24`.

   For example:

   On Apache 2.4:

   ```
   cd WebGate_Oracle_Home\webgate\apache\tools\EditHttpConf
   ```

   ```
   EditHttpConf -f \home\webserver-apache24\conf\httpd.conf -oh
   \home\Webgate_Oracle_Home\ -w \home\webgate_instance4Apache\ -ws apache24
   ```

Verifying the Installation and Configuration of Apache HTTP 2.4 Server WebGate

After installing Apache HTTP 2.4 Server WebGate for Oracle Access Manager, you can examine the `installDATE-TIME_STAMP.out` log file to verify the installation. The default location of the log is in the following file:

WebGate_Home`/oraInst.loc`

Getting Started with a New Apache HTTP 2.4 Server WebGate

Before you can use the new Apache HTTP 2.4 Server WebGate for Oracle Access Manager, you must complete the following tasks:

- Registering the New WebGate Agent for Apache HTTP 2.4 Server WebGate
- Copying Generated Artifacts to the Apache HTTP 2.4 Server WebGate Instance Location

- Deleting the previous version files

Registering the New WebGate Agent for Apache HTTP 2.4 Server WebGate

You can register the new WebGate with Oracle Access Manager by using the Oracle Access Manager Administration Console.

This section includes the following topics:

- Locating and Preparing the RREG Tool
- Updating the OAM11gRequest.xml File
- Running the RREG Tool
- Files and Artifacts Generated by RREG

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 OAM11gRequest.xml File

You must update the agent parameters, such as `agentName`, in the `OAM11GRequest.xml` file 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 11*g* WebGate is installed.

- `preferredHost`

  Specify the host and the port of the machine on which Oracle Traffic Director 11*g* 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.

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:

   cd *RREG_HOME*/bin/

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

   chmod +x oamreg.sh

4. Run the following command:

   ./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:

  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:

```
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:

```
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

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:

- `cwallet.sso`
- `ObAccessClient.xml`
- RREG from OAM 11.1.2.3 will generate two cwallet.ss:
  - `rreg/output/<webgate_id>/cwallet.sso`
  - `rreg/output/<webgate_id>/wallet/cwallet.sso`
- For WebGate 11.1.2.2, copy `rreg/output/<webgate_id>/cwallet.sso` to the `WebGate_Instance_Home/webgate/config/ folder.`
- For WebGate 11.1.2.3, copy `rreg/output/<webgate_id>/wallet/cwallet.sso` to the `WebGate_Instance_Home/webgate/config/wallet/ folder`

- In **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 **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 Artifacts to the Apache HTTP 2.4 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 Apache configuration directory on the Web tier host.

The location of the files in the Apache 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 Apache 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*.

File	Location When Using OPEN Mode	Location When Using SIMPLE Mode	Location When Using CERT Mode
wallet/cwallet.sso	*OHS_CONFIG_DIR*/webgate/config/wallet	*OHS_CONFIG_DIR*/webgate/config/wallet/	*OHS_CONFIG_DIR*/webgate/config/wallet/
ObAccessClient.xml	*OHS_CONFIG_DIR*/webgate/config	*OHS_CONFIG_DIR*/webgate/config/	*OHS_CONFIG_DIR*/webgate/config/
password.xml	N/A	*OHS_CONFIG_DIR*/webgate/config/	*OHS_CONFIG_DIR*/webgate/config/
aaa_key.pem	N/A	*OHS_CONFIG_DIR*/webgate/config/simple/	*OHS_CONFIG_DIR*/webgate/config/
aaa_cert.pem	N/A	*OHS_CONFIG_DIR*/webgate/config/simple/	*OHS_CONFIG_DIR*/webgate/config/
aaa_chain.pem	N/A	N/A	*OHS_CONFIG_DIR*/webgate/config/

> **Note:**
>
> aaa_chain.pem is generated when certificates are created for CERT mode.

- Generating a New Certificate
- Migrating an Existing Certificate

Generating a New Certificate

You can generate a new certificate as follows:

1. Go to the *WebGate_Home*/webgate/apache/tools/openssl directory.
2. Create a certificate request as follows:

   ```
   ./openssl req -utf8 -new -nodes -config openssl_silent_apache11g.cnf -
   keyout aaa_key.pem -out aaa_req.pem -rand WebGate_Home/webgate/apache/
   config/random-seed
   ```

3. Self-sign the certificate as follows:

   ```
   ./openssl ca -config openssl_silent_apache11g.cnf -policy
   policy_anything -batch -out aaa_cert.pem -infiles aaa_req.pem
   ```

4. Copy the following generated certificates to the *WebGate_Instance_Home*/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`), then 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, then the `password.xml` file generated by RREG will not match the passphrase used to encrypt the key.

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

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

Deleting the previous version files

After installing the newer version of the Apache HTTP 2.4 Server WebGate, you must manually delete the older files in the configuration folder.

Complete the following steps:

1. Go to the *`{Oracle_OAMWebGate1}`*`/webgate/apache/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 Apache HTTP 2.4 Server WebGate Instance

To stop the server, run the following command:

```
httpd.exe -k stop
```

To start the server, run the following command:

```
SET PATH=$WEBGATE_HOME\webgate\apache\lib;%PATH%
httpd.exe -k start
```

To restart the Apache HTTP 2.4 Server WebGate instance, stop all running instances, and then run the start command.

Deinstalling Apache HTTP 2.4 Server WebGate

You should always use the instructions provided in this section for removing the Apache HTTP 2.4 Server WebGate for Oracle Access Manager. If you try to remove the software manually, then you may experience problems when you try to reinstall the software again at a later time. Following the procedures in this section will ensure that the software is properly removed.

To deinstall the WebGate agent, do the following:

1. Go to the *MW_HOME/Webgate_Home*/oui/bin directory on Windows.
2. Run the following command:

```
deinstall.cmd
```

> **Note:**
>
> Ensure that you specify the absolute path to your *JRE_LOCATION*; relative paths are not supported.

After the deinstaller starts, the **Welcome** screen is displayed, proceed with the deinstallation.

- Deinstallation Screens and Instructions
- Manually Removing the Oracle Home Directory

Deinstallation Screens and Instructions

Follow the instructions in Table 6-2 to complete the deinstallation.

If you need additional help with any of the deinstallation screens, then click **Help** to access the online help.

Table 6-2 Deinstallation Flow

Sl. No.	Screen	Description	Action Required
1.	Welcome	Each time the deinstaller starts, the **Welcome** screen is displayed.	Click **Next**.

Table 6-2 (Cont.) Deinstallation Flow

Sl. No.	Screen	Description	Action Required
2.	Deinstall Oracle Home	The **Deinstall Oracle Home** screen shows the Oracle home you are about to deinstall.	Verify the Oracle home you are about to deinstall. Click **Deinstall**. On the Warning screen, select whether or not you want the deinstaller to remove the Oracle home directory in addition to removing the software. Click **Yes** to have the deinstaller remove the software and Oracle home, **No** to remove only the software, or **Cancel** to return to the previous screen. If you select **No**, go to Manually Removing the Oracle Home Directory for instructions on how to manually remove your Oracle home directory.
3.	Deinstallation progress	The **Deinstallation Progress** screen shows the progress and status of the deinstallation.	Wait until the **Deinstallation Complete** screen appears.
4.	Deinstallation Complete	The **Deinstallation Complete** screen appears when the deinstallation is complete.	Click **Finish** to dismiss the screen.

Manually Removing the Oracle Home Directory

If you have selected **No** on the warning screen during deinstallation, then you must manually remove your *Webgate_Home* directory and any sub-directories. For example: if your Oracle WebGate home directory was `\home\Oracle\Middleware\Oracle_OAMWebGate1`, run the following command:

```
cd \home\Oracle\Middleware\

rm -rf Oracle_OAMWebGate1
```

On Windows, if your Oracle Common home directory was `C:\Oracle\Middleware\Oracle_OAMWebGate1`, then use a file manager window, go to the `C:\Oracle\Middleware` directory, right-click on the `Oracle_OAMWebGate1` folder, and then select **Delete**.

Silent Installation for Apache HTTP 2.4 Server WebGate

To run the Apache HTTP 2.4 Server WebGate in silent mode, complete the following steps:

1. Set the contents of the `silent.rsp` file. For example:

```
[ENGINE]
#DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0
[GENERIC]
ORACLE_HOME=/home/MW_HOME/apache_WebGate_home
#Set this variable value to the Installation Type selected. to ApacheWebgate.
INSTALL_TYPE=ApacheWebgate
[SYSTEM]
[APPLICATIONS]
[RELATIONSHIPS]
```

In the preceding file, the parameters are as follows:

- `ORACLE_HOME`: Provide the Oracle home location. This is the directory in which you want to install the new Apache WebGate. The location must be an immediate child folder under the specified Middleware home location. The Oracle home directory name can contain only alphanumeric, hyphen (-), dot (.), and underscore (_) characters, and must begin with an alphanumeric character. The total length has to be less than or equal to 128 characters. For example, `home/middleware/apache_webgate`.

2. Set the contents of the `oraInst.loc` file. For example:

```
#Oracle Installer Location File Location
inst_group=<group_name (like dba/root/oracle etc.)>
inventory_loc=<location of oraInventory like (/home/testuser/oraInventory)>
```

3. Run the following command:

```
WebGate_Installer_Directory/setup_fmw_12.2.1.4.0_apache24webgate_win64.exe -
invPtrLoc Absolute_Path_Of_the_oraInst.loc_file -silent -responseFile
Absolute_Path_Of_the_silent.rsp_file
```

In the preceding command:

- `WebGate_Installer_Directory` is the absolute path to the directory in which you have extracted the contents of the WebGate installer.
- `Absolute_Path_Of_the_oraInst.loc_file` is the absolute path to the `oraInst.loc` file like `/home/testuser/oraInst.loc`.
- `Absolute_Path_Of_the_ silent.rsp_file` is the absolute path to the `silent.rsp` file you created like `/home/testuser/silent.rsp`.

7

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.

> **Note:**
>
> As of 12.2.1.4.0, Oracle Traffic Director is deprecated. In the future, for equivalent functionality, use Oracle HTTP Server, Microsoft IIS Web Server, or Apache HTTP Server plug-ins, or a native Kubernetes load balancer, such as Traefik.

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.
- Configuring Domain Frontend Host
  The Domain Frontend Host screen can be used to configure the frontend host for the domain.
- Targeting the Deployments
  The Deployments Targeting screen can be used to target the available deployments to the servers.
- Targeting the Services
  The Services Targeting screen can be used to target the available services to the Servers.
- Reviewing Your Configuration Specifications and Configuring the Domain
  The Configuration Summary screen shows detailed configuration information for the domain you are about to create.
- Writing Down Your Domain Home and Administration Server URL
  The End of Configuration screen shows information about the domain you just configured.

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:**
>
> To extend the B2B domain from SOA domain, select B2B classic template instead of Oracle B2B Reference Configuration template. Extending a reference-configured SOA domain is not supported.

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 theWebgate template.

Selecting this template automatically selects the following as dependencies:

- Oracle Enterprise Manager
- Oracle JRF
- WebLogic Coherence Cluster Extension

> **Note:**
>
> The basic WebLogic domain is pre-selected.

More information about the options on this screen can be found in Templates in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

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.

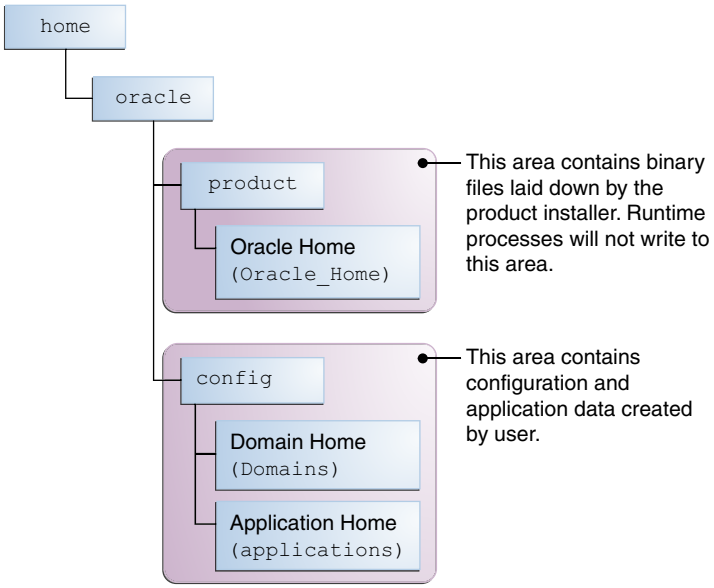
Fusion Middleware documentation refers to the Application home directory as *APPLICATION_HOME* and includes all folders up to and including the domain name. For example, if you name your domain `exampledomain` and you locate your application data in the `/home/oracle/config/applications` directory, the 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 7-1.

Figure 7-1 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:

Field	Description
DBMS/Service	Enter the database DBMS name, or service name if you selected a service type driver. Example: `orcl.exampledomain.com`
Host Name	Enter the name of the server hosting the database. Example: `examplehost.exampledomain.com`
Port	Enter the port number on which the database listens. Example: `1521`
Schema Owner Schema Password	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 *`prefix`*`_STB`, where *`prefix`* is the custom prefix that you defined in the RCU.

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:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK

Successfully Done.
```

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`.

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**.

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

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/*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:

   ```
   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:

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 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_Hom`*e 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 Consolein 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 `OAM12cRequest.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 `OAM12cRequest.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\OAM12cRequest.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 `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 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
  - 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:
  - wallet
  - 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:

  - 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.

8

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 ./
   ```

9

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 artificats to WebGate. See Regenerating, Copying, and Configuring the WebGate Artifacts.

  OR

- Manually add `SHA256` certificate to the existing WebGate `cwallet.sso` after deleting `md5 cert`.

> **Note:**
>
> OHS WebGate is included as part of the Oracle HTTP Server 12c installation and is upgraded as part of the Oracle HTTP Server upgrade process through Upgrade Assistant. For more information, see Upgrading Oracle HTTP Server from 11g to 12c and Upgrading Oracle HTTP Server from a Previous 12c Release.
>
> OTD WebGate is included as part of Oracle Traffic Director 12c installation and is upgraded as part of the Oracle Traffic Director upgrade process through Upgrade Assistant. For more information, see Upgrading Oracle Traffic Director from 11g Release and Upgrading Oracle Traffic Director from an Earlier or a Previous 12c Release.

This section contains following topic:

- Regenerating, Copying, and Configuring the WebGate Artifacts

Regenerating, Copying, and Configuring the WebGate Artifacts

This section provides information about regenerating, copying, and configuring the WebGate artifacts:

Regenerating the WebGate Artifacts

You can regenerate the WebGate artifacts by making the minor change to the WebGate that you want to regenerate.

Following are the steps to regenerate the WebGate artifacts:

1. Log in to the OAM Console.
2. Click **Agents**.
3. Search for the **Agent** you are interested in, and then click on it to bring up the **configuration** page. For example: Webgate_IDM_11g.

4. Change one of the existing values and click **Apply** (you can always change it back and apply again). This will regenerate the Agent forcefully.
5. Click **Download**. The Agent Config will be downloaded to your machine.

Copying Artifacts to the WEBHOSTs

Copy the file that was downloaded on your host for each of the WebGate machines.

Configuring the WebGate

Log in to each of your WEBHOSTs and use the uploaded file to configure the WebGates.

Following are the steps to configure the WebGates:

1. Change Directory to the WebGate configuration directory

   For example:

   ```
   cd /u02/private/oracle/config/domains/ohsDomain/config/fmwconfig/
   components/OHS/ohs1/webgate
   ```

2. Unzip the file you uploaded. You should place the files in the correct locations inside the config.

   > **Note:**
   >
   > If you need to redeploy the `ObAccessClient.xml` to WEBHOST1 and WEBHOST2, delete the cached copy of `ObAccessClient.xml` and its lock file, and `ObAccessClient.xml.lck` from the servers.
   >
   > The cache location on WEBHOST1 is: `WEB_DOMAIN_HOME/servers/ohs1/cache/`.

3. Restart the Oracle HTTP Server.