Oracle® Fusion Middleware

Installing WebGates for Oracle Access Manager

14c (14.1.2.0.0)
F85518-01
December 2024

ORACLE

Oracle Fusion Middleware Installing WebGates for Oracle Access Manager, 14c (14.1.2.0.0)

F85518-01

Primary Author: Oracle Corporation

Contents

4 Installing and Configuring Apache WebGate for OAM

5 Installing and Configuring IHS WebGate for OAM

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 14c (14.1.2.0.0) 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 14c (14.1.2.0.0) documentation library:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*
- *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, review the preupgrade requirements for your deployment.

Before you configure Oracle HTTP Server WebGate, you must have installed and configured a certified version of Oracle Access Manager. 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 14c (14.1.2.0.0), the WebGate software is installed as part of the Oracle HTTP Server 14c (14.1.2.0.0) 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  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

Oracle Access Manager WebGate component utilizes a high availability environment to eliminate a single point of failure and to distribute the workload using a load balancer (LBR). OAM needs to be registered only once, the same resulting artifacts are used by all the OAM WebGates that are behind the LBR.

You can register the new WebGate agent with Oracle Access Manager using any one of the following options:

Oracle Access Manager Administration console

For complete information about registering WebGate agent using Oracle Access Manager console, see Registering an OAM Agent Using the Console in *Administrator's Guide for Oracle Access Management*.

RREG tool

For complete information about registering WebGate agent using RREG tool, see:

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 OAM11gRequest.xml File

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

> **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 (`OAM11gRequest_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`/idm/oam/server/rreg/input`

   If you are using out-of-band mode, then change directory to the location where you unpacked the RREG archive on the WEBHOST1 server.
2. Make a copy of the `OAM11gRequest.xml` file template with an environment-specific name.

   ```
   cp OAM11gRequest.xml OAM11gRequest_edg.xml
   ```
3. Review the properties listed in the file, and then update your copy of the `OAM11gRequest.xml` file to make sure the properties reference the host names and other values specific to your environment.

OAM11gRequest.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.

OAM11gRequest.xml Property	Set to...
`security`	Must be set to the security mode configured on the Oracle Access Management server. The mode options are open or certificate. **Note:** 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
`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 14c (14.1.2.0.0) 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.

OAM11gRequest.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>`

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

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

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

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

1. The Oracle Access Manager server administrator provides you with a copy of the RREG archive file (`RREG.tar.gz`).

   The server administrator can find it in the location described in Updating the Standard Properties in the OAM11gRequest.xml File.

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

   For example:

   ```
   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 OAM11gRequest.xml File to update the OAM11gRequest.xml file, and send the completed OAM11gRequest.xml file to the Oracle Access Manager server administrator.
4. The Oracle Access Manager server administrator then uses the instructions in Running the RREG Tool in Out-Of-Band Mode to run the RREG Tool and generate the *AgentID*_response.xml file.
5. The Oracle Access Manager server administrator sends the *AgentID*_response.xml file to you.
6. Use the instructions in Running the RREG Tool in Out-Of-Band Mode to run the RREG Tool with the *AgentID*_response.xml file and generate the required artifacts and files on the client system.

Running the RREG Tool in In-Band Mode

To run the RREG Tool in in-band mode:

1. Navigate to the RREG home directory.

   If you are using in-band mode, the RREG directory is inside the Oracle Access Manager Oracle home:

   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/OAM11gRequest_edg.xml

In this example:

- It is assumed the edited OAM11gRequest.xml file is located in the *RREG_HOME*/input directory.
- The output from this command will be saved to the following directory:

  RREG_HOME/output/

The following example shows a sample RREG session:

```
Welcome to OAM Remote Registration Tool!
Parameters passed to the registration tool are:
Mode: inband
Filename: /u01/oracle/products/fmw/iam_home/oam/server/rreg/client/rreg/input/
OAM11gRequest_edg.xml
Enter admin username:weblogic_idm
Username: weblogic_idm
```

```
Enter admin password:
Do you want to enter a Webgate password?(y/n):
n
Do you want to import an URIs file?(y/n):
n

----------------------------------------
Request summary:
OAM11g Agent Name: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/OAM11gRequest.xml
```

In this example:

- Replace *RREG_HOME* with the location where the RREG archive file was unpacked on the server.
- The edited `OAM11gRequest.xml` file is located in the *RREG_HOME*`/input` directory.
- The RREG Tool saves the output from this command (the *AgentID*`_response.xml` file) to the following directory:

  ```
  RREG_HOME/output/
  ```

  The Oracle Access Manager server administrator can then send the *AgentID*`_response.xml` to the user who provided the `OAM11gRequest.xml` file.

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

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

In this example:

- Replace *RREG_HOME* with the location where you unpacked the RREG archive file on the client system.
- The *AgentID*`_response.xml` file, which was provided by the Oracle Access Manager server administrator, is located in the *RREG_HOME*/input directory.
- The RREG Tool saves the output from this command (the artifacts and files required to register the Webgate software) to the following directory on the client machine:

RREG_HOME/output/

Files and Artifacts Generated by RREG

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

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

OAM_ORACLE_HOME/oam/server/rreg/client

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

File	Location
cwallet.sso	• *RREG_HOME*/output/Agent_ID/ - For WebGate 14c (14.1.2.0.0) . • *RREG_HOME*/output/Agent_ID/wallet - For WebGate 14c (14.1.2.0.0) and OHS 14c (14.1.2.0.0).
ObAccessClient.xml	*RREG_HOME*/output/Agent_ID/

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
password.xml	*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 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:**
>
> 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 CERT Mode
`wallet/cwallet.sso`	*`OHS_CONFIG_DIR`*`/webgate/config/wallet`	*`OHS_CONFIG_DIR`*`/webgate/config/wallet/`
`ObAccessClient.xml`	*`OHS_CONFIG_DIR`*`/webgate/config`	*`OHS_CONFIG_DIR`*`/webgate/config/`
`password.xml`	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/`
`aaa_key.pem`	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/`
`aaa_cert.pem`	N/A	*`OHS_CONFIG_DIR`*`/webgate/config/`
`aaa_chain.pem`	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/`

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 *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 *Administering Oracle HTTP Server*.

Enabling Support for Legacy Resource WebGates

In 14c (14.1.2.0.0), the use of MD5 hashing by older WebGates will cause errors when using legacy 12.2.1.4.0 resources with your 14.1.2.0.0 resources. If you are using legacy components in 14c (14.1.2.0.0), then you will need to explicitly enable MD5 usage in 14*c* WebGates after installation.

The 14c (14.1.2.0.0) WebGate has changed the hashing algorithms which makes it incompatible with 12.2.1.4.0 WebGates. If you are using legacy components in 14c (14.1.2.0.0), then you will need to explicitly enable MD5 after the installation.

For a 14.1.2.0.0 WebGate acting as DCC, if you wish to enable support for legacy Resource WebGates, you will need to add the following user-defined parameter in the 14c (14.1.2.0.0) WebGate profile:

```
dccForLegacyRWG=true
```

For a 14.1.2.0.0 WebGate acting as a Resource WebGate to a 12.2.1.4.0 or older DCC WebGate, you will need to add the following user-defined parameter in the 14c (14.1.2.0.0) WebGate profile:

```
rwgForLegacyDCC=true
```

> **Note:**
>
> The 14c (14.1.2.0.0) WebGate will work in 12.2.1.4.0 compatibility mode with this setting.

3

Installing and Configuring IIS WebGate for OAM

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

Installation Overview of IIS WebGate

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

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

Prerequisites for Installing IIS 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.

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) 17 or higher installed.

Installing Visual C++ Redistributable for Visual Studio

You must install Visual C++ Redistributable for Visual Studio for Windows 2015 - 2022 (or later).

> **WARNING:**
>
> During IIS 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.

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 Oracle Access Manager

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 or Cert mode, see Securing Communication in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager* .

Installing IIS WebGate

This section contains the following topics:

Obtaining the Software

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

Starting the IIS 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_14.1.2.0.0_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 WebGate.

Installation Flow and Procedure of IIS WebGate

To install IIS 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.
6	Installation Complete Screen	Click **Finish** to dismiss the Installer.

Post-Installation Steps for IIS WebGate

This section includes the following topics:

Deploying the IIS WebGate Instance

Create an IIS WebGate instance by using the `deployWebGateInstance.bat` 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:

   ```
   (UNIX) ./deployWebGateInstance.sh -w WebGate_Instancedir -oh
   WebGate_Oracle_Home
   ```

   ```
   (Windows) deployWebGateInstance.bat -w WebGate_Instancedir -oh
   WebGate_Oracle_Home
   ```

   In the preceding command:

   - `WebGate_Instancedir` is the directory in which the new WebGate instances should be created. This directory should be outside of the WebGate Oracle Home.
   - `WebGate_Oracle_Home` is the WebGate Oracle home directory you specified while installing IIS WebGate.
   - `WebServer` is IIS.

Example:

```
deployWebGateInstance.bat -w c:\Oracle\wg_instance4iis -oh
C:\Oracle\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:\Oracle\Oracle_OAMWebGate1 -w
   c:\Oracle\wg_instance4iis -site "Default WebSite" -o configure_iis.log
   ```

> **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.
>
> Review output file created by ConfigureIISWebGate.bat for any errors.

Verifying the Installation and Configuration of IIS WebGate

After installing IIS 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 WebGate

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

Registering the New IIS WebGate

Oracle Access Manager WebGate component utilizes a high availability environment to eliminate a single point of failure and to distribute the workload using a load balancer (LBR). OAM needs to be registered only once, the same resulting artifacts are used by all the OAM WebGates that are behind the LBR.

You can register the new IIS WebGate with Oracle Access Manager by using any one of the following options:

Oracle Access Manager Administration console

For complete information about registering WebGate agent using Oracle Access Manager console, see Registering an OAM Agent Using the Console in *Administrator's Guide for Oracle Access Management*.

RREG tool

For complete information about registering WebGate agent using RREG tool, see:

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 14c (14.1.2.0.0) WebGate is installed.
- `preferredHost`

  Specify the host and the port of the machine on which Oracle Traffic Director 14c (14.1.2.0.0) 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

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 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 OAM11gRequest.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 `OAM14cRequest.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 `OAM14cRequest.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 **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`.

Restarting the IIS Instance

> **Note:**
>
> Before you restart the IIS instance, you must update the system PATH environment variables.
>
> Add `<IIS_Webgate_Home>\bin` and `<IIS_Webgate_Home>\webgate\iis\lib` to the system PATH environment variable.

To stop the server, run the following command:

```
iisreset /stop
```

To start the server, run the following command:

```
iisreset /start
```

To restart the IIS instance, run the following command:

```
iisreset
```

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 **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

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.

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

Deinstalling IIS WebGate

You should always use the instructions provided in this section for removing the IIS 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**.
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.

Table 3-2 (Cont.) Deinstallation Flow

Sl. No.	Screen	Description	Action Required
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:

If your Oracle WebGate home directory was `C:\Oracle\Oracle_OAMWebgate1`, run the following command:

```
cd C:\Oracle

del /F Oracle_OAMWebgate1
```

Silent Installation for IIS WebGate

To run the IIS 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]

#Set this to true if you wish to skip software updates
DECLINE_AUTO_UPDATES=true

#My Oracle Support User Name
MOS_USERNAME=

#My Oracle Support Password
MOS_PASSWORD=<SECURE VALUE>

#If the Software updates are already downloaded and available on your local system,
then specify the path to the directory where these patches are available and set
SPECIFY_DOWNLOAD_LOCATION to true
AUTO_UPDATES_LOCATION=

#Proxy Server Name to connect to My Oracle Support
SOFTWARE_UPDATES_PROXY_SERVER=
```

```
#Proxy Server Port
SOFTWARE_UPDATES_PROXY_PORT=

#Proxy Server Username
SOFTWARE_UPDATES_PROXY_USER=

#Proxy Server Password
SOFTWARE_UPDATES_PROXY_PASSWORD=<SECURE VALUE>

#The oracle home location. This can be an existing Oracle Home or a new Oracle Home
ORACLE_HOME=C:\home\MW_HOME\iis_WebGate_home

#The federated oracle home locations. This should be an existing Oracle Home.
Multiple values can be provided as comma seperated values
FEDERATED_ORACLE_HOMES=

#The jdk home location.
JDK_HOME=C:\jdk17
```

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/MW_HOME/iis_WebGate_home`.

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

```
setup_fmw_14.1.2.0.0_iiswebgate_win64.exe -silent -responseFile
Absolute_Path_Of_the_silent.rsp_file
```

In the preceding command:

- `Absolute_Path_Of_the_ silent.rsp_file` is the absolute path to the `silent.rsp` file you created.

4

Installing and Configuring Apache WebGate for OAM

This chapter describes how to install and configure Apache 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 WebGate

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

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

Prerequisites for Apache 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.

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) 17 or higher installed.

You can download the latest JRE from the following download site:

```
http://www.oracle.com/technetwork/java/javase/downloads/index.html
```

Installing and Configuring Apache 2.4

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

Installing and Configuring OAM

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 or Cert mode, see Securing Communication in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager* .

Installing Apache WebGate

This section includes the following topics:

Obtaining the Software

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

Starting the Apache 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:

```
(UNIX) ./fmw_14.1.2.0.0_apachewebgate_linux64.bin

(Windows) fmw_14.1.2.0.0_apachewebgate_win64.bat
```

After the Installer starts, the Welcome screen appears. Continue by referring to the section Installation Flow and Procedure of Apache 14*c* WebGate for installing Apache WebGate for Oracle Access Manager.

Installation Flow and Procedure of Apache 14*c* WebGate

To install Apache 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.

Table 4-1 (Cont.) Installation Flow of Apache WebGate

No.	Screen	Description and Action Required
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 WebGate

This section includes the following topics:

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 WebGate.
   - Web server is Apache.

Setting the Environment Variable

For Apache WebGate, set the environment variable:

- **On Linux**:

```
export LD_LIBRARY_PATH="$APACHE_HOME:$WEBGATE_ORACLE_HOME/lib:$LD_LIBRARY_PATH"
```

- **On Windows**:

```
set PATH=%WEBGATE_ORACLE_HOME%\bin;%PATH%
```

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
   ```

   On Windows:

   ```
   \EditHttpConf.bat \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 WebGate

After installing Apache 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 WebGate

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

Registering the New WebGate Agent for Apache WebGate

Oracle Access Manager WebGate component utilizes a high availability environment to eliminate a single point of failure and to distribute the workload using a load balancer (LBR). OAM needs to be registered only once, the same resulting artifacts are used by all the OAM WebGates that are behind the LBR.

You can register the new WebGate agent with Oracle Access Manager using any one of the following options:

Oracle Access Manager Administration console

For complete information about registering WebGate agent using Oracle Access Manager console, see Registering an OAM Agent Using the Console in *Administrator's Guide for Oracle Access Management*.

RREG tool

For complete information about registering WebGate agent using RREG tool, see:

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 OAMRequest.xml File

Before you can register the Webgate agent with Oracle Access Manager, you must update some required properties in the `OAMRequest.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 (`OAM14cRequest_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 `OAMRequest.xml` file template with an environment-specific name.

   ```
   cp OAMRequest.xml OAMRequest_edg.xml
   ```
3. Review the properties listed in the file, and then update your copy of the `OAMRequest.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.

OAM12cRequest.xml Property	Set to...
`security`	Must be set to the security mode configured on the Oracle Access Management server to either open or certificate. **Note:** 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
`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 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>`

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

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 OAMRequest.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 OAMRequest.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 14c (14.1.2.0.0) . • *RREG_HOME*/output/Agent_ID/wallet - For WebGate 14c (14.1.2.0.0) and OHS 14c (14.1.2.0.0).
ObAccessClient.xml	*RREG_HOME*/output/Agent_ID/

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
password.xml	*RREG_HOME*/output/Agent_ID/

Copying Generated Artifacts to the Apache 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 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.

File	Location When Using OPEN Mode	Location When Using CERT Mode
wallet/cwallet.sso	*APACHE_CONFIG_DIR*/webgate/config/wallet	*APACHE_CONFIG_DIR*/webgate/config/wallet/
ObAccessClient.xml	*APACHE_CONFIG_DIR*/webgate/config	*APACHE_CONFIG_DIR*/webgate/config/

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 WebGate

You should always use the instructions provided in this section for removing the Apache 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

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**.

Table 4-2 (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:

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 WebGate

To run the Apache 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_14.1.2.0.0_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 WebGate for OAM

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

Installation Overview of IHS WebGate

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

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

Prerequisites for Installing IHS 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.

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.

Installing and Configuring OAM 14c (14.1.2.0.0)

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 or Cert mode, see Securing Communication in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager* .

Installing IHS WebGate

This section contains the following topics:

Obtaining the Software

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

Starting the IHS 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_14.1.2.0.0_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 WebGate for installing IHS WebGate for Oracle Access Manager.

Installation Flow and Procedure of IHS WebGate

To install IHS 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 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.

Table 5-1 (Cont.) Installation Flow of IHS WebGate

No.	Screen	Description and Action Required
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 WebGate

This section includes the following topics:

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 14*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 WebGate

After installing HIS 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 WebGate

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

Registering the New IHS WebGate

Oracle Access Manager WebGate component utilizes a high availability environment to eliminate a single point of failure and to distribute the workload using a load balancer (LBR). OAM needs to be registered only once, the same resulting artifacts are used by all the OAM WebGates that are behind the LBR.

You can register the new WebGate agent with Oracle Access Manager using any one of the following options:

Oracle Access Manager Administration console

For complete information about registering WebGate agent using Oracle Access Manager console, see Registering an OAM Agent Using the Console in *Administrator's Guide for Oracle Access Management*.

RREG tool

For complete information about registering WebGate agent using RREG tool, see:

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

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 OAMRequest.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 OAMRequest.xml File to update the `OAM14cRequest.xml` file, and send the completed `OAM14cRequest.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 OAM14cRequest.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 OAM14cRequest.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/OAM14cRequest_edg.xml
```

In this example:

- It is assumed the edited `OAM14cRequest.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/
OAM14cRequest_edg.xml
Enter admin username:
Username:
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:
OAM14c Agent Name:SOA14120_EDG_AGENT
Base URL:
URL String:null
Registering in Mode:inband
Your registration request is being sent to the Admin server at:
---------------------------------------

Jul 08, 2024 7:18:13 PM oracle.security.jps.util.JpsUtil disableAudit
INFO: JpsUtil: isAuditDisabled set to true
Jul 08, 2024 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 OAMRequest.xml File

Before you can register the Webgate agent with Oracle Access Manager, you must update some required properties in the `OAMRequest.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 (`OAMRequest_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 `OAM14cRequest.xml` file template with an environment-specific name.

   ```
   cp OAM14cRequest.xml OAM14cRequest_edg.xml
   ```

3. Review the properties listed in the file, and then update your copy of the `OAM14cRequest.xml` file to make sure the properties reference the host names and other values specific to your environment.

OAM14cRequest.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 either be open or certificate. **Note:** 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

OAM14cRequest.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 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>

Copying Generated Files and Artifacts to the HIS 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 **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

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
     ```

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 WebGate

You should always use the instructions provided in this section for removing the IHS 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

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.
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 WebGate

To run the IHS 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_14.1.2.0.0_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
Upgrading OHS WebGate

OHS WebGate is included as part of the Oracle HTTP Server installation and is upgraded as part of the Oracle HTTP Server upgrade process through Upgrade Assistant. Upgrading Oracle HTTP Server.

7

Upgrading Non-OHS WebGate

This document describes the steps needed to upgrade an existing 12c (12.2.1.4.0) WebGates environment for non-OHS web containers, such as Apache, IHS and IIS to 14c (14.1.2.0.0).

Prerequisites for Upgrading Non-OHS WebGate from 12c (12.2.1.4.0) to 14c (14.1.2.0.0)

- Verifying Certification and System Requirements

  Review the certification matrix and system requirements documents to verify that your environment meets the necessary requirements. Beofre you begin the upgrade, verify that all prerequisites for OS certifications, Web Server (Apache, IHS or IIS), and VC Runtime version (Windows) are satisfied.

  Whenever new certifications occur, they are added to the appropriate certification document right away. New certifications can occur at any time, and for this reason the certification documents are kept outside of the documentation libraries and are available on Oracle Technical Resources. See the Certification Matrix for 14c (14.1.2.0.0).

  > **Note:**
  >
  > When checking the certification, system requirements, and interoperability information, be sure to check specifically for any operating system requirements. It is important for you to download software specifically designed for your operating system environment, explicitly.

- Verify That the JDK Is Certified for This Release of Oracle Fusion Middleware

  You must have a 64-bit Java runtime environment (JRE) 17 or higher installed.

  Refer to the Oracle Fusion Middleware Supported System Configurations information on the Oracle Technology Network (OTN) to verify that the JDK you are using is supported.

- Switch to OAP over REST (if needed)

  If WebGate to be upgraded is using OAP over TCP for communicating with OAM Server, switch it to use OAP over REST

- Create a Complete Backup

  Ensure that your exiting installation of 12.2.1.4.0 WebGate is backed up and copied to a different location.

Installing Webgate for Apache / IHS / IIS

Install the new WebGate for Apache, IHS and IIS 14c (14.1.2.0.0) in the same location as previous 12c WebGate installation. For detailed instructions on how to obtain and install the new versions, see the previous installation chapters in this guide:

- Installing Apache WebGate
- Installing IIS WebGate
- Installing IHS WebGate

Post-Installation Steps for WebGate Upgrade

- Maintaining Customized Scripts and Configuration Files

As the new WebGate 14c (14.1.2.0.0) software is installed at the same location as your previous 12c (12.2.1.4.0) WebGate installation, references to WebGate Oracle Home in various configurations (like Web Server configuration files, custom scripts, etc) will remain valid for WebGate instances referring to this installation.

Exceptions:

- If the WebGate instance directory for the older 12.2.1.4.0 installation was under the WebGate Oracle Home and was moved during the backup step above, you will have to copy / restore it under new 14c installation at the same location.
- You may need to update Apache / IHS / IIS startup scripts to include `Webgate_Oracle_Home/lib` or `Webgate_Oracle_Home/bin` location in `LD_LIBRARY_PATH` or `PATH`

- Adding Permissons for IIS WebGate

  After IIS WebGate 14c (14.1.2.0.0) is installed in the same location as the 12c (12.2.1.4.0) IIS WebGate, you will need to add new permissions.

  1. . Run the following commands:

     ```
     set WebGateHome=<14.1.2-Webgate-OH>

     cacls %WebGateHome% /E /T /G IUSR:f
     cacls %WebGateHome% /E /T /G IIS_IUSRS:f
     cacls %WebGateHome% /E /T /G NETWORK:f
     cacls %WebGateHome% /E /T /G "NETWORK SERVICE":f
     ```

  2. Copy the *webgate.ini* file from the 12.2.1.4.0 WebGate installation located in the following directory and copy it to the new 12c (12.2.1.4.0) installation under same location:

     ```
     OH\webgate\iis\lib
     ```