Oracle® Fusion Middleware

API Gateway Installation and Configuration Guide

11g Release 2 (11.1.2.1.0)

January 2013

Oracle API Gateway Installation and Configuration Guide, 11g Release 2 (11.1.2.1.0)

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

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services. This documentation is in prerelease status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Software License and Service Agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Contents

System Requirements

Overview

This topic provides the system requirements for the Oracle API Gateway, and specific requirements for other components. For more details on API Gateway components, see the *Oracle API Gateway User Guide*.

Operating System Requirements

This section describes the operating system requirements for the API Gateway:

Platform	***Supported Versions***	***Hardware Prerequisites***
Windows	• Windows Server 2008 SP1+ • Windows Server 2003 R2+ • Windows Server 2003 SP2 • Windows XP SP2+	• Intel Core or AMD Opteron at 2Ghz with Dual Core or faster • Minimum 1 GB free disk space, 50 GB recommended • Minimum 4 GB physical memory
Solaris	• Solaris 10 Update 4+	• Solaris compatible SPARC processor at 440 MHz, or faster • Minimum 1 GB free disk space, 50 GB recommended • Minimum 4 GB physical memory
Linux	• Oracle Linux 5 (UL3+) • Red Hat Enterprise Linux 5 (UL3+) • SUSE Linux Enterprise Server 11 (all SP levels) Oracle software may not run on systems that do not meet these requirements (see **Important** below).	• Intel Core or AMD Opteron at 2Ghz with Dual Core or faster (i386 or x86_64) • Minimum 1 GB free disk space, 50 GB recommended • Minimum 4 GB physical memory

Important

When new Linux kernels and distributions are released, Oracle modifies and tests its products for stability and reliability on these platforms. Oracle makes every effort to add support for new kernels and distributions in a timely manner. However, until a kernel or distribution is added to this list, its use with Oracle products is not supported. Oracle endeavors to support any generally popular Linux distribution on a release that the vendor still supports.

Specific Requirements

This section describes requirements for specific components:

Component	***Requirement***
Policy Studio	Runs on the same platforms as the API Gateway with the following additional requirements on Linux and Solaris: • X-Windows environment • GTK+ 2
API Gateway Manager	Supports the following browsers: • Internet Explorer 8 or higher • Firefox 13.0 or higher • Safari 5.1.7 or higher
Oracle API Gateway Analytics	Server component has the same platform requirements as the API Gateway. Supports the following databases: • MySQL Server 5.1 • Microsoft SQL Server 2000, 2005, 2008 • Oracle 10.2.0.4+, 11.1.0.7+, 11.2.0.1 • IBM DB2 9.1 Browser-based client component has same requirements as API Gateway Manager.

Default Ports

This section describes the default ports used by specific components.

API Gateway
The default ports used by the API Gateway are as follows:

- Traffic Port: `8080`
- Management Port: `8085`

Admin Node Manager
The default port used by the Admin Node Manager for monitoring and management is `8090`.

Oracle API Gateway Analytics
The default port used by API Gateway Analytics for reporting, monitoring, and management is `8040`.

Policy Studio
The default URL address used by Policy Studio to connect to the Admin Node Manager is as follows:

```
https://localhost:8090/api
```

Installing the API Gateway

Prerequisites

This topic describes how to install the API Gateway on the following platforms:

- Windows
- Linux
- Solaris

System Requirements
See the *System Requirements* to ensure that the target machine is of a suitable specification. For details on API Gateway components and concepts, see the *Oracle API Gateway User Guide*.

GUI Installation

When you run the installation executable in default GUI mode, you are presented with an introductory welcome screen. Click **Next** to continue with the installation.

Installation Directory

Enter or click **Browse** to specify the directory where you wish to install API Gateway components, for example:

Windows	`C:\OEG-11.1.2.1.0`
Linux/UNIX	`/opt/OEG-11.1.2.1.0`

Click **Next** to continue.

Select Components

Select the components that you wish to install, or deselect those that you do not wish to install:

- **Oracle API Gateway**:
  The main API Gateway component, which enables you to create API Gateway instances. The API Gateway is a comprehensive operating platform for managing, delivering, and securing APIs. It enables enterprises to create and apply policies to APIs to enforce security, compliance, and operational requirements.
- **Oracle API Gateway Analytics**:
  The web-based tool for monitoring and analyzing API use over a specified time. Reported metrics include what APIs are used, how often they are used, when they are used, and who is using them.
- **Oracle Policy Studio**:
  The policy development and configuration tool that enables you to develop and configure policies to enforce security, compliance, and operational requirements.

Click **Next** to continue.

Note

This topic describes how to install the main API Gateway component. For details on installing the other components, see

- *Installing Oracle API Gateway Analytics*
- *Installing the Policy Studio*

Domain Connection

Select whether this is the first system in a new API Gateway domain. Defaults to **Yes**, which configures the system with a new Admin Node Manager.

If you select **No**, the system is configured with a local Node Manager, which connects to an existing Admin Node Manager. You are asked to enter the connection details to an existing Admin Node Manager.

Click **Next** to continue.

Admin Node Manager Details

If you selected **Yes** in the **Domain Connection** screen, configure the following settings. Otherwise, skip to the section called “Local Node Manager Details”.

Use SSL/HTTPS Scheme for Connection:
Select whether to use SSL/HTTP to connect to the Node Manager. This setting is selected by default.

Hostname or IP Address:
Select a host address from the **Autodetected List** (defaults to the installation hostname), or choose **Select Manually**, and enter a host address.

Local Management Port:
Enter the local port used to manage the Node Manager. Defaults to `8090`.

Click **Next** to continue.

Local Node Manager Details

If you selected **No** in the **Domain Connection** screen, configure the following settings:

Use SSL/HTTPS Scheme for Connection:
Select whether to use SSL/HTTP to connect to the Node Manager. This setting is selected by default.

Hostname or IP Address:
Select a host address from the **Autodetected List** (for example, `127.0.0.1`), or choose **Select Manually**, and enter a host address.

Local Management Port:
Enter the local port used to manage the Node Manager. Defaults to `8090`.

Click **Next** to continue.

Admin Node Manager Connection Details

If you selected **No** in the **Domain Connection** screen, configure the following settings to connect to an existing Admin Node Manager. Otherwise, skip to the next section.

Connection URL:
Enter the URL to connect to the Admin Node Manager. Defaults to the following:

```
https://[admin-node-hostname-or-IP]:8090
```

Modify Default Values?:
Select whether to modify the default Admin Node Manager username/password (`admin/changeme`). When this is selected, enter a new username/password. This setting is unselected by default.

Click **Next** to continue.

Node Manager Service Details

Configure the following settings:

Add a Service for the Node Manager:
Select whether to add a service for the Node Manager. Defaults to **No**.

Run Service as non default user:
Select whether to run the Node Manager service as a non-default user. This setting is not selected by default. When you select this setting, you can enter a non-default user in the **Username** field. The default user is `admin`.

Click **Next** to continue.

API Gateway Configuration

Select whether to configure a new API Gateway instance. Defaults to **Yes**. When **Yes** is selected, you are asked to enter connection details for the new API Gateway instance in the next step.

Click **Next** to continue.

API Gateway Details

If you selected to configure a new API Gateway instance in the previous step, configure the following settings. Otherwise, skip to the section called “Ready to Install”.

API Gateway Name:
Enter a name for the API Gateway instance. Defaults to `Gateway1`.

API Gateway Group:
Enter a group name for the API Gateway instance. Defaults to `Group1`.

Use SSL/HTTPS Scheme for Connection:
Select whether to use SSL/HTTP to connect to the API Gateway instance. This setting is selected by default.

Local Management Port:
Enter the local port that the Node Manager uses to manage the API Gateway instance. Defaults to `8085`.

External Traffic Port:
Enter the port that the API Gateway uses for message traffic from external clients. Defaults to `8080`.

Click **Next** to continue.

API Gateway Service Details

If you selected to configure a new API Gateway instance, you can configure the following settings:

Add a Service (/etc/init.d script) for the API Gateway Instance:
Select whether to add a service for the API Gateway instance. Defaults to **No**.

Run Service as non default user:
Select whether to run the Node Manager service as a non-default user. This setting is not selected by default. When you select this setting, you can enter a non-default user in the **Username** field. The default user is `admin`.

Click **Next** to continue.

Oracle API Gateway Startup

Select whether to start the Admin Node Manager and the new API Gateway instance after installation. Defaults to **Yes** (recommended).

Note

If you select **No**, you must start the Admin Node Manager and the new API Gateway instance manually after installation.

Click **Next** to continue.

Ready to Install

The installer is ready to start installing the selected components and settings on your system.

Click **Next** to continue.

Installing

A progress screen is displayed showing the progress of the installation of files. Please wait for the installation to complete.

Click **Next** to continue.

Completing the Oracle API Gateway Setup

After the installer has finished, you can connect to the Admin Node Manager using the connection URL. You can also select whether to connect to the Policy Studio if this was installed.

Click **Finish** to complete the installation. You can access the API Gateway Manager tools in your browser. The default URL is displayed in the dialog (`https://`*`hostname`*`:8090/`).

Click **OK** to finish. Policy Studio also launches if this was selected.

Starting the API Gateway

If you did not select to start the API Gateway after installation, you can start the API Gateway as follows:

1. Open a command prompt in the following directory:

Windows	`INSTALL_DIR\apigateway\Win32\bin`
Linux/UNIX	`INSTALL_DIR/apigateway/posix/bin`

2. Run the `startinstance` command, for example:

```
startinstance -n "Server1" -g "Group1"
```

Note

On UNIX/Linux, you must ensure that the `startinstance` has execute permissions.

3. To manage and monitor the API Gateway, you must ensure that the Admin Node Manager is running. Use the `nodemanager` command to start the Admin Node Manager from the same directory.

Important

You can encrypt all sensitive API Gateway configuration data with an encryption passphrase. For example, you can specify this passphrase in your API Gateway configuration file, or on the command line when the API Gateway is starting up. For more details, see the *Oracle API Gateway User Guide*.

Starting the Policy Studio

If you did not select to launch the Policy Studio automatically after installation, see the section called “Starting the Policy Studio”.

Unattended Installation

You can run the API Gateway installer in unattended mode on the command line. The following command shows an example of installing the API Gateway component only:

Windows

```
OEG-11.1.2.1.0-windows-installer.exe --mode unattended
  --enable-components nodemanager --disable-components analytics,policystudio
```

Linux

```
./OEG-11.1.2.1.0-linux-installer.run --mode unattended
  --enable-components nodemanager --disable-components analytics,policystudio
```

The specified components are installed in the background.

Further Information
For a description of all available command options and default settings, enter the `--help` option. This outputs the help text in a separate console.

Creating a New Domain

If you wish to create a new managed domain and API Gateway instance, you can do this using the `managedomain` script. For more details, see *Configuring a Managed Domain*.

Configuring a Managed Domain

Overview

This topic describes how to use the managedomain script to configure a managed API Gateway domain. It shows how to register a host in a new domain, and create a new API Gateway instance. These are the minimum steps required to configure a domain.

You can also use the topology view in the web-based API Gateway Manager tool to manage a newly created domain. For example, you can perform tasks such as creating and deleting groups and API Gateway instances.

Important

To use the API Gateway, you must have a domain configured in your API Gateway installation. If you did not already configure a domain when installing the API Gateway, you must configure a domain using managedomain.

A single API Gateway installation supports a single API Gateway domain only. If you wish to run API Gateways in different domains on the same host, you need separate installations for each domain. For an introduction to the API Gateway domain and group runtime architecture, see the *Oracle API Gateway User Guide*.

Managedomain Script

When configuring a domain, the managedomain script enables you to perform tasks such as the following:

- Host management (registering and deleting hosts, or changing Admin Node Manager credentials)
- API Gateway management (creating and deleting API Gateway instances, or adding Windows and Linux/Solaris services)
- Group management (editing or deleting API Gateway groups)
- Topology management (viewing topologies)
- Deployment (deploying to a group, listing deployments, creating or downloading deployment archives, and editing group passphrases)

For example, you can use the managedomain script to register a host in a domain and create a new API Gateway instance. These are the minimum tasks required to create a new domain, which are documented in this topic.

Further Information
For details on selecting specific options, enter the managedomain command in the following directory, and follow the instructions at the command prompt:

Windows	`INSTALL_DIR\apigateway\Win32\bin`
UNIX/Linux	`INSTALL_DIR/apigateway/posix/bin`

Note

To register an API Gateway instance as a service on Windows or Linux/UNIX, you must run the managedomain command as Administrator on Windows or root on Linux/UNIX.

For more details on managedomain options, see *Managedomain Command Reference*.

Registering a Host in a Domain

To register a host in a managed domain, perform the following steps:

1. Change to the following directory in your API Gateway installation:

Windows	`INSTALL_DIR\apigateway\Win32\bin`
UNIX/Linux	`INSTALL_DIR/apigateway/posix/bin`

2. Enter the following command:

```
managedomain
```

3. Enter **1** to register your host, and follow the instructions when prompted. For example, if this is the first host in the domain, enter **y** to configure an Admin Node Manager on the host. Alternatively, to add the host to an existing domain, enter **n** to configure a local Node Manager that connects to the Admin Node Manager in the existing domain.
4. Enter **q** to quit when finished.
5. Enter the following command to start the Admin Node Manager or local Node Manager on the registered host:

```
nodemanager
```

Note

You must ensure the Admin Node Manager is running in the domain to enable monitoring and management of API Gateway instances.

When registering multiple hosts in a domain, the API Gateway must be installed on each host machine, and option 1 must be run on each machine.

Creating an API Gateway Instance

To create an API Gateway instance, perform the following steps:

1. Open a new command window.
2. Change to the following directory in your API Gateway installation:

Windows	`INSTALL_DIR\apigateway\Win32\bin`
UNIX/Linux	`INSTALL_DIR/apigateway/posix/bin`

3. Enter the following command:

```
managedomain
```

4. Enter **5** to create a new API Gateway instance, and follow the instructions when prompted. You can repeat to create multiple API Gateway instances on local or remote hosts.
5. Enter **q** to quit when finished.

6. Use the `startinstance` command to start the API Gateway, for example:

   ```
   startinstance -n "my_server" -g "my_group"
   ```

Note

You can add an API Gateway instance on any registered host in the domain, not just the local host. However, if you are creating Windows or UNIX services for the API Gateway, you must run `managedomain` on same host.

You must run `startinstance` on the host on which you intend to start the instance. On UNIX/Linux, you must ensure that the `startinstance` file has execute permissions. Running `startinstance` without any arguments lists all API Gateway instances available on the host.

Connecting to an API Gateway Instance

You can test the connection to the new API Gateway instance by connecting to the Health Check service. For example, enter the following default URL in your browser:

```
http://HOST:8080/healthcheck
```

This should display a simple `<status>ok</status>` message.

You can view the newly created API Gateway instance on the API Gateway Manager dashboard. For example, the default URL is as follows:

```
https://HOST:8090
```

The port numbers used to connect depend on those entered when configuring the domain using `managedomain`, and are available from the localhost only.

Alternatively, you can also connect to the new API Gateway instance in the Policy Studio. For more details, see *Installing the Policy Studio*.

Managing a Domain in API Gateway Manager

You can also use the topology view in the web-based API Gateway Manager tool to manage an existing domain. For example, you can perform tasks such as creating or deleting groups and API Gateway instances.

Note

When using API Gateway Manager to manage an existing domain, you must ensure that the host was first registered in the domain (for example, using `managedomain`). If you create an API Gateway instance, you must start it on the command line using `startinstance`.

Managing Groups
To use the API Gateway Manager to create an API Gateway group, perform the following steps:

1. Click the **Menu** button in the topology view on the **Dashboard** tab.
2. Select **Create New Group**.
3. Enter a group name (for example, `Engineering`).
4. Click **OK**.

To delete a group, perform the following steps:

1. Ensure that the API Gateway instances in the group have been stopped.
2. Hover over the group in the topology view, and click the edit button on the right.
3. Select **Delete Group**.
4. Click **OK**.

Managing API Gateway Instances

To use the API Gateway Manager to create an API Gateway instances, perform the following steps:

1. Hover over the API Gateway instance in the topology view, and click the edit button on the right.
2. Select **Create New Group**.
3. Configure the following fields:
   - **Name**: API Gateway instance name (for example, `Server2`).
   - **Management Port**: Local management port (for example, `8086`).
   - **Services Port**: External traffic port (for example, `8081`).
   - **Host**: Host address (for example, `127.0.0.1`).
4. Click **OK**.

To delete an API Gateway instance, perform the following steps:

1. Ensure that the API Gateway instance has been stopped.
2. Hover over the API Gateway instance in the topology view, and click the edit button on the right.
3. Select **Delete Server**.
4. Click **OK**.

Upgrading a Previous Installation

Overview

This topic describes how to upgrade your existing configuration data (policies, filters, certificate store, and so on) from a previous version to API Gateway version 11.1.2.1.0. This enables you to migrate the policies that you configured in a previous version to API Gateway version 11.1.2.1.0.

API Gateway 11.1.2.1.0 provides a script to upgrade existing configuration from previous versions, which is the recommended approach. This script generates a `.fed` file, which you can deploy using the Policy Studio, the `managedomain` script, or the Web-based API Gateway Manager tool.

Upgrade Steps
The main steps required for upgrading are as follows:

1. Install Oracle API Gateway 11.1.2.1.0 (see *Installing the API Gateway*).
2. Create a managed domain for your deployment topology (see *Configuring a Managed Domain*).
3. Upgrade your existing configuration using the API Gateway upgrade script.
4. Upgrade Role-Based Access Control (if upgrading from version 11.1.1.6.x).
5. Upgrade your reports database (if Oracle API Gateway Analytics is installed).

This topic assumes that you have already performed steps 1-2, and describes how to perform steps 3-5. For details on product components and concepts, see the *Oracle API Gateway User Guide*.

Prerequisites

You must have already installed API Gateway 11.1.2.1.0, and configured a managed domain.

Important

These steps describe only how to upgrade the configuration data from a previous version to 11.1.2.1.0. The supplied upgrade scripts do *not* upgrade the version of the Oracle server software installed on the machine.

You must ensure that API Gateway 11.1.2.1.0 is installed into a different directory from the existing (pre-11.1.2.1.0) version.

Upgrading to Version 11.1.2.1.0

Complete the following steps to upgrade a version 5.x or 6.x installation to API Gateway version 11.1.2.1.0 using the upgrade script:

1. Stop your pre-version 11.1.2.1.0 server.
2. Make a backup copy of the following existing directory that needs to be upgraded:

   ```
   INSTALL_DIR/apigateway/conf
   ```

3. Create a directory to store the output `.fed` file (for example, `C:\upgraded`).
4. Open a command prompt at the following directory in your 11.1.2.1.0 installation:

   Windows

   ```
   INSTALL_DIR\apigateway\Win32\bin
   ```

UNIX/Linux

```
INSTALL_DIR/apigateway/posix/bin
```

5. Run the `upgradeconfig` command. For example:

   Windows

   ```
   upgradeconfig -d C:\oraclegateway -o C:\upgraded
   ```

   UNIX/Linux

   ```
   ./upgradeconfig -d /opt/oraclegateway -o /opt/upgraded
   ```

   When the script has finished running, the `.fed` file is generated in the specified destination (for example, `C:\upgraded`).
6. Deploy the `.fed` file. For details, see the section called “Deploying the .fed File”.
7. Upgrade your RBAC configuration. For details, see the section called “Upgrading Role-Based Access Control”.
8. If you wish upgrade the database used for Oracle API Gateway Analytics, see the section called “Upgrading a Reports Database”.

For full details on all command options, enter `upgradeconfig --help` at the command prompt.

Deploying the .fed File

You can deploy the generated `.fed` file using the Policy Studio, the Web-based API Gateway Manager tools, or the `managedomain` script.

Deploying with the Policy Studio
To deploy an upgraded `.fed` file using the Policy Studio, perform the following steps:

1. Ensure that the Admin Node Manager and API Gateway instances that you wish to deploy to are running.
2. Start the Policy Studio, and click **Connect To Server**, or click an existing server session.
3. In the **Topology** view, click the **Deploy** button in the toolbar.
4. In the **Select the servers(s) you wish to deploy to** section, select a server group from the list, and select the server instance(s) in the box below.
5. In the **Select the configuration you wish to deploy** section, select **I wish to deploy an existing archive**.
6. In the **Location of archive** field, click **Browse**, and select the generated `.fed` file.
7. Click **Deploy** to upload the archive to the Admin Node Manager, and deploy it to the currently active selected server(s).
8. When the archive has deployed, click **Finish**.

Deploying with API Gateway Manager
API Gateway Manager is a centralized Web-based dashboard that enables administrators to control and manage API Gateway and groups in a domain. You can access the API Gateway Manager tools at `https://localhost:8090`. To deploy an upgraded `.fed` file using API Gateway Manager, perform the following steps:

1. On the **Dashboard** tab, in the **Topology** section, select the group to which you wish to deploy the configuration.
2. Click the icon to the right of the group name, and select **Deploy Configuration**.
3. Select **I wish to deploy an existing archive**, and browse to select the `.fed` that you generated.
4. Click **Next**.
5. Select the server instances in the group that you want to deploy to and click **Deploy**.
6. Click **Finish**, and test your configuration.

Deploying with the managedomain Script

You can also deploy a generated `.fed` file using the `managedomain` script in the following directory:

Windows

```
INSTALL_DIR\apigateway\Win32\bin\managedomain
```

UNIX/Linux

```
INSTALL_DIR/apigateway/posix/bin/managedomain
```

When you run `managedomain`, you can select a set of options. Option 18 is for deploying from a `.fed` file. Enter `18`, and follow the instructions in the output (user input in bold):

```
Select option: 18
Select a group:
  1) Group1
  2) Enter group name
Enter selection from 1-2 [2]: 1
Select one of the following options for deployment:
  1) Enter name of directory containing federated store config files
  2) Enter name of deployment archive file
  3) Enter tagname
Enter selection [1]: 1
Enter name of directory containing configuration files
[/Oracle-11.1.2.1.0/apigateway/skel/system/conf/templates]: /path/to/fed/file/
Enter name: Upgraded Config
Enter description: the upgraded configuration
Enter version: v1.5
Enter version comment: Upgraded of v1
Do you wish to deploy to all API Gateways in the group ? [y]: y
Loading configuration '7b2f0a3b-89cd-4bdb-8b66-732992400d47' to hosts running group...
Loaded configuration '7b2f0a3b-89cd-4bdb-8b66-732992400d47' to hosts running group.
Deploying to API Gateway 'APIServer1'...
Deployed to API Gateway 'APIServer1' successfully.
Deploying to API Gateway 'APIServer2'...
Deployed to API Gateway 'APIServer2' successfully.
Hit enter to continue...
```

Upgrading Role-Based Access Control

In API Gateway version 11.1.2.0.0, the Role-Based Access Control (RBAC) support changed to use a JSON-based implementation with new API Gateway user roles. If you are upgrading from version 11.1.1.6.x, you must reconfigure your RBAC settings.

The API Gateway provides the following sample script to migrate your existing users:

```
INSTALL_DIR/samples/migrate/pdMigrate.py
```

This script extracts the existing users from the following file:

```
INSTALL_DIR/apigateway/conf/pdEntities.xml
```

and places them into the following file:

```
INSTALL_DIR/apigateway/conf/adminUsers.json
```

For example, you can run this script as follows:

Windows

```
INSTALL_DIR\Win32\bin\jython ..\..\samples\scripts\migrate\pdMigrate.py
C:\from\oraclegateway; C:\to\apigateway
```

Linux/UNIX

```
INSTALL_DIR/posix/bin/jython ../../samples/scripts/migrate/pdMigrate.py
from/oraclegateway; to/apigateway
```

For more details on RBAC, see the chapter on "Configuring Role-Based Access Control" in the *Oracle API Gateway User Guide*.

Upgrading a Reports Database

If you have an existing installation of Oracle API Gateway Analytics version 11.1.1.6.x, and wish to upgrade your existing reports database to version 11.1.2.0.x, you can upgrade your database tables using the `dbsetup` script. For more details, see *Configuring the Database for Oracle API Gateway Analytics*.

Important

Only upgrades of version 11.1.1.6.x databases are supported. Upgrades of earlier versions are not supported. Upgrades of version 11.1.2.0.x are not required.

Further Information

If you encounter any problems with upgrading from a previous version, contact the Oracle Support team with your queries (see *Oracle Contact Details*).

Installing the Policy Studio

Prerequisites

This topic describes how to install the Policy Studio on the following platforms:

- Windows
- Linux
- Solaris

System Requirements
See the *System Requirements* to ensure that the target machine is of a suitable specification. For details on API Gateway components and concepts, see the *Oracle API Gateway User Guide*.

Note

This topic describes how to install the Policy Studio. For details on installing other components, see

- *Installing the API Gateway*
- *Installing Oracle API Gateway Analytics*

GUI Installation

When you run the installation executable in default GUI mode, you are presented with an introductory welcome screen. Click **Next** to continue with the installation.

Installation Location

Enter or click **Browse** to specify the directory where you wish to install API Gateway components, for example:

Windows	`C:\OEG-11.1.2.1.0`
Linux/UNIX	`/opt/OEG-11.1.2.1.0`

Click **Next** to continue.

Select Components

Select the Policy Studio component from the list, and click **Next** to continue.

Ready to Install

The installer is ready to start installing the selected components and settings on your system.

Click **Next** to continue.

Installing

A progress screen is displayed showing the progress of the installation. Wait for the installation to complete.

Click **Next** to continue.

Completing the Oracle Policy Studio Setup

After the installer has finished, you can select whether launch Policy Studio. This setting is selected by default.

Click **Finish** to complete the installation.

Ensure the API Gateway is Running

Before starting the Policy Studio, you should ensure that the Admin Node Manager and the API Gateway instance that you wish to manager are running. For more details, see the topic on *Installing the API Gateway*.

Starting the Policy Studio

If you did not select to launch the Policy Studio after installation, perform the following steps:

1. Open a command prompt.
2. Change to your Policy Studio installation directory (for example, `INSTALL_DIR\policystudio`).
3. Start `policystudio`.

Making a Server Connection
When the Policy Studio starts up, click a link to a server session to display the **Open Connection** dialog. You can use this dialog to specify **Connection Details** (for example, host, port, user name, and password), or to specify **Saved Sessions**.

If you wish to connect to the server using a non-default URL, click **Advanced**, and enter the **URL**. The default URL for the Admin Node Manager is:

```
https://localhost:8090/api
```

For more details on the settings in the **Open Connection** dialog, see the *Oracle API Gateway User Guide*.

Unattended Installation

You can run the API Gateway installer in unattended mode on the command line. The following command shows an example of installing the Policy Studio component only:

Windows

```
OEG-11.1.2.1.0-windows-installer.exe --mode unattended
  --enable-components policystudio --disable-components analytics,nodemanager
```

Linux

```
./OEG-11.1.2.1.0-linux-installer.run --mode unattended
  --enable-components policystudio --disable-components analytics,nodemanager
```

The specified components are installed in the background.

Further Information
For a description of all available command options and default settings, enter the `--help` option. This outputs the help text in a separate console.

Installing Oracle API Gateway Analytics

Prerequisites

This topic describes how to install Oracle API Gateway Analytics on the following platforms:

- Windows
- Linux
- Solaris

System Requirements
See the *System Requirements* to ensure that the target machine is of a suitable specification. For details on API Gateway components and concepts, see the *Oracle API Gateway User Guide*.

PDF Report Generation
If you wish to enable the automatic generation of PDF reports, you must download the wkhtmltopdf tool, and install it into your API Gateway Analytics installation when installed. For more details, see the section called “Next Steps”.

Note

This topic describes how to install the Oracle API Gateway Analytics component. For details on installing other components, see

- *Installing the API Gateway*
- *Installing the Policy Studio*

GUI Installation

When you run the installation executable in default GUI mode, you are presented with an introductory welcome screen. Click **Next** to continue with the installation.

Installation Location

Enter or click **Browse** to specify the directory where you wish to install API Gateway components, for example:

Windows	`C:\OEG-11.1.2.1.0`
Linux/UNIX	`/opt/OEG-11.1.2.1.0`

Click **Next** to continue.

Select Components

Select the Oracle API Gateway Analytics component from the list, and click **Next** to continue.

Oracle API Gateway Analytics Information

Important

Before starting API Gateway Analytics, you must perform the following steps:

1. Create a new database instance. For more details, see *Configuring the Database for Oracle API Gateway Analytics*. Alternatively, if you already have an existing database, skip to the next step.
2. Setup your database tables using the `dbsetup` script. For more details, see *Configuring the Database for Oracle API Gateway Analytics*.
3. Configure your API Gateway Analytics settings using the `configureserver` script. For more details, see *Configuring Oracle API Gateway Analytics*.

Oracle API Gateway Analytics is about to be installed.

Ready to Install

The installer is ready to start installing the selected components and settings on your system.

Click **Next** to continue.

Installing

A screen is displayed showing the progress of the installation of files. Please wait for the installation to complete.

Click **Next** to continue.

Completing the Oracle API Gateway Analytics Setup

After the installer has finished, click **Finish** to complete the installation.

Next Steps

When you have installed API Gateway Analytics, the next step is *Configuring the Database for Oracle API Gateway Analytics*.

PDF Report Generation
If you wish to enable the automatic generation of PDF reports, perform the following steps:

1. Download the wkhtmltopdf tool from the following location:
   http://code.google.com/p/wkhtmltopdf
2. Install wkhtmltopdf into the following directory in your API Gateway Analytics installation:

Windows	`INSTALL_DIR\analytics\Win32\lib\wkhtmltopdf`
UNIX/Linux	`INSTALL_DIR/analytics/posix/lib/wkhtmltopdf`

Unattended Installation

You can run the API Gateway installer in unattended mode on the command line. The following command shows an example of installing the API Gateway Analytics component only:

Windows

```
OEG-11.1.2.1.0-windows-installer.exe --mode unattended
  --enable-components analytics --disable-components nodemanager,policystudio
```

Linux

```
./OEG-11.1.2.1.0-linux-installer.run --mode unattended
  --enable-components analytics --disable-components nodemanager,policystudio
```

The specified components are installed in the background.

Further Information
For a description of all available command options and default settings, enter the `--help` option. This outputs the help text in a separate console.

Configuring the Database for Oracle API Gateway Analytics

Overview

The API Gateway stores and maintains the monitoring and transaction data read by Oracle API Gateway Analytics in a JDBC-compliant database. This topic describes how to create and configure the reports database for use with Oracle API Gateway Analytics. It describes the prerequisites and shows an example of creating a reports database. It also shows how to setup the database tables or upgrade them from a previous version.

Prerequisites

The prerequisites for setting up the database are as follows:

JDBC Database Installation
You must have a JDBC-compliant database installed to store the API Gateway monitoring and transaction data. API Gateway Analytics provides setup scripts for the following databases:

- MySQL
- Microsoft SQL Server
- Oracle
- IBM DB2

For details on how to install your chosen JDBC database, see your database product documentation.

API Gateway Analytics Installation
For details on how to install Oracle API Gateway Analytics, see the topic on *Installing Oracle API Gateway Analytics*.

Creating the Reports Database

API Gateway Analytics reads message metrics from a database and displays this information in a visual format to administrators. This is the same database in which the API Gateway stores its audit trail and message metrics data. You first need to create this database using the database product of your choice (MySQL, Microsoft SQL Server, Oracle, or IBM DB2). For details on how to do this, see the product documentation for your chosen database. In this topic, the example database is named `reports`, but you can use whatever name you wish.

The following example shows creating a MySQL database:

```
mysql> CREATE DATABASE reports;
Query OK, 1 row affected (0.00 sec)
```

Setting up the Database Tables

When you have created the reports database, the next step is to set up the database tables. You can do this by running the `dbsetup` command from the following API Gateway Analytics directory:

Windows	`INSTALL_DIR\analytics\Win32\bin`
Linux/UNIX	`INSTALL_DIR/analytics/posix/bin`

The following example command shows setting up new database tables:

```
> dbsetup.bat
New database
Schema successfully upgraded to: 001-topology
```

Upgrading Existing Database Tables

The `dbsetup` utility also enables you to upgrade an existing reports database from an initial API Gateway version 11.1.1.6.x schema to version 11.1.2.x schema.

Important

You must upgrade version 11.1.1.6.x database schemas to 11.1.2.x for the API Gateway to function correctly. Pre-11.1.1.6.x database schema upgrades are not supported. If your existing API Gateway installation is version 11.1.2.x, you do not need to upgrade the database tables.

The `dbsetup` utility always checks the existing version, and modifies only if an update is required. For example, to start an interactive upgrade, run this script as follows:

```
> dbsetup.bat
Connecting to configuration at: federated:file:///INSTALL_DIR\analytics/conf/fed/
configs.xml

Using Configured Database:
DB Name: Default Database Connection
DB URL: jdbc:mysql://127.0.0.1:3306/reports
DB User: root
Current schema version: 000-initial
Latest schema version: 001-topology
Continue with upgrade (Y, N) [N]: y
Schema successfully upgraded to: 001-topology
```

`dbsetup` uses SQL upgrade scripts for all supported databases located in the following directory:

```
INSTALL_DIR/system/conf/sql/upgrade
```

The subdirectories are named for the upgrade applied, and the order in which they must be executed. The following upgrades are currently available:

Upgrade Name	Description
`000-initial`	11.1.1.6.x version of the schema.
`001-topology`	11.1.2.x version of the schema.

Specifying Options to dbsetup

Note

When you specify command-line arguments to `dbsetup`, the script does not run interactively, and the setup is fully automatic.

You can specify the following options to the `dbsetup` command:

Option	Description
`-h, --help`	Displays help message and exits.
`-p PASSPHRASE, --passphrase=PASSPHRASE`	Specifies the configuration passphrase (blank for zero length).
`--dbname=DBNAME`	Specifies the database name (mutually exclusive with `--dburl`, `--dbuser`, and `--dbpass`).
`--dburl=DBURL`	Specifies the database URL.
`--dbuser=DBUSER`	Specifies the database user.
`--dbpass=DBPASS`	Specifies the database passphrase.
`--reinstall`	Forces a reinstall of the database, dropping all data.
`--stop=STOP`	Stops the database upgrade after the named upgrade.

The following are some examples of using `dbsetup` command options:

Connecting to a Named Database

You can use the `--dbname` option to connect to a named database connection configured under the **External Connections** node in the Policy Studio tree. For example:

```
> dbsetup.bat --dbname=Oracle
Current schema version: 001-initial
Latest schema version: 001-topology
Schema successfully upgraded to: 001-topology
```

Connecting to a Database URL

You can use the `--dburl` option to manually connect to a database instance directly using a URL. For example:

```
> dbsetup.bat --dburl=jdbc:mysql://localhost/reports --dbuser=root --dbpass=admin
Current schema version: 001-initial
Latest schema version: 001-topology
Schema successfully upgraded to: 001-topology
```

Installing a Database

You can also use the `--dburl` option to setup a newly created database instance where none already exists. For example:

```
> dbsetup.bat --dburl=jdbc:mysql://localhost/reports --dbuser=root --dbpass=admin
New database
Schema successfully upgraded to: 001-topology
```

Reinstalling a Database

You can use the `--reinstall` option to wipe and reinstall a database. For example:

```
> dbsetup.bat --dburl=jdbc:mysql://localhost/reports --dbuser=root --dbpass=admin
--reinstall
Re-installing database...
Schema successfully upgraded to: 001-topology
```

SQL Database Schema Scripts

As an alternative to using the dbsetup command, API Gateway Analytics also provides separate SQL schema scripts to set up the database tables for each of the supported databases. However, these scripts set up the new tables only, and do not perform any upgrades of existing tables. These scripts are provided in the INSTALL_DIR/system/conf/sql folder in the following directories:

- /mysql
- /mssql
- /oracle
- /db2

You can run the SQL commands in the db_schema.sql file in the appropriate directory for your database. The following example shows creating the tables in a MySQL database:

```
mysql> \. C:\oracle\analytics\system\conf\sql\mysql\db_schema.sql
Query OK, 0 rows affected, 1 warning (0.00 sec)
Query OK, 0 rows affected, 1 warning (0.00 sec)
...
```

Next Steps

When you have set up your database, you must ensure that the API Gateway is configured correctly for API Gateway Analytics before launching API Gateway Analytics. For more details, see *Configuring Oracle API Gateway Analytics*.

Configuring Oracle API Gateway Analytics

Overview

This topic describes the steps involved in setting up Oracle API Gateway Analytics. For example, this includes configuring the API Gateway Analytics port, database connection, and user credentials. The recommended way to configure Oracle API Gateway Analytics is to use the `configureserver` script to guide you through all the required steps. You can also use the Policy Studio to configure the Oracle API Gateway Analytics configuration file.

Prerequisites

The prerequisites for configuring Oracle API Gateway Analytics are as follows:

API Gateway Analytics Installation
For details on how to install Oracle API Gateway Analytics, see *Installing Oracle API Gateway Analytics*.

API Gateway Installation
Because API Gateway Analytics reports on transactions processed by the API Gateway in real time, you must ensure that the API Gateway is also installed. For more details, see *Installing the API Gateway*.

Important

To view API Gateway metrics in Oracle API Gateway Analytics, you must also configure the API Gateway to record metrics in the database for Oracle API Gateway Analytics to read. For more details, see the *Oracle API Gateway User Guide*.

JDBC Database Installation
The API Gateway stores and maintains the monitoring and transaction data read by API Gateway Analytics in a JDBC-compliant database. For more details, see *Configuring the Database for Oracle API Gateway Analytics*.

Configuring API Gateway Analytics

By default, API Gateway Analytics is configured to read message metrics from a MySQL database stored on the local machine. Typically, you may wish to use an alternative database, change the user credentials on the default database connection, or use a different listening port. This section explains how to configure API Gateway Analytics using the `configureserver` command.

Configuring API Gateway Analytics on the Command Line
Perform the following steps to run `configureserver` in interactive mode:

1. Change to the following directory:

Windows	`INSTALL_DIR\analytics\Win32\bin`
Linux/UNIX	`INSTALL_DIR/analytics/posix/bin`

2. Run the `configureserver` command.
3. Enter the port on which the API Gateway Analytics server will listen. Defaults to `8040`. If you have another process already using this port on the machine on which API Gateway Analytics is installed, configure API Gateway Analytics to listen on different port.
4. Enter the database connection URL. Defaults to `dbc:mysql://127.0.0.1:3306/reports`.

   The following table lists examples of connection URLs for the supported databases, where `reports` is the name of the database and `DB_HOST` is the IP address or host name of the machine on which the database is running:

Database	***Example Connection URL***
Oracle	`jdbc:oracle:thin:@DB_HOST:1521:reports`
Microsoft SQL Server	`jdbc:sqlserver://DB_HOST:1433;DatabaseName=reports;integratedSecurity=false;`
MySQL	`jdbc:mysql://DB_HOST:3306/reports`
IBM DB2	`jdbc:db2://DB_HOST:50000/reports`

5. Enter the database user name. Defaults to `root`.
6. Enter the database password.
7. Enter whether API Gateway Analytics generates PDF-based reports. Defaults to `N`, which means that PDF reports are not generated. When set to `Y`, API Gateway Analytics generates PDF reports that include the same metrics displayed in the API Gateway Analytics screen (for example, number of client requests, requests per service, and so on). For more details on generated PDF reports, see the *Oracle API Gateway User Guide*.
8. Enter the user name to connect to the API Gateway Analytics process that generates PDF reports. Defaults to an `admin` user.

Note

This is not the operating system user. This is the user that connects to the API Gateway Analytics web server process, which generates the PDF reports. You can add new users on the **Users and Groups** tab in the Policy Studio.

9. Enter the password to connect to the API Gateway Analytics process that generates PDF reports.
10. Enter the directory to which generated PDF reports are output (for example, `c:\reports`).
11. Enter whether to send generated PDF reports to email recipients. You will require an SMTP account with which to send the reports. Defaults to `N`.

The following command shows some example output in interactive mode:

```
C:\Oracle\analytics\Win32\bin>configureserver.bat
Connecting to configuration at : federated:file:///C:\Oracle\analytics/conf/fed/
configs.xml

Listening port [8040]:
Configuring Database: Default Database Connection
Database URL [jdbc:mysql://127.0.0.1:3306/reports]:
Database user name [root]:
Database password []: *****
Enable report generation (Y, N) [N]: y
Report generation process connects as user name [admin]:
Report generation process connects using password []: ********
Report output directory []: c:\reports
Email reports (Y, N) [N]: y
Default email recipient []: joe@example.com
Email from []: apigateway@vordel.com
Choose SMTP connection type:
   0) None
   1) SSL
   2) TLS/SSL
Choice [0]:
SMTP host []: localhost
SMTP port [25]:
SMTP user name []: jbloggs
SMTP password []: *********
Delete report file after emailing (Y, N) [Y]:
Press enter to exit...
```

Configuring API Gateway Analytics using Command-Line Options
You can also run the `configureserver` command with various options (`--port`, `--dburl`, `--emailfrom`, `--emailto`, `--smtphost`, and so on). For example, the following command configures the database connection without emailing reports:

```
configureserver --dburl=jdbc:mysql://127.0.0.1:3306/631v2 --dbuser=root
--dbpass=changeme --no-email
```

The following command specifies to email reports and the associated SMTP settings:

```
configureserver --dburl=jdbc:mysql://127.0.0.1:3306/reports --dbuser=root
--dbpass=changeme –-email --emailto=joe@example.com --emailfrom=apigateway@vordel.com
--smtptype=NONE --smtphost=192.168.0.174 --smtpport=25 --smtpuser=jbloggs
--smtppass=changeme --generate --gpass=changeme --gtemp=c:\reports
```

For descriptions of all available options, enter the `configureserver --help` command.

Configuring API Gateway Analytics in the Policy Studio
The recommended way to configure API Gateway Analytics is using the `configureserver` command, which guides you through the required settings. However, you can also use the Policy Studio to configure specific settings in your API Gateway Analytics configuration file. For example, to configure the `reports` database, perform the following steps:

1. In your Policy Studio installation directory, run the `policystudio` command.
2. On the Policy Studio **Home** tab, click **Open File**, and browse to your API Gateway Analytics configuration file, for example:

   ```
   INSTALL_DIR/analytics/conf/fed/configs.xml
   ```

3. Click the **External Connections** button on the left of the Policy Studio, and expand the **Default Database** tree node.
4. Right-click the **Default Database Connection** tree node, and select **Edit**.
5. The **Database Connection** dialog enables you to configure the database connection details. By default, the connection is configured to read metrics data from the `reports` database. Edit the details for the **Default Database Connection** on this dialog. For example, you should enter a non-default database user name and password. If you wish to connect to a database other than the default local database, right-click **Database Connections** in the tree, and select **Add a Database Connection**. For more details, see the *Oracle API Gateway User Guide*.

Note

You can verify that your database connection is configured correctly by clicking the **Test Connection** button on the **Configure Database Connection** dialog.

Launching API Gateway Analytics

To launch API Gateway Analytics, perform the following steps:

1. Start the API Gateway Analytics server using the `analytics` script in the `/bin` directory of your API Gateway Analytics installation.

2. Using the default port, connect to the API Gateway Analytics interface in a browser at the following URL:

   ```
   http://HOST:8040/
   ```

   where `HOST` points to the IP address or hostname of the machine on which API Gateway Analytics is installed.
3. Log in using the default `admin` user with password `changeme`. You can edit this user in Policy Studio using the **Users** interface from the Policy Studio tree view.

Note

API Gateway Analytics produces reports based on metrics stored by the API Gateway when processing messages. To produce a graph showing the number of connections made by the API Gateway to a service, you must first configure a policy that routes messages to that service. When this policy is configured, send messages through the policy so they are routed to the target service.

If you change to another database that has a different set of remote hosts/clients configured, you must restart the API Gateway and API Gateway Analytics.

Further Information

For more details on topics such as using the Policy Studio to configure policies, scheduled reports, viewing monitoring data in API Gateway Analytics, or purging the reports database, see the *Oracle API Gateway User Guide*.

Managedomain Command Reference

Overview

The managedomain script enables you to perform tasks such as the following:

- Host management (registering and deleting hosts, or changing Admin Node Manager credentials)
- API Gateway management (creating and deleting API Gateway instances, or adding Windows and Linux/Solaris services)
- Group management (editing or deleting API Gateway groups)
- Topology management (viewing topologies)
- Deployment (deploying to a group, listing deployments, creating or downloading deployment archives, and editing group passphrases)

To run this command, enter `managedomain` in the following directory, and follow the instructions at the command prompt:

Windows	`INSTALL_DIR\apigateway\Win32\bin`
UNIX/Linux	`INSTALL_DIR/apigateway/posix/bin`

Host Management

The `managedomain` command options for host management are as follows:

Option	Description	Why Use this Option
1	`Register host`	Add a new host that runs an API Gateway to a domain topology. You must ensure that the host is registered in order to create and run API servers. For example, you can specify the following: • If host is an Admin Node Manager • Use SSL • Hostname • Node Manager name • Node Manager port • Node Manager passphrase • Windows/UNIX service for Node Manager • Trust store details If the host you are registering is not the Admin Node Manager, you must specify the Admin Node Manager host details. The Admin Node Manager must also be running.
2	`Edit a host`	Edit the details for a host registered in a domain topology. Used occasionally.

Option	Description	Why Use this Option
		You can update the following: • Hostname • Node Manager name • Node Manager port • Node Manager passphrase • Windows/UNIX service for Node Manager • Use SSL When you get a license for an evaluation mode API Gateway, you must use this option to change the host from `127.0.0.1` to a network reachable address or hostname. You must also restart the Node Manager to pick up any changes.
3	`Delete a host`	Delete a registered host from a domain topology. Used occasionally. You must first stop and delete all API Gateways running on the host. This option is only for use on a remote non-Admin Node Manager node that is being removed from the topology. You must also stop the remote Node Manager process. This option will not work on the Admin Node Manager host, or if run locally on the host to be removed.
4	`Change credentials for Admin Node Manager, currently connecting as: user admin with truststore None`	By default, you connect to the Node Manager using `managedomain` with the credentials `admin/changeme`. You can override these at startup by passing the `--username --password` command line parameters, or reset while running `managedomain` with this option. This username/password refers to an `admin` user configured in the Policy Studio.

API Gateway Management

The `managedomain` command options for API Gateway management are as follows:

Option	Description	Why Use this Option
5	`Create API Gateway instance`	Create a new API Gateway instance. You can also do this in Policy Studio and API Gateway Manager. You can create API Gateway instances locally or on any host configured in the topology.

Option	Description	Why Use this Option
6	`Edit an API Gateway (rename, change management port)`	Rename the API Gateway instance, enable/disable SSL, or change the management port. This functionality is not available in Policy Studio and API Gateway Manager.
7	`Delete API Gateway instance`	Delete an API Gateway instance from the topology, and optionally delete the files on disk. You can also do this in Policy Studio and API Gateway Manager. You must ensure that the API Gateway instance has stopped.
8	`Add a tag to an API Gateway`	Add a name-value tag to the API Gateway. The `Topology` view on the API Gateway Manager `Dashboard` displays tags and enables you to filter for API Gateway instances by tag.
9	`Delete a tag from an API Gateway`	Delete a name-value tag from the API Gateway. The tag will no longer be displayed in the API Gateway Manager `Dashboard`.
10	`Add a Windows/UNIX service for existing local API Gateway Group Management`	Must be run by a user with permission to create a service on the host operating system (`root` on Linux, or `Administrator` on Windows). When run on Linux, adds an `init.d` script.

Group Management

The `managedomain` command options for group management are as follows:

Option	Description	Why Use this Option
11	`Edit group (rename it)`	Rename an API Gateway group. This functionality is not available in the Policy Studio and API Gateway Manager.
12	`Delete a group`	Delete all API Gateways in the group and the group itself. You must ensure that all API Gateways in the group have been stopped first.

Topology Management

The `managedomain` command options for topology management are as follows:

Option	Description	Why Use this Option
13	`Print topology`	Output the contents of the deployed

Option	Description	Why Use this Option
		domain topology. This includes the following: • Topology version • Hosts • Admin Node Manager • Groups • API Gateway instances (tags)
14	`Check topologies are in sync`	For advanced users. Check that all Node Managers are running the same topology version. Useful only in multi-host environment. Topologies should be in sync if everything is running correctly.
15	`Check the Admin Node Manager topology against another topology`	For advanced users. Compare the two topologies and highlights differences. There should be no differences if everything is running correctly.
16	`Sync all topologies`	For advanced users. Forces a sync of all topologies.
17	`Reset the local topology`	For advanced users. Delete the contents of the `apigateway/groups` directory. This means that you would need to re-register the host and recreate a local API Gateway instance. Alternatively, you can manually delete the contents of this directory to prevent issues if the host has been registered with other node managers.

Deployment

The `managedomain` command options for deployment are as follows:

Option	Description	Why Use this Option
18	`Deploy to a group`	Deploy a configuration (`.fed` file) to API Gateways. This functionality is also available in Policy Studio and API Gateway Manager.
19	`List deployment information`	List the deployment information for all API Gateways in a topology. This functionality is also available in Policy Studio and API Gateway Manager.
20	`Create deployment archive`	Create a deployment archive from a directory that contains a federated API Gateway configuration.
21	`Download deployment archive`	Download the `.fed` file deployed to an

Option	Description	Why Use this Option
		API Gateway. This functionality is also available in Policy Studio.
`22`	`Update deployment archive properties`	Update the manifest properties relating to the deployed configuration only. This functionality is also available in Policy Studio. Enables you to update the properties without performing a new deployment.
`23`	`Change group configuration passphrase`	The default passphrase for the API Gateway configuration is `“”`. Use this option to set a more secure password. This functionality is also available in Policy Studio.

License Acknowledgments

Overview

Oracle API Gateway uses several third-party toolkits to perform specific types of processing. In accordance with the Licensing Agreements for these toolkits, the relevant acknowledgments are listed below.

Acknowledgments

Apache Software Foundation:
This product includes software developed by the Apache Software Foundation [http://www.apache.org/].

OpenSSL Project:
This product includes software developed by the OpenSSL Project [http://www.openssl.org/] for use in the OpenSSL Toolkit.

Eric Young:
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

James Cooper:
This product includes software developed by James Cooper.

Oracle Contact Details

Contact Details

For online technical assistance, and a complete list of locations, primary service hours, and telephone numbers, contact Oracle Technical Support at the following address:
https://support.oracle.com