Oracle® Fusion Middleware

Oracle API Gateway Installation Guide

11g Release 2 (11.1.2.4.0)

July 2015

ORACLE

Oracle API Gateway Installation Guide, 11g Release 2 (11.1.2.4.0)

27 July 2015

Contents

Preface

This document describes how to install API Gateway. It also describes how to upgrade from API Gateway version 11.1.2.x or 11.1.1.x to version 11.1.2.4.0.

Who should read this document

The intended audience for this document is system engineers who are responsible for installing, configuring, and maintaining API Gateway.

Before installing API Gateway you should have an understanding of API Gateway concepts and features. For more information, see the *API Gateway Concepts Guide*.

Others who might find parts of this document useful include network or systems administrators and other technical or business users.

How to use this document

This document should be used in conjunction with the other documents in the API Gateway documentation set.

Before you begin installing API Gateway, review this document thoroughly. The following is a brief description of the contents of each chapter:

Plan the deployment on page 10 - Describes what you should consider when planning for deploying and configuring your system architecture.

Prerequisites on page 12 – Describes the prerequisites for installing, including the system requirements.

Install on page 16 – Describes how to perform an installation using the GUI mode or unattended command-line mode.

Install API Gateway components on page 24 – Describes how to install the API Gateway components.

Post-installation on page 41 – Provides instructions on how to check if the installation was successful and describes additional tasks, such as securing API Gateway, that you should perform after installation.

Update API Gateway on page 45 – Describes how to apply service packs or patches to update your API Gateway installation.

Upgrade and migration on page 46 – Describes how to upgrade the software from API Gateway version 11.1.2.x or 11.1.1.x to version 11.1.2.4.0, and migrate your configuration data.

API Gateway documentation set

The API Gateway documentation set includes the following documents:

- *API Gateway Installation Guide*

  Describes how to install API Gateway components on all platforms, how to configure a domain and API Gateway instances, and how to upgrade API Gateway versions.

- *API Gateway Concepts Guide*

  Provides an overview of the API Gateway components, tools, and architecture.

- *API Gateway Policy Developer Guide*

  Describes the main API Gateway features (for example, all policies, filters, configuration options and so on), and how to configure them using the Policy Studio graphical tool.

- *API Gateway Administrator Guide*

  Describes how to administer an API Gateway deployment.

- *API Gateway OAuth User Guide*

  Describes how to configure API Gateway for OAuth 2.0 and OpenID Connect.

- *API Gateway Deployment and Promotion Guide*

  Describes how to promote and deploy API Gateway configuration between different environments (for example, development, testing, and production).

- *API Gateway Explorer User Guide*

  Describes how to use the API Gateway Explorer graphical tool to test REST-based APIs and SOAP-based web services.

- *API Gateway Developer Guide*

  Describes how to extend, leverage, and customize API Gateway.

- *API Gateway Key Property Store User Guide*

  Describes the API Gateway Key Property Store (KPS).

- *API Gateway Security Guide*

  Describes how to strengthen the security of API Gateway.

What's new

This release of the API Gateway Installation Guide contains the following changes:

- The API Gateway installer now prompts you to set an administrator user name and password. For more details, see *Set the administrator user name and password* on page 18.
- The API Gateway installer now prompts you to set an API administrator user name and password for API Manager. For more details, see *Installation options* on page 17.
- The default user names and passwords have been removed from all documentation for security reasons. If you choose not to set your own user names and passwords during installation, you can obtain the default user names and passwords from your Oracle Account Manager.
- The upgrade process has been greatly simplified. For more details, see *Upgrade and migration* on page 46.
- The guide has been reorganized and a number of new sections have been added:
  - *Plan the deployment* on page 10
  - *Post-installation* on page 41
  - *Update API Gateway* on page 45

Plan the deployment 1

This topic discusses how to plan your deployment. For more information on planning an API Gateway system, and how API Gateway interacts with existing infrastructure, see the *API Gateway Administrator Guide*.

Platforms

For more information on the exact platforms that Oracle supports for API Gateway, see *System requirements* on page 12.

API Gateway components

Before installing API Gateway you need to consider which components you require. Some components, for example, API Gateway Analytics, have additional requirements, such as a database. For more information, see *Specific component requirements* on page 14.

For more information on API Gateway components, see the *API Gateway Concepts Guide*.

Client considerations

API Gateway includes the Policy Studio developer tool, a thick client that is supported on Windows and UNIX/Linux. It also includes several web-based tools, for example, API Gateway Manager. For more information on supported thick client platforms and supported web browsers, see *System requirements* on page 12.

Cluster considerations

A cluster is a group of computers linked together in a network that share disk resources in a high availability (HA) environment. The machines in a cluster cooperate to provide a set of services or resources to clients.

In a cluster configuration, if the platform supporting a set of applications fails, the functions of the applications are transferred to a backup platform. This backup (or standby) platform is ready to immediately provide support for the critical application processes normally assured by the principal platform.

In most cluster solutions, when the original platform recovers from failure, it recovers application processes from the secondary system that has temporarily acted as the active system.

For a resilient high availability API Gateway configuration, a minimum of at least two active API Gateway instances at any time, with a third and fourth in passive mode, is recommended. For more information on configuring API Gateway high availability, see the *API Gateway Administrator Guide*.

Connection to other products

API Gateway supports integration with a wide range of Oracle (for example, Oracle Access Manager) and third-party (for example, LDAP or JMS providers) products. The requirements for a deployment of API Gateway with such an integration differs based on the specific product being integrated. For more information on a particular integration, see the appropriate integration or interoperability guide, available from Oracle Support.

Prerequisites 2

This topic describes the prerequisites for installing API Gateway. This includes the system requirements, any platform-specific preparation, required software, preinstallation tasks, and so on. You must ensure that your target system meets all of the prerequisites before installing API Gateway.

This topic includes the following:

System requirements

This section describes the supported platforms and other system requirements for Oracle API Gateway, and specific requirements for API Gateway components. For more details on API Gateway components, see the *API Gateway Concepts Guide*.

Operating systems and hardware

This section describes the operating system requirements for API Gateway.

Platform	Supported versions	Hardware prerequisites
Windows	• Windows 8.1 • Windows 7 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 SP1+	• Supports 32-bit and 64-bit hardware (Win32 mode when running on 64-bit hardware) • Intel Core or AMD Opteron at 2Ghz with Dual Core or faster
Solaris	• Solaris 10 Update 4+	• Supports 32-bit and 64-bit Solaris running on 32-bit and 64-bit hardware respectively (32-bit application when running on 64-bit hardware) • Solaris compatible SPARC processor at 440 MHz or faster, sparc32 or sparc64 (32-bit or 64-bit)

Platform	Supported versions	Hardware prerequisites
Linux	• Oracle Linux 5.x, 6.x • Red Hat Enterprise Linux 5.x, 6.x • SUSE Linux Enterprise Server 11.x Oracle software might not run on systems that do not meet these requirements (see **Note** below).	• Supports 32-bit and 64-bit Linux running on 32-bit and 64-bit hardware respectively • Intel Core or AMD Opteron at 2Ghz with Dual Core or faster, i386 or x86_64 (32-bit or 64-bit)

Note 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.

Disk space and RAM requirements

The disk space and RAM requirements for Windows, Solaris, and Linux platforms are:

- Minimum 2 GB free disk space, 50 GB recommended
- Minimum 4 GB physical memory

Additionally, Solaris and Linux platforms require the following:

- Minimum 500 MB available in the `/tmp` directory and writable permissions on the `/tmp`, `/var/tmp`, and `/usr/tmp` directories

Databases

API Gateway Analytics supports the following databases:

- MySQL Server 5.1, 5.6
- Microsoft SQL Server 2005, 2008, 2012
- Oracle 11.2.0.1.0, 12.1.0.1.0
- IBM DB2 9.7, 10.5

Web browsers

API Gateway Manager and other browser-based client components support the following browsers:

- Internet Explorer 8, 9, 10, and 11
- Firefox 13.0 or higher
- Safari 5.1.7 or higher

Thick client platforms

Policy Studio runs on the same platforms as API Gateway with the following additional requirements on Linux and Solaris:

- X-Windows environment
- GTK+ 2

Specific component requirements

This section describes requirements for specific API Gateway components.

Component	Requirements
Policy Studio	Policy Studio is a thick client and supports the platforms described in *Thick client platforms* on page 14.
API Gateway Manager	API Gateway Manager is a web-based client ans supports the web browsers listed in *Web browsers* on page 13.
API Gateway Analytics	The API Gateway Analytics server component has the same operating system and hardware requirements as API Gateway. See *Operating systems and hardware* on page 12. API Gateway Analytics requires a database. For database requirements, see *Databases* on page 13. The browser-based client component supports the same browsers as API Gateway Manager. See *Web browsers* on page 13.

Default ports

This section describes the default ports used by API Gateway components.

API Gateway

The default ports used by API Gateway are as follows:

- **Traffic port**: `8080` (between clients and API Gateway)
- **Management port**: `8085` (between API Gateway and Admin Node Manager)

Admin Node Manager

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

Policy Studio

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

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

API Gateway Manager

The default URL address used by the API Gateway Manager web console to connect to the Admin Node Manager is as follows:

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

API Gateway Analytics

The default port used by API Gateway Analytics for reporting, monitoring, and management is `8040` .The default URL address by the API Gateway Analytics web console is as follows:

```
http://localhost:8040/
```

UNIX-based platforms

The following prerequisites apply when installing API Gateway on UNIX-based platforms.

Executable permission

On UNIX/Linux, you must ensure that the installation executable has the appropriate permissions in your environment. For example, you can use the `chmod` command to update the file permissions.

Service packs

Service packs for API Gateway are available from Oracle Support. If any service packs are available for API Gateway 11.1.2.4.0, download and apply them when the installation completes.

For more information on applying a service pack, see *Update API Gateway* on page 45.

Certificates

API Gateway uses Secure Sockets Layer (SSL) for communications between all processes in a domain (for example, internal management traffic between the Admin Node Manager and API Gateway instances).

Certificates are not required during installation, however, certificates will be required after installation to secure API Gateway domains. For more information on configuring and securing API Gateway domains, see the *API Gateway Administrator Guide*.

Install 3

This topic describes the API Gateway installer, including the modes available and how to start the installer in each mode. It also describes the options that you are presented with when performing a GUI mode installation, and the command-line options for the unattended mode.

This topic includes the following:

For information on installing API Gateway components, see *Install API Gateway components* on page 24.

Installation modes

The API Gateway installer has the following installation modes:

- GUI mode
- Unattended command-line mode

Start installation

This section describes how to start the API Gateway installer. The installer is supported on the following platforms:

- Windows
- Linux
- Solaris

Prerequisites

- You have downloaded the installation setup file for your target operating system.
- You have reviewed the prerequisites and system requirements in *Prerequisites* on page 12 and have ensured that your target system is suitable.

Start the API Gateway installer

Locate and run the setup file for your operating system. For example:

Windows

```
OAG-11.1.2.4.0-windows-installer.exe
```

Linux

```
OAG-11.1.2.4.0-linux-installer.run
```

Tip To run the setup in unattended mode, see *Unattended installation* on page 21.

Installation options

When you run the installation setup file it launches in GUI mode by default. The following sections detail the installation options in GUI mode.

Welcome

When you run the setup file in GUI mode, you are presented with an introductory welcome window. Click **Next** to continue with the installation.

Select components

Select the components to be installed, and deselect those that are not to be installed. The API Gateway Server component is selected by default.

Click **Next** to continue.

Specify installation directory

Enter a location or click the browse button to specify the directory where the API Gateway components are to be installed, for example:

Windows	`C:\OAG-11.1.2.4.0`
UNIX/Linux	`/opt/OAG-11.1.2.4.0`

Click **Next** to continue.

Set the administrator user name and password

It is important to secure your API Gateway system to protect it from internal and external threats. This window enables you to set the administrator user name and password. This administrator account is used to log in to Policy Studio and API Gateway Manager. These administrator credentials are also used by `managedomain` when connecting to an Admin Node Manager.

Select the check box to set the user name and password for the administrator account and enter a user name and password in the fields.

Caution Ensure that you remember these credentials or you will not be able to log in to Policy Studio or API Gateway Manager.

This option is selected by default, to ensure that you set your own administrator user name and password. To use a default administrator user name and password, you must deselect the check box. The default credentials are available from your Oracle Account Manager.

Click **Next** to continue.

Specify 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.

Specify Admin Node Manager details

This window is only displayed if you selected **No** in *Specify domain connection* on page 18.

Configure the following settings for the Node Manager:

Host Name or IP Address:
Select a host address from the list (defaults to the installation host name).

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

Click **Next** to continue.

Specify local Node Manager details

This window is only displayed if you selected **No** in *Specify domain connection* on page 18.

Configure the following settings for the local Node Manager:

Host Name or IP Address:
Select a host address from the list (for example, `127.0.0.1`).

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

Click **Next** to continue.

Specify Admin Node Manager connection details

This window is only displayed if you selected **No** in *Specify domain connection* on page 18.

Configure the following settings to connect to an existing Admin Node Manager:

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 user name and password (`admin/changeme`). When this is selected, enter a new user name and password. This setting is not selected by default.

Click **Next** to continue.

Specify 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.

Select server configuration option

Select whether to configure a new API Gateway server instance. Defaults to **Yes**.

Click **Next** to continue.

Specify API Gateway server details

This window is only displayed if you selected **Yes** in *Select server configuration option* on page 20.

Configure the following settings:

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`.

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.

Specify API Gateway service details

This window is only displayed if you selected **Yes** in *Select server configuration option* on page 20.

Configure the following settings:

Add a Service 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.

Select startup option

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.

Acknowledge API Gateway Analytics information

This window is only displayed if you selected to install API Gateway Analytics.

An information window is displayed to remind you that you must perform additional steps before you start API Gateway Analytics.

Review the information and click **Next** to continue.

Installation summary

The installer displays a summary of the components that will be installed on your system.

Review the information and click **Next** to begin installing.

Installing

A progress window is displayed showing the progress of the installation. When the installation is complete, click **Next** to continue.

Installation complete

A window is displayed to indicate that the installation is complete. If you selected to install Policy Studio you can select the option to **Launch Oracle Policy Studio**.

The URL of the Admin Node Manager is displayed (for example, `https://127.0.0.1:8090`). You can go to this URL in your browser to access the API Gateway Manager tools.

Click **Finish** to complete the installation. Policy Studio is launched if you selected that option.

Unattended installation

You can run the API Gateway installer in unattended mode on the command line. Perform the following steps:

1. Change to the directory where the setup file is located.
2. Run the setup file with the `--mode unattended` option.

The following example shows how to install all API Gateway components in unattended mode:

Windows

```
OAG-11.1.2.4.0-windows-installer.exe --mode unattended
--prefix C:\OAG-11.1.2.4.0
```

Linux

```
./OAG-11.1.2.4.0-linux-installer.run --mode unattended
--prefix /opt/OAG-11.1.2.4.0
```

The components are installed in the background, in the directory specified by the `--prefix` option.

Unattended mode options

For a description of all the available command-line options and their default settings, run the setup file with the `--help` option. This outputs the help text in a separate console. For example:

Windows

```
OAG-11.1.2.4.0-windows-installer.exe --help
```

Linux

```
./OAG-11.1.2.4.0-linux-installer.run --help
```

The following table summarizes some of the more common options:

Option	Description
`--help`	Display available options and default settings.
`--mode`	Specify an installation mode.
`--setup_type`	Specify a setup type.
`--enable-components`	Specify a comma-separated list of components to enable.
`--disable-components`	Specify a comma-separated list of components to disable.
`--prefix`	Specify an installation directory.
`--unattendedmodeui`	Specify different levels of user interaction when installing on Windows or on a UNIX/Linux system with X-Windows.

Option	Description
`--optionfile`	Specify options in a properties file. For more information on option files, go to: http://installbuilder.bitrock.com/docs/installbuilder-userguide.html

Install API Gateway components

4

This topic describes how to install API Gateway components.

The API Gateway installer enables you to install the following API Gateway components:

- API Gateway Server – See *Install the API Gateway server* on page 24.
- API Gateway Analytics – See *Install API Gateway Analytics* on page 26.
- Policy Studio – See *Install Policy Studio* on page 37.
- API Gateway Explorer – See *Install API Gateway Explorer* on page 38.
- Configuration Studio – See *Install Configuration Studio* on page 40.

For more details on API Gateway components and concepts, see the *API Gateway Concepts Guide*.

Install the API Gateway server

Overview

The API Gateway server is the main runtime environment consisting of an API Gateway instance and a Node Manager. For more details on API Gateway components and concepts, see the *API Gateway Concepts Guide*.

Prerequisites

Ensure that all of the prerequisites detailed in *Prerequisites* on page 12 are met.

Install the API Gateway server

To install the API Gateway server in GUI mode, perform an installation following the steps described in *Installation options* on page 17, using the following selections:

- Select to install the API Gateway server component only.

To install the API Gateway server in unattended mode, follow the steps described in *Unattended installation* on page 21.

The following example shows how to install the API Gateway server component in unattended mode:

```
./OAG-11.1.2.4.0-linux-installer.run --mode unattended
--setup_type advanced
--enable-components apigateway
--disable-components nodemanager,analytics,policystudio,
apitester,configurationstudio
```

Start API Gateway

If you selected to start the API Gateway after installation, the Admin Node Manager and API Gateway instance start automatically. Otherwise, you must start them manually.

To start the API Gateway manually, follow these steps:

1. Open a command prompt in the following directory:

Windows	`INSTALL_DIR\apigateway\Win32\bin`
UNIX/Linux	`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.
4. To launch API Gateway Manager, enter the following address in your browser:

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

   `HOST` refers to the host name or IP address of the machine on which API Gateway is running (for example, `https://localhost:8090/`).
5. Enter the administrator user name and password. This is the administrator user name and password you entered during installation.

Note 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 *API Gateway Administrator Guide*.

Related topics

Set up services on page 43

Install API Gateway Analytics

Overview

API Gateway Analytics is a server runtime and web-based console for analyzing and reporting on API use over extended periods of time. For more details on API Gateway components and concepts, see the *API Gateway Concepts Guide*.

Prerequisites

Ensure that all of the prerequisites detailed in *Prerequisites* on page 12 are met.

Enable PDF report generation

To enable the automatic generation of PDF reports, you must download the `wkhtmltopdf` tool, and install it into your API Gateway Analytics installation. For more details, see *Enable PDF report generation* on page 27.

Install API Gateway Analytics

To install API Gateway Analytics in GUI mode, perform an installation following the steps described in *Installation options* on page 17, using the following selections:

- Select to install the API Gateway Analytics component only.

To install API Gateway Analytics in unattended mode, follow the steps described in *Unattended installation* on page 21.

The following example shows how to install the API Gateway Analytics component in unattended mode:

```
./OAG-11.1.2.4.0-linux-installer.run --mode unattended
--setup_type advanced
--enable-components analytics
--disable-components nodemanager,apigateway,policystudio,
apitester,configurationstudio
```

Configure your API Gateway Analytics database

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

1. Create a database instance. For more details, see *Configure the database for API*

Gateway Analytics on page 28. Alternatively, if you already have an existing database, skip to the next step.

2. Update your API Gateway Analytics configuration with the database details using the `configureserver` script. For more details, see *Configure API Gateway Analytics* on page 33.
3. Configure the database tables using the `dbsetup` script. For more details, see *Configure the database for API Gateway Analytics* on page 28.
4. Enable writing of metrics from your API Gateway instance to the database using the managedomain tool. For more details, see *Configure API Gateway Analytics* on page 33.

Start API Gateway Analytics

To start 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. To launch API Gateway Analytics, enter the following address in your browser:

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

   `HOST` refers to the host name or IP address of the machine on which API Gateway Analytics is running (for example, `https://localhost:8040/`).
3. Enter the API Gateway Analytics user name and password.

   Note This is not the same as the API Gateway Manager user name and password. You can edit the API Gateway Analytics user in Policy Studio under the **Users and Groups > Users** node.

Note API Gateway Analytics produces reports based on metrics stored by API Gateway when processing messages. To produce a graph showing the number of connections made by 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 or clients configured, you must restart API Gateway and API Gateway Analytics.

Enable PDF report generation

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/platform/bin/wkhtmltopdf`

Further information

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

Related topics

Set up services on page 43

Configure the database for API Gateway Analytics

Overview

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 a database for use with API Gateway Analytics. It describes the prerequisites and shows an example of creating a 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:

Install API Gateway Analytics

You must install Oracle API Gateway Analytics. For details on how to install API Gateway Analytics, see *Install API Gateway Analytics* on page 26.

Install a JDBC database

You must install a JDBC-compliant database 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.

Add JDBC driver files

You must add the JDBC driver files for your chosen database to your API Gateway, API Gateway Analytics, and Policy Studio installations.

Add JDBC drivers to API Gateway

To add the third-party JDBC driver files for your database to API Gateway, perform the following steps:

1. Add the binary files for your database driver as follows:
   - Add `.jar` files to the following directories
     - `INSTALL_DIR/apigateway/ext/lib`
     - `INSTALL_DIR/apigateway/groups/GROUP-ID/INSTANCE-ID/ext/lib`
   - Add `.dll` files to the `INSTALL_DIR\apigateway\Win32\lib` directory.
   - Add `.so` files to the `INSTALL_DIR/apigateway/platform/lib` directory.
2. Restart API Gateway.

Add JDBC drivers to API Gateway Analytics

To add the third-party JDBC driver files for your database to API Gateway Analytics, perform the following steps:

1. Add the binary files for your database driver as follows:
   - Add `.jar` files to the `INSTALL_DIR/analytics/ext/lib` directory.
   - Add `.dll` files to the `INSTALL_DIR\analytics\Win32\lib` directory.
   - Add `.so` files to the `INSTALL_DIR/analytics/platform/lib` directory.
2. Restart API Gateway Analytics.

Add JDBC drivers to Policy Studio

To add third-party binaries to Policy Studio, perform the following steps:

1. Select **Windows** > **Preferences** > **Runtime Dependencies** from the Policy Studio main menu.
2. Click **Add** to select a JAR file to add to the list of dependencies.
3. Click **Apply** when finished. A copy of the JAR file is added to the `plugins` directory in your Policy Studio installation.
4. Click **OK**.
5. Restart Policy Studio using the `policystudio -clean` command.

Create the 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 API Gateway stores its message metrics and audit trail data. You must first create this database using the third-party database 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.

The following example shows creating a MySQL database:

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

In this example, the database is named `reports`, but you can use any appropriate name.

Set up the database tables

When you have created the database, the next step is to set up the database tables. You can do this by running the `dbsetup` command without any options from the following API Gateway Analytics directory:

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

The following example command shows setting up new database tables:

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

Specify options to dbsetup

Note When you specify command-line arguments to `dbsetup`, the script does not run interactively. You should run `dbsetup` without any options to create the database tables.

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).

Option	Description
`--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.

dbsetup examples

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

Connect 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
```

Connect 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
```

Install a database

You can also use the `--dburl` option to set up 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
```

Reinstall 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` directory in the following subdirectories:

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

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

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

Configure API Gateway Analytics

Overview

This topic describes how to update API Gateway Analytics configuration (for example, the API Gateway Analytics port, database connection, and user credentials) before starting API Gateway Analytics. You can use the `configureserver` script (recommended) to guide you through all the required steps, or you can use Policy Studio to configure the API Gateway Analytics configuration file.

Prerequisites

The prerequisites for configuring API Gateway Analytics are as follows:

Install API Gateway

Because API Gateway Analytics reports on transactions processed by API Gateway in real time, you must first install API Gateway. For more details, see *Install the API Gateway server* on page 24.

Note To view API Gateway metrics in API Gateway Analytics, you must also enable the recording of metrics. For more details, see *Enable metrics for your API Gateway host* on page 36.

Install API Gateway Analytics

You must install API Gateway Analytics. For details on how to install API Gateway Analytics, see *Install API Gateway Analytics* on page 26.

Configure a database

You must install a JDBC-compliant database to store the API Gateway monitoring and transaction data. For more details, see *Configure the database for API Gateway Analytics* on page 28.

Update API Gateway Analytics configuration

By default, API Gateway Analytics is configured to read message metrics from a MySQL database stored on the local machine. You can use the `configureserver` command to configure API Gateway Analytics to use an alternative database, change the user credentials on the default database connection, or use a different listening port.

Update configuration 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`
UNIX/Linux	`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 a different port.
4. Enter the database connection URL. Defaults to `jdbc: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 window (for example, number of client requests, requests per service, and so on). For more details on generated PDF reports, see the *API Gateway Administrator 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 under the **Users and Groups** node in 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@oracle.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...
```

Update configuration 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@oracle.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.

Update configuration in 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 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. 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 *API Gateway Policy Developer Guide*.

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

Enable metrics for your API Gateway host

Finally, you must use the managedomain tool to enable writing of metrics from the API Gateway instances on your host to the metrics database. This enables the Node Manager to process event logs from your API Gateway instances, and to write metrics data to the metrics database.

The following example uses the interactive `managedomain --menu` command:

```
Select option: 2
Select a host:
1) LinuxMint01
2) Enter host name
Enter selection from 1-2 [2]: 1
Hit enter to continue...
Enter a new host name [LinuxMint01]:
Enter a new Node Manager name [Node Manager on LinuxMint01]:
Enter a new Node Manager port [8090]:
There is only one Node Manager in this domain so it must remain as an Admin Node
Manager
Do you want to create an init.d script for this Node Manager [n]:
```

```
Do you want to reset the passphrase for the Node Manager on this host ? [n]:
Do you wish to edit metrics configuration (y or n) ? [n]: y
Do you wish to enable metrics (y or n) ? [y]: y
Enter metrics database URL [jdbc:mysql://127.0.0.1:3306/reports]:
Enter metrics database username [root]:
Enter metrics database plaintext password [*******]:
Testing Database connectivity for : jdbc:mysql://127.0.0.1:3306/reports, user : root
Metrics database connectivity succeeded
Metrics generation enabled. All other specified metrics settings updated.
Metrics settings updated successfully. Please reboot Node Manager on completion of
this program.
Completed successfully.
```

For more details on configuring API Gateway for API Gateway Analytics, see the *API Gateway Administrator Guide*.

Install Policy Studio

Overview

Policy Studio is a graphical IDE that enables developers to virtualize APIs and develop policiesto enforce security, compliance, and operational requirements. For more details on API Gateway components and concepts, see the *API Gateway Concepts Guide*.

Prerequisites

Ensure that all of the prerequisites detailed in *Prerequisites* on page 12 are met.

Install Policy Studio

To install Policy Studio in GUI mode, perform an installation following the steps described in *Installation options* on page 17, using the following selections:

- Select to install the Policy Studio component only.

To install Policy Studio in unattended mode, follow the steps described in *Unattended installation* on page 21.

The following example shows how to install the Policy Studio component in unattended mode:

```
./OAG-11.1.2.4.0-linux-installer.run --mode unattended
--setup_type advanced
--enable-components policystudio
```

```
--disable-components analytics,nodemanager,apigateway,
apitester,configurationstudio
```

Start Policy Studio

Note Before starting Policy Studio, ensure that the Admin Node Manager and the API Gateway instance are running. For more details, see *Start API Gateway* on page 25.

If you did not select to launch 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. Run `policystudio`.
4. When Policy Studio starts up, click the Admin Node Manager link to display the Open Connection dialog.
5. In the Open Connection dialog, enter the administrator user name and password and click **OK**. This is the administrator user name and password you entered during installation.
6. In the Topology view, double-click the API Gateway instance to load the configuration for the active API Gateway.
7. If Node Manager credential checking is enabled, enter the administrator user name and password in the Node Manager credentials dialog, and click **OK**. This is the administrator user name and password you entered during installation. To disable credential checking for future deployment or topology operations, deselect the **Always prompt for user credentials** check box.
8. If a passphrase has been set, enter it in the Enter Passphrase dialog, and click **OK**. Alternatively, if no passphrase has been set, click **OK**. For more details on setting a passphrase, see the *API Gateway Administrator Guide*.

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

Install API Gateway Explorer

Overview

API Gateway Explorer is a graphical tool that enables you to test API functionality, performance, and security. For more details on API Gateway components and concepts, see the *API Gateway Concepts Guide* .

Prerequisites

Ensure that all of the prerequisites detailed in *Prerequisites* on page 12 are met.

Install API Gateway Explorer

To install API Gateway Explorer in GUI mode, perform an installation following the steps described in *Installation options* on page 17, using the following selections:

- Select to install the API Gateway Explorer component only.

To install API Gateway Explorer in unattended mode, follow the steps described in *Unattended installation* on page 21.

The following example shows how to install the API Gateway Explorer component in unattended mode:

```
./OAG-11.1.2.4.0-linux-installer.run --mode unattended
--setup_type advanced
--enable-components apitester
--disable-components analytics,nodemanager,apigateway,
policystudio,configurationstudio
```

Start API Gateway Explorer

Note Before starting API Gateway Explorer, ensure that the Admin Node Manager and the API Gateway instance are running. For more details, see *Start API Gateway* on page 25.

To start API Gateway Explorer after installation, perform the following steps:

1. Open a command prompt.
2. Change to your API Gateway Explorer installation directory (for example, `INSTALL_DIR\apitester`).
3. Run `apitester`.

For more details on API Gateway Explorer, see the *API Gateway Explorer User Guide*.

Install Configuration Studio

Overview

Configuration Studio is a graphical tool that enables administrators to configure environment-specific properties to deploy APIs and policies in non-development environments. For more details, see the *API Gateway Deployment and Promotion Guide*.

Prerequisites

Ensure that all of the prerequisites detailed in *Prerequisites* on page 12 are met.

Install Configuration Studio

To install Configuration Studio in GUI mode, perform an installation following the steps described in *Installation options* on page 17, using the following selections:

- Select to install the Configuration Studio component only.

To install Configuration Studio in unattended mode, follow the steps described in *Unattended installation* on page 21.

The following example shows how to install the Configuration Studio component in unattended mode:

```
./OAG-11.1.2.4.0-linux-installer.run --mode unattended
--setup_type advanced
--enable-components configurationstudio
--disable-components analytics,nodemanager,apigateway,
apitester,policystudio
```

Start Configuration Studio

To start Configuration Studio after installation, perform the following steps:

1. Open a command prompt.
2. Change to your Configuration Studio installation directory (for example, `INSTALL_DIR\configurationstudio`).
3. Run `configurationstudio`.

For more details on Configuration Studio, see the *API Gateway Deployment and Promotion Guide*.

Post-installation 5

This topic describes various tasks that you might perform after installing API Gateway. This includes how to check if an installation has been successful, any initial configuration needed before you can start API Gateway, what you should do to secure API Gateway, and so on.

This topic includes the following:

Verify the installation

To verify your installation, follow these guidelines:

- Check the installation results
- Start API Gateway components
- Log in to the API Gateway tools

Check the installation log

You can examine the installation log in the root directory of the installation (for example, `Oracle-installLog.log`).

Start API Gateway components

- To start the API Gateway Server and Admin Node Manager, see *Start API Gateway* on page 25.
- To start API Gateway Analytics, see *Start API Gateway Analytics* on page 27.

Log in to the API Gateway tools

- To start the Policy Studio desktop tool, see *Start Policy Studio* on page 38.
- To log in to the API Gateway Manager web-based administration tool, see *Start API Gateway* on page 25.
- To start the Configuration Studio desktop tool, see *Start Configuration Studio* on page 40.
- To start the API Gateway Explorer desktop tool, see *Start API Gateway Explorer* on page 39.
- To log in to the web-based API Gateway Analytics interface, see *Start API Gateway Analytics* on page 27.

Initial configuration

Depending on the installation options you selected, the following tasks might need to be completed before you can start API Gateway.

Create a new domain

To create a new managed domain and API Gateway instance, you can use the `managedomain` script.

You can run `managedomain` from the following directory:

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

For more details on running `managedomain`, see the *API Gateway Administrator Guide*.

Set up a database for API Gateway Analytics

If you installed API Gateway Analytics, you must set up a JDBC-compliant database, before you can start API Gateway Analytics:

- First, you must install and configure a database to store the monitoring and transaction data read by API Gateway Analytics. See *Configure the database for API Gateway Analytics* on page 28.
- Next, you must configure API Gateway Analytics to use this database instead of the default (a MySQL database stored on the local machine). See *Configure API Gateway Analytics* on page 33.

Secure API Gateway

It is important to secure your API Gateway system as soon as possible after installation, to protect the API Gateway environment from internal or external threats.

Change default passwords

If you did not set an administrator user name and password during installation, you should change the default administrator user name and password now. For more details on managing administrator users, see the *API Gateway Administrator Guide*.

Change default certificates

The default certificates used to secure API Gateway components are self-signed. You can replace these self-signed certificates with certificates issued by a Certificate Authority (CA). For more information, see the *API Gateway Administrator Guide*.

Encrypt API Gateway configuration

By default, API Gateway configuration is unencrypted. You can specify a passphrase to encrypt API Gateway instance configuration. For more details, see the *API Gateway Administrator Guide*.

Run as non-root on UNIX/Linux

In a typical deployment on Linux or Solaris, the process for the API Gateway instance runs as `root`, to enable the API Gateway to listen on privileged ports. However, you can run the API Gateway process as a non-root user and still allow access to privileged ports. For more details, see the *API Gateway Administrator Guide*.

Set up services

You can run Node Managers and API Gateway instances as services using the `managedomain` script. To register a Node Manager or an API Gateway instance as a service on Windows or UNIX/Linux, you must run the `managedomain` command as `Administrator` on Windows or `root` on UNIX/Linux.

To run a Node Manager as a service, enter the `managedomain --menu` command to run the managedomain utility and choose option 2, `Edit a host`.

To run an API Gateway instance as a service, enter the `managedomain --menu` command and choose option 10, `Add script or service for existing local API Gateway`.

Alternatively, you can run `managedomain` in command mode with the `--add_service` option to create a service for a Node Manager or API Gateway instance.

For more information on `managedomain`, see the *API Gateway Administrator Guide*.

API Gateway Analytics

You can also run API Gateway Analytics as a service. However, in this case you must create the script manually. A sample script and *ReadMe* is provided in the `INSTALL_DIR/analytics/posix/samples/etc/init.d/` directory.

Set up clustering

To set up API Gateway for high availability, you need to configure the embedded Apache Cassandra database for clustering. For more information, see the *API Gateway Administrator Guide*.

Next steps

Consult the *API Gateway Administrator Guide* for more information on administering, managing, and troubleshooting an API Gateway system. This guide contains many topics that you will find useful after installing API Gateway. For example:

- Manage an API Gateway domain
- Configure API Gateway for high availability
- Backup and disaster recovery
- Configure scheduled reports
- Manage user access

Update API Gateway 6

This section describes how to apply service packs or patches to API Gateway components.

Install a service pack

This section describes how to install a service pack on an existing installation of API Gateway.

To install a service pack, follow these general guidelines:

1. Stop any Node Managers and API Gateway servers.
2. Back up your existing installation. For more information on backing up, see the *API Gateway Administrator Guide*.
3. Download the service pack and the associated *Readme*.
4. Review the *Readme* for any specific installation instructions.
5. Unzip and extract the service pack. A service pack contains new binaries only and does not overwrite the existing configuration.
6. Restart the Node Managers and API Gateway servers.

Upgrade and migration 7

This topic outlines the tasks to upgrade API Gateway from version 11.1.2.x or 11.1.1.x to version 11.1.2.4.0. This process can be used to both upgrade your component binaries and migrate your configuration data.

The upgrade process enables you to upgrade the following from version 11.1.2.x or 11.1.1.x to version 11.1.2.4.0:

Component	Description
Configuration (policies, filters, certificates, and so on)	Configuration data for API Gateway instances, Node Managers, and groups.
Domain topology	Domains, hosts, API Gateways, and groups.
Client Application Registry	The Client Application Registry is used to store OAuth 2.0 client applications.
KPS	The key property store (KPS) is used to store metadata for policies, and OAuth client application data.
Databases	Databases can be used to store OAuth tokens and codes, and as a persistent store for the key property store.
Cassandra	Embedded Apache Cassandra database.
LDAP directory services	LDAP directory services can be used instead of the API Gateway user store to store user authentication information.
Administrator users	Users who were created in the API Gateway Manager web interface, including the default administrator user.
Ext/lib	Contents of the `ext/lib` directory. This directory contains any external JAR files that have been added to the API Gateway CLASSPATH.
System configuration	Java virtual machine arguments and other configuration in `jvm.xml`.

Upgrade is supported on Linux and Windows platforms.

This topic includes the following:

Before you upgrade

This topic details any issues you should consider before you upgrade.

Upgrades from version 11.1.2.3.0 and higher

If you are upgrading from version 11.1.2.3.0 or higher, the SSL certificates from the old installation will be used by the new installation. If you are upgrading from earlier versions, new SSL certificates are generated, and a system-generated domain private key and certificate is used by default. To use another certificate management option for the internal certificates (for example, a user-provided domain private key and certificate, or an external CA), you can replace the certificates using the `managedomain --regen_certs` option after the upgrade. For more information on regenerating certificates, see the *API Gateway Administrator Guide* .

SSL is used for internal communications. The certificates mentioned in this section relate to the certificates for internal communications between two Node Managers, and between a Node Manager and an API Gateway.

Ensure groups are consistent

Before you upgrade, you must ensure that all groups are consistent (all API Gateways in a group must have the same configuration). Upgrade is not supported for inconsistent groups.

Upgrade steps

This section describes how to upgrade your existing 11.1.1.x or 11.1.2.x installation and migrate your data to API Gateway version 11.1.2.4.0. It describes the steps involved in an upgrade from version 11.1.1.x or version 11.1.2.x (old installation) to version 11.1.2.4.0 (new installation) for both single node and multinode systems.

Back up the old installation

Back up the old 11.1.2.x installation on each node, including any databases:

- Back up the `apigateway` or `apiserver` directory.
- Back up any databases. For example, you can back up a MySQL database by creating a DUMP file of the tables in use. For more information, see the user documentation for your database.

For more information on backing up the system, see the *API Gateway Administrator Guide*.

Important points to note when completing this step

Do not shut down the old installation.

Install API Gateway 11.1.2.4.0

Install API Gateway 11.1.2.4.0 in a different directory to your old 11.1.2.x installation on each node. For example, if the old installation is installed in `OLD_INSTALL_DIR`, install the new installation in `NEW_INSTALL_DIR`. For more information on installation, see *Installation options* on page 17.

Important points to note when completing this step

- Do not overwrite the old installation.
- Use the **Advanced** installation option to install API Gateway and select the Admin Node Manager and API Gateway server components only.
- Do not create or start any Node Managers, groups, or API Gateways in the new installation.
- Do not shut down the old installation.

Perform the upgrade

To perform an upgrade, a script called `sysupgrade` is provided. The `sysupgrade` script exports your data from an existing installation, upgrades it, and imports it into a new API Gateway11.1.2.4.0 installation.

The steps you must follow to preform the upgrade differ for upgrades on a single node system and a multinode system.

Single node upgrade

To perform an upgrade on a single node system, follow these steps:

1. Change to the following directory in the new installation:

   ```
   NEW_INSTALL_DIR/apigateway/upgrade/bin
   ```

2. Run the `sysupgrade` command:

   ```
   ./sysupgrade
   ```

Note For more information on the options you can specify to the sysupgrade command, see *Upgrade script* on page 54.

3. You are prompted to enter the full path of the old installation (the installation being upgraded).
4. You are presented with a summary of the upgrade process. This includes the following information:
   - The location of the log files
   - The version of API Gateway being upgraded
   - Whether this is a single node or multinode system
   - The trace level
5. The upgrade proceeds. The process consists of four steps. You are prompted for various information and to complete various tasks during the course of the upgrade.

   Step 1 – Export
   - The data is exported from the old installation.
   - You are prompted to enter the administrator user name and password for the old installation.

   Step 2 – Upgrade
   - The data from the old installation is upgraded.

   Step 3 – Upgrade external database
   - Any external databases used for KPS or OAuth are upgraded if required.

   Step 4 – Create and import
   - A new system is created that matches the old topology and the upgraded data is imported.
   - You are prompted to shut down the old installation.
   - The Node Manager in the new installation is started by the upgrade process (upgrades on Linux) or you are prompted to start the Node Manager in the new installation (upgrades on Windows). The API Gateway instance is then started by the upgrade process.
6. When all steps are completed successfully, the upgrade completes with the message `"System upgrade complete"`.

   Note In the case of any errors during the upgrade process, consult the log files to find the source of the problem. When you have resolved any problems you can rerun the upgrade. For more information on resolving problems and rerunning the upgrade, see *Troubleshooting an upgrade* on page 53.

Multinode upgrade

To perform an upgrade on a multinode sytem, the process is similar to upgrading a single node system (see *Single node upgrade* on page 48), however, you must upgrade the nodes in a specific order. Follow these steps:

1. Run the `sysupgrade` command on an Admin Node Manager node.
2. Run the `sysupgrade` command on the other nodes in the system.
3. Wait until all nodes are prompting you to shut down the old installation.
4. Shut down the old installation.
5. Continue the upgrade on the Admin Node Manager node.
6. Continue the upgrade on the other nodes in the system.
7. Start the node managers in the new installations on each node when prompted.
8. The upgrade completes on all nodes.

Additional steps for upgrade from 11.1.2.x

The following additional steps might be required, depending on your configuration:

- RBAC – Administrator users are imported into the new 11.1.2.4.0 installation. However, if you have made changes to the Role-Based Access Control (RBAC) files in your API Gateway to modify roles and permissions, you must reapply these changes manually in the new API Gateway installation.
- Node Managers and API Gateways as a service – If any of your processes are running as a service, you must manually update the services with the new settings.
- Cassandra HA – If you are using Cassandra in a high availability (HA) configuration you must set the replication factor and resynchronize the cluster. For more information, see *Set the replication factor and resynchronize Cassandra HA* on page 50.
- OAuth client applications – If you are upgrading from version 11.1.2.0.x, use the `migrateFrom71.py` script to migrate any existing client applications. See the *API Gateway OAuth User Guide* for more information.

Set the replication factor and resynchronize Cassandra HA

The following example steps show how to set a replication factor of 3 and resynchronize a 3 node cluster consisting of `node-1`, `node-2`, and `node-3`:

1. Open a command prompt at the following directory in your new 11.1.2.4.0 installation:

   ```
   NEW_INSTALL_DIR/apigateway/posix/bin
   ```

2. Enter `./cassandra-cli [-h node-1]` to connect the Cassandra command-line interface to the `node-1` node.
3. Enter `use kps;` to use the `kps` keyspace.
4. Enter the following:

   ```
   update keyspace kps with strategy_options = {replication_factor:3};
   ```

5. Enter the following to quit:

```
quit;
```

6. Run the following commands to synchronize the update on each node:

```
./nodetool -h node-1 repair kps
./nodetool -h node-2 repair kps
./nodetool -h node-3 repair kps
```

7. Run the following command against each node to display cluster information:

```
./nodetool -h node-1 ring kps
./nodetool -h node-2 ring kps
./nodetool -h node-3 ring kps
```

   You should see an effective ownership of 100% on each node.

For more information on configuring high availability, see the *API Gateway Administrator Guide*.

Additional steps for upgrade from 11.1.1.x

The following additional steps might be required, depending on your configuration:

- API Gateway Analytics database tables – If you have an existing installation of API Gateway Analytics version 11.1.1.6.x, you can upgrade your database tables to version 11.1.2.0.x using the `dbsetup` script. For more information, see *Upgrade API Gateway Analytics database tables* on page 51.
- API Gateway Analytics – If you have made changes to the configuration of an existing installation of API Gateway Analytics, and you do not wish to reconfigure these changes, you can use the `upgradeconfig` script to upgrade API Gateway Analytics. For more information, see *Upgrade API Gateway Analytics* on page 52.

Upgrade API Gateway Analytics database tables

Note You must upgrade version 11.1.1.6.x database schemas to 11.1.2.x for API Gateway to function correctly. Database schema upgrades are not supported for versions earlier than 11.1.1.6.x. 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\&lc_
reporter;/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
```

The `dbsetup` utility uses SQL upgrade scripts located in the following directory:

`INSTALL_DIR/apigateway/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.

Upgrade API Gateway Analytics

To upgrade API Gateway Analytics, run the `upgradeconfig` script from the following location:

Windows

`INSTALL_DIR\analytics\Win32\bin`

UNIX/Linux

`INSTALL_DIR/analytics/posix/bin`

For more details on running this script, see the version 11.1.2.2.1*API Gateway Installation and Configuration Guide*.

Note This step is normally not required unless you have made significant changes to the configuration of an existing installation of API Gateway Analytics (for example, for RBAC).

Verify the upgrade

To verify that the upgrade has been successful, perform the following steps:

- Use the `managedomain` tool to:
  - Print the topology.
  - Download a deployment archive.

  For more information on using `managedomain`, see the *API Gateway Administrator Guide*.

- Start Policy Studio and connect to an Admin Node Manager. For more information, see the *API Gateway Policy Developer Guide*.
- Start API Gateway Manager and view the topology, administrator users, and Key Property Stores. For more information, see the *API Gateway Administrator Guide*.
- Start the Client Application Registry web interface and view the client applications. For more information, see the *API Gateway OAuth User Guide*.

Troubleshooting an upgrade

This section provides some advice on troubleshooting the upgrade process.

Resolve upgrade failures

If the upgrade process fails, you can examine the logs to find the cause of the failure. All output from the upgrade process is logged to the `out/logs` directory. The summary provided when you run `sysupgrade` also provides the location of the log file.

The following are common problems and solutions when running `sysupgrade`:

Problem: Step 1 (Export), step 2 (Upgrade), or step 3 (Upgrade external database) failed.

Solution: Resolve the issue and rerun `sysupgrade`.

Problem: Step 4 (Create and import) failed.

Solution: Resolve the issue, shut down the new system (if it is running), and rerun `sysupgrade` with the `--reapply` option.

Problem: The upgrade failed and you want to start the upgrade again from scratch.

Solution: Run `sysupgrade` again with the `--clean` option.

ext/lib customizations

If you have customizations in your `ext/lib` directory they might cause problems in the new 11.1.2.4.0 installation. Customizations might need to be reapplied against the latest installation.

Tracing

When running any of the commands you can add the following options to the command-line to generate more debug information:

```
--tracelevel=DEBUG
```

```
--tracelevel=VERBOSE
```

Upgrade script

To perform an upgrade, a Python script called `sysupgrade` is provided. The `sysupgrade` script is located in the following directory:

```
NEW_INSTALL_DIR/apigateway/upgrade/bin
```

sysupgrade command-line options

For a description of all the available command-line options and their default settings, run the `sysupgrade` command with the `--help` option.

The following table summarizes some of the more common options:

Option	Description
`--help` `-h`	Display available options and default settings.
General options:	
`--clean`	Clean the previous upgrade output and force a system upgrade from scratch.
`--reapply`	Redo new system creation and data import.
`--tracelevel=TRACELEVEL`	Trace level to use for system upgrade process. The default is `INFO`.The available options are: • FATAL • ALWAYS • ERROR • INFO • MIN • DEBUG • VERBOSE Use DEBUG or VERBOSE for detailed debug output.

Option	Description
`--noprompt`	Allow automated control of system upgrade. In this case the sysupgrade command returns the following values: • 0 – The upgrade completed successfully. • 1 – You must shutdown the old installation and rerun. • 100+ – An error occurred. See the log files for details.
`--docs`	Display full help text.
Node Manager options:	
`--scheme=SCHEME`	Scheme for Admin Node Manager. The default is `https`.
`--host=HOST`	Host name for Admin Node Manager. The default is `localhost`. Specify `localhost` for the first host being upgraded. Specify the host name of the running upgraded Admin Node Manager for all subsequent hosts.
`--port=PORT`	Port number for Admin Node Manager. The default is `8090`.
`--username=USERNAME`	User name for authenticating to the Admin Node Manager.
`--password=PASSWORD`	Password for authenticating to the Admin Node Manager.

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.

OpenSSL Project:
This product includes software developed by the OpenSSL Project 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.

iconmonstr:
This product includes graphic icons developed by iconmonstr.