Oracle® Fusion Middleware

Oracle API Gateway Installation and Configuration Guide

11g Release 2 (11.1.2.3.0)

April 2014

Oracle API Gateway Installation and Configuration Guide, 11g Release 2 (11.1.2.3.0)

30 April 2014

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 API Gateway:

Platform	Supported Versions	Hardware Prerequisites
Windows	• Windows Server 2008 SP1+ • Windows Server 2003 R2+ • Windows Server 2003 SP2 • Windows XP SP2+	• 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 • Minimum 2 GB free disk space, 50 GB recommended • Minimum 4 GB physical memory
Solaris	• Solaris 10 Update 4+	• Supports 32-bit Solaris running on 32-bit hardware only • Solaris compatible SPARC processor at 440 MHz, or faster • Minimum 2 GB free disk space, 50 GB recommended • Minimum 4 GB physical memory
Linux	• Oracle Linux 5.x, 6.x • Red Hat Enterprise Linux 5.x, 6.x • SUSE Linux Enterprise Server 11.x Oracle software may not run on systems that do not meet these requirements (see **Important** 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) • Minimum 2 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 and 9 • Firefox 13.0 or higher • Safari 5.1.7 or higher
API Gateway Analytics	Server component has the same platform requirements as the API Gateway. 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 Browser-based client component supports the same browsers as API Gateway Manager.

Default ports

This section describes the default ports used by specific 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/
```

Installation

Overview

You can install API Gateway in GUI mode or in unattended command-line mode.

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

- API Gateway Server
- API Gateway Analytics
- Policy Studio
- Configuration Studio
- API Gateway Explorer

For more details on API Gateway components and concepts, see the *API Gateway Concepts Guide*. This topic describes how to install API Gateway components on the following platforms:

- Windows
- Linux
- Solaris

Prerequisites

You must ensure the following:

System requirements
See the *System requirements* to ensure that the target machine is of a suitable specification.

Executable permission
On Linux/UNIX, 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.

GUI installation

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

Launch API Gateway installer

Locate and run the setup file for your operating system.

Windows

```
OAG-11.1.2.3.0-windows-installer.exe
```

Linux

```
OAG-11.1.2.3.0-linux-installer.run
```

Tip

To run the setup in unattended mode, see the section called “Unattended installation”.

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 Core 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-11.1.2.3.0`
Linux/UNIX	`/opt/OAG-11.1.2.3.0`

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 the section called “Specify domain connection”.

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 the section called “Specify domain connection”.

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 the section called “Specify domain connection”.

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 username/password (`admin/changeme`). When this is selected, enter a new username/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 the section called “Select server configuration option”.

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 the section called “Select server configuration option”.

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-11.1.2.3.0-windows-installer.exe --mode unattended --prefix C:\OAG-11.1.2.3.0
```

Linux

```
./OAG-11.1.2.3.0-linux-installer.run --mode unattended --prefix /opt/OAG-11.1.2.3.0
```

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-11.1.2.3.0-windows-installer.exe --help
```

Linux

```
./OAG-11.1.2.3.0-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 Linux/UNIX system with X-Windows.
`--optionfile`	Specify options in a properties file. For more information on option files, go to: http://installbuilder.bitrock.com/docs/installbuilder-userguide.html

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*.

Install the API Gateway Core Server

Overview

The API Gateway Core 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*.

Note

It is not necessary to install the API Gateway Core Server on the API Gateway appliance because this component is pre-installed on the appliance.

Prerequisites

Ensure that all of the prerequisites detailed in the section called “Prerequisites” are met.

Install the API Gateway Core Server

To install the API Gateway Core Server in GUI mode, perform an installation following the steps described in the section called “GUI installation”, using the following selections:

- Select to install the API Gateway Core Server component only.

To install the API Gateway Core Server in unattended mode, follow the steps described in the section called “Unattended installation”.

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

Windows

```
OAG-11.1.2.3.0-windows-installer.exe --mode unattended
--setup_type advanced
--enable-components apigateway
--disable-components nodemanager,analytics,policystudio,
apitester,configurationstudio
```

Linux

```
./OAG-11.1.2.3.0-linux-installer.run --mode unattended
--setup_type advanced
--enable-components apigateway
--disable-components nodemanager,analytics,policystudio,
apitester,configurationstudio
```

Note

This topic describes how to install the API Gateway Core Server component only. For details on installing other components, see the following topics:

- *Install API Gateway Analytics*
- *Install Policy Studio*
- *Install API Gateway Explorer*
- *Install Configuration Studio*

Start API Gateway

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

To start the API Gateway manually, follow these steps:

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 Administrator Guide*.

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 the section called “Prerequisites” 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 the section called “Enable PDF report generation”.

Install API Gateway Analytics

To install API Gateway Analytics in GUI mode, perform an installation following the steps described in the section called “GUI installation”, 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 the section called “Unattended installation”.

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

Windows

```
OAG-11.1.2.3.0-windows-installer.exe --mode unattended
--setup_type advanced
--enable-components analytics
--disable-components nodemanager,apigateway,policystudio,
apitester,configurationstudio
```

Linux

```
./OAG-11.1.2.3.0-linux-installer.run --mode unattended
--setup_type advanced
--enable-components analytics
--disable-components nodemanager,apigateway,policystudio,
apitester,configurationstudio
```

Note

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

- *Install the API Gateway Core Server*
- *Install Policy Studio*
- *Install API Gateway Explorer*
- *Install Configuration Studio*

Start API Gateway Analytics

Important

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*. Alternatively, if you already have an existing database, skip to the next step.
2. Configure the database tables using the `dbsetup` script. For more details, see *Configure the database for API Gateway Analytics*.
3. Update your API Gateway Analytics configuration using the `configureserver` script. For more details, see *Configure API Gateway Analytics*.

To start API Gateway Analytics, perform the following steps:

1. Start the API Gateway Analytics server using the `oaganalytics` 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 host name 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 under the **Users and Groups** node in the Policy Studio tree view.

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/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\oaganalytics\Win32\lib\wkhtmltopdf`
UNIX/Linux	`INSTALL_DIR/oaganalytics/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 reports database, see the *Oracle API Gateway User Guide* and the *Oracle API Gateway Administrator Guide*.

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 the *Install API Gateway Analytics* topic.

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 `INSTALL_DIR/apigateway/ext/lib` directory.
   - 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/oaganalytics/ext/lib` directory.
   - Add `.dll` files to the `INSTALL_DIR\oaganalytics\Win32\lib` directory.
   - Add `.so` files to the `INSTALL_DIR/oaganalytics/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 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.

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 whatever name you wish.

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 from the following API Gateway Analytics directory:

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

The following example command shows setting up new database tables:

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

Specify 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:

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 `db_schema.sql` file in the appropriate directory for your database. The following example shows creating the tables for a MySQL database:

```
mysql> \. C:\oracle\oaganalytics\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)
...
```

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 Core Server*.

Important

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

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

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*.

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\oaganalytics\Win32\bin`
Linux/UNIX	`INSTALL_DIR/oaganalytics/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 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\oaganalytics\Win32\bin>configureserver.bat
Connecting to configuration at : federated:file:///C:\Oracle\oaganalytics/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/oaganalytics/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. 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.

Install Policy Studio

Overview

Policy Studio is a graphical IDE that enables developers to virtualize APIs and develop policies to 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 the section called “Prerequisites” are met.

Install Policy Studio

To install Policy Studio in GUI mode, perform an installation following the steps described in the section called “GUI installation”, using the following selections:

- Select to install the Policy Studio component only.

To install Policy Studio in unattended mode, follow the steps described in the section called “Unattended installation”.

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

Windows

```
OAG-11.1.2.3.0-windows-installer.exe --mode unattended
--setup_type advanced
--enable-components policystudio
--disable-components analytics,nodemanager,apigateway,
apitester,configurationstudio
```

Linux

```
./OAG-11.1.2.3.0-linux-installer.run --mode unattended
--setup_type advanced
--enable-components policystudio
--disable-components analytics,nodemanager,apigateway,apitester,
configurationstudio
```

Note

This topic describes how to install the Policy Studio component only. For details on installing other components, see the following topics:

- *Install the API Gateway Core Server*
- *Install API Gateway Analytics*
- *Install API Gateway Explorer*
- *Install Configuration Studio*

Start Policy Studio

Important

Before starting Policy Studio, ensure that the Admin Node Manager and the API Gateway instance are running. For more details, see the section called “Start API Gateway”.

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`.

Connect to a server

When 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**.

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*.

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 the section called “Prerequisites” are met.

Install API Gateway Explorer

To install API Gateway Explorer in GUI mode, perform an installation following the steps described in the section called “GUI installation”, 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 the section called “Unattended installation”.

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

Windows

```
OAG-11.1.2.3.0-windows-installer.exe --mode unattended
--setup_type advanced
--enable-components apitester
--disable-components analytics,nodemanager,apigateway,
policystudio,configurationstudio
```

Linux

```
./OAG-11.1.2.3.0-linux-installer.run --mode unattended
--setup_type advanced
--enable-components apitester
--disable-components analytics,nodemanager,apigateway,
policystudio,configurationstudio
```

Note

This topic describes how to install the API Gateway Explorer component only. For details on installing other components, see the following topics:

- *Install the API Gateway Core Server*
- *Install Policy Studio*
- *Install API Gateway Analytics*
- *Install Configuration Studio*

Start API Gateway Explorer

Important

Before starting API Gateway Explorer, ensure that the Admin Node Manager and the API Gateway instance are running. For more details, see the section called “Start API Gateway”.

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\apigatewayexplorer`).
3. Run `apigatewayexplorer`.

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 the section called “Prerequisites” are met.

Install Configuration Studio

To install Configuration Studio in GUI mode, perform an installation following the steps described in the section called “GUI installation”, using the following selections:

- Select to install the Configuration Studio component only.

To install Configuration Studio in unattended mode, follow the steps described in the section called “Unattended installation”.

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

Windows

```
OAG-11.1.2.3.0-windows-installer.exe --mode unattended
--setup_type advanced
--enable-components configurationstudio
--disable-components analytics,nodemanager,apigateway,
apitester,policystudio
```

Linux

```
./OAG-11.1.2.3.0-linux-installer.run --mode unattended
--setup_type advanced
--enable-components configurationstudio
--disable-components analytics,nodemanager,apigateway,
apitester,policystudio
```

Note

This topic describes how to install the Configuration Studio component only. For details on installing other components, see the following topics:

- *Install the API Gateway Core Server*
- *Install Policy Studio*
- *Install API Gateway Analytics*
- *Install API Gateway Explorer*

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.*

Upgrade from version 11.1.2.x

Upgrade from 11.1.2.x overview

This topic describes how to upgrade your existing 11.1.2.x installation and migrate your data to API Gateway version 11.1.2.3.0. API Gateway 11.1.2.3.0 provides a `sysupgrade` script to export your data from an existing installation, upgrade it, and import it into a new API Gateway 11.1.2.3.0 installation.

The `sysupgrade` script enables you to upgrade the following from version 11.1.2.x to version 11.1.2.3.0:

- 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 registry – The client 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 (`admin/changeme`).
- 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.

Tip

To upgrade from a version of API Gateway earlier than 11.1.2.x, see the *Upgrade from version 11.1.1.x* topic.

Upgrade from 11.1.2.x summary

The steps involved in an upgrade are summarized as follows:

1. Backup the old installation and databases on all nodes.

   Note

   Do not shut down the old installation.

2. Install API Gateway 11.1.2.3.0 (new installation) on each node.

   Note

   Do not create or start any groups, Node Managers, or API Gateways.

3. Set up the upgrade tools on the old installation on all nodes.
4. Export the data from the old installation on all nodes.

Tip

The exported data can also be used for backup.

5. Copy the exported data from the old installation to the new installation on each node, and then upgrade the data on each node of the new installation.
6. Apply the upgrade to the new installation on all nodes.

Note

Shut down any Node Managers or API Gateways on the old installation before applying the upgrade.

Upgrade API Gateway from 11.1.2.x to 11.1.2.3.0

This section describes the steps involved in an upgrade from version 11.1.2.x (old installation) to version 11.1.2.3.0 (new installation).

Backup old installation

Backup the old 11.1.2.x installation on all nodes, including any databases. For more information on backing up the system, see the *API Gateway Administrator Guide*.

Install API Gateway 11.1.2.3.0

Install API Gateway 11.1.2.3.0 in a different directory to your old 11.1.2.x installation on all nodes. For example, if the old installation is installed in `OLD_INSTALL_DIR`, you should install the new installation in `NEW_INSTALL_DIR`. For more information on installation, see the *Installation* topic.

Note

- Do not overwrite the old installation.
- Do not create or start any Node Managers, groups, or API Gateways.
- Do not shut down the old system.

Copy upgrade tools to old installation

To copy the upgrade tools from the new 11.1.2.3.0 installation to the old installation, copy the `upgrade` directory from the 11.1.2.3.0 installation to the old installation.

Copy this directory from your 11.1.2.3.0 installation:

Windows

```
NEW_INSTALL_DIR\apigateway\upgrade
```

UNIX/Linux

```
NEW_INSTALL_DIR/apigateway/upgrade
```

After copying, the old installation should contain the following directory:

Windows

```
OLD_INSTALL_DIR\apigateway\upgrade
```

UNIX/Linux

```
OLD_INSTALL_DIR/apigateway/upgrade
```

Note

On API Gateway versions earlier than 11.1.2.2.1 the `apigateway` directory is named `apiserver`.

Install the exporter tool on the old installation

The exporter tool differs based on the version of your old installation. Ensure you install the correct tool for your version.

Perform these steps to install the exporter tool on your old installation:

1. If your old installation is version 11.1.2.0.x or 11.1.2.1.x, open a command prompt at the following directory in your old installation:

   Windows

   ```
   OLD_INSTALL_DIR\apigateway\upgrade\legacy\7.1x
   ```

   UNIX/Linux

   ```
   OLD_INSTALL_DIR/apigateway/upgrade/legacy/7.1x
   ```

2. If your old installation is version 11.1.2.2.x, open a command prompt at the following directory in your old installation:

   Windows

   ```
   OLD_INSTALL_DIR\apigateway\upgrade\legacy\7.2x
   ```

   UNIX/Linux

   ```
   OLD_INSTALL_DIR/apigateway/upgrade/legacy/7.2x
   ```

3. Run the `install` command.
4. Repeat on each node of the old installation.

Export data from the old installation

Note

Before you export, ensure that the Node Managers and API Gateways are running on the old installation.

Perform these steps to export the data from your old installation:

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

   Windows

```
OLD_INSTALL_DIR\apigateway\Win32\bin
```

UNIX/Linux

```
OLD_INSTALL_DIR/apigateway/posix/bin
```

2. Delete the `out` directory if it already exists.
3. Run the `sysupgrade` command to export the data.

   Windows

   ```
   sysupgrade export
   ```

   UNIX/Linux

   ```
   ./sysupgrade export
   ```

   The data is exported to the `out` directory.
4. Repeat on each node of the old installation.

Copy exported data to new installation

To copy the exported data from the old installation to the new 11.1.2.3.0 installation, copy the `out` directory from the old installation to the 11.1.2.3.0 installation.

Copy this directory from your old installation:

Windows

```
OLD_INSTALL_DIR\apigateway\Win32\bin\out
```

UNIX/Linux

```
OLD_INSTALL_DIR/apigateway/posix/bin/out
```

After copying, the new installation should contain the following directory:

Windows

```
NEW_INSTALL_DIR\apigateway\Win32\bin\out
```

UNIX/Linux

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

Upgrade the exported data

Perform these steps to upgrade the data exported from your old installation:

1. Open a command prompt at the following directory in your new 11.1.2.3.0 installation:

   Windows

   ```
   NEW_INSTALL_DIR\apigateway\Win32\bin
   ```

   UNIX/Linux

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

2. Run the `sysupgrade` command to upgrade the exported data in the `out` directory.

   Windows

   ```
   sysupgrade upgrade
   ```

   UNIX/Linux

   ```
   ./sysupgrade upgrade
   ```

   The data in the `out` directory is upgraded to version 11.1.2.3.0.
3. Repeat on each node of the new installation.

Apply the upgrade

Note

You must shut down any Node Managers or API Gateways on the old installation before applying the upgrade.

Perform these steps to apply the upgraded data to your new 11.1.2.3.0 installation:

1. Open a command prompt at the following directory in your new 11.1.2.3.0 installation:

   Windows

   ```
   NEW_INSTALL_DIR\apigateway\Win32\bin
   ```

   UNIX/Linux

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

2. Apply database upgrade step

   ### Note

   If KPS or OAuth tables in your system are backed by a database then please run this step else it can be safely skipped.

   Please ensure required database driver files are copied into:

   Windows

   ```
   NEW_INSTALL_DIR\apigateway\ext\lib
   ```

   UNIX/Linux

   ```
   NEW_INSTALL_DIR/apigateway/ext/lib
   ```

   Run the `sysupgrade` command to apply database upgrades in the `out` directory.

   Windows

```
sysupgrade applyDB
```

UNIX/Linux

```
./sysupgrade applyDB
```

The database upgrades are applied to the new 11.1.2.3.0 installation.

3. Run the `sysupgrade` command to apply the upgrades in the `out` directory.

   Windows

   ```
   sysupgrade apply
   ```

   UNIX/Linux

   ```
   ./sysupgrade apply
   ```

   The upgrades are applied to the new 11.1.2.3.0 installation.
4. Repeat on each node of the new installation.

Verify the upgrade

To verify that the upgrade was 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 User 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 Guide*.

Example upgrade scenarios

This section details some common upgrade scenarios.

Upgrade from 11.1.2.x to 11.1.2.3.0 – single node

To upgrade a single node from 11.1.2.x to 11.1.2.3.0, follow these steps:

1. Backup the 11.1.2.x installation:
   - Backup the `apigateway` or `apiserver` directory.
   - Backup any databases by creating a DMP file of the tables in use.
2. Install 11.1.2.3.0 alongside your 11.1.2.x installation. For more information, see the section called “Install API Gateway 11.1.2.3.0”.
3. Set up the upgrade tools in your 11.1.2.x installation. For more information, see the section called “Copy upgrade tools to old installation” and the section called “Install the exporter tool on the old installation”.
4. Export the data from your 11.1.2.x installation. For more information, see the section called “Export data from the old installation”.

5. Copy the data to your 11.1.2.3.0 installation and upgrade the data. For more information, see the section called “Copy exported data to new installation” and the section called “Upgrade the exported data”.
6. Apply the upgrade to your 11.1.2.3.0 installation. For more information, see the section called “Apply the upgrade”.

Upgrade from 11.1.1.x to 11.1.2.3.0 – single node

To upgrade a single node from 11.1.1.x to 11.1.2.3.0, follow the steps in the section called “Upgrade API Gateway from 11.1.1.x to 11.1.2.3.0”.

Upgrade from 11.1.2.x to 11.1.2.3.0 – production (two nodes)

For node 1, follow these steps:

1. Backup the 11.1.2.x installation:
   - Backup the `apigateway` or `apiserver` directory.
   - Backup any databases by creating a DMP file of the tables in use.
2. Install 11.1.2.3.0 alongside your 11.1.2.x installation. For more information, see the section called “Install API Gateway 11.1.2.3.0”.
3. Set up the upgrade tools in your 11.1.2.x installation. For more information, see the section called “Copy upgrade tools to old installation” and the section called “Install the exporter tool on the old installation”.
4. Export the data from your 11.1.2.x installation. For more information, see the section called “Export data from the old installation”.
5. Copy the data to your 11.1.2.3.0 installation and upgrade the data. For more information, see the section called “Copy exported data to new installation” and the section called “Upgrade the exported data”.
6. Apply the upgrade to your 11.1.2.3.0 installation. For more information, see the section called “Apply the upgrade”.

For node 2, follow the same steps as for node 1. If database upgrades were applied in node 1 at step 6 then it is not necessary to run this again on node 2. The `--host` option is necessary to connect to the Admin Node Manager. For example:

Windows

```
sysupgrade export --host=10.142.58.144 --port=8090
```

UNIX/Linux

```
./sysupgrade export --host=10.142.58.144 --port=8090
```

Upgrade from 11.1.1.x to 11.1.2.3.0 – production (two nodes)

To upgrade two nodes from 11.1.1.x to 11.1.2.3.0, follow the steps in the section called “Upgrade API Gateway from 11.1.1.x to 11.1.2.3.0” on each node.

Additional upgrade steps

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

- RBAC – Administrator users are imported into the new 11.1.2.3.0 installation. However, if you have made changes to the RBAC files in your API Gateway to modify roles and permissions, you must reapply these changes manually in the new API Gateway installation.
- Inconsistent Group – You might get a message to say that the groups are inconsistent. This is because all `.fed` files are deployed directly to each instance. It should not cause any issues. To resolve the issue of inconsistent groups, save a `.fed` file of the group and redeploy to the group.
- 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.

Troubleshoot the upgrade

This section provides some advice on troubleshooting the upgrade process.

ext/lib customizations

If you have customizations in your `ext/lib` directory they might cause problems in the new 11.1.2.3.0 installation. Customizations might need to be reapplied against the latest installation.

Running a single component

As each component completes, it marks the component as done by creating a `done` file in the component's directory. To run a single component again, you must first delete the `done` file and then run the `sysupgrade` command with the `--component` option, for example:

```
sysupgrade upgrade --component=db
```

Note

Running a single component is not supported for the Apply process

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
```

Trace files are located in the following directories:

```
INSTALL_DIR/posix/bin/out/export/sysexport.trc
```

```
INSTALL_DIR/posix/bin/out/upgrade/sysupgrade.trc
```

```
INSTALL_DIR/posix/bin/out/applydb/sysapplydb.trc
```

```
INSTALL_DIR/posix/bin/out/apply/sysapply.trc
```

sysupgrade script

To perform an upgrade from version 11.1.2.x to version 11.1.2.3.0, a Python script called `sysupgrade` is provided. The `sysupgrade` script is located in the following directory:

Windows

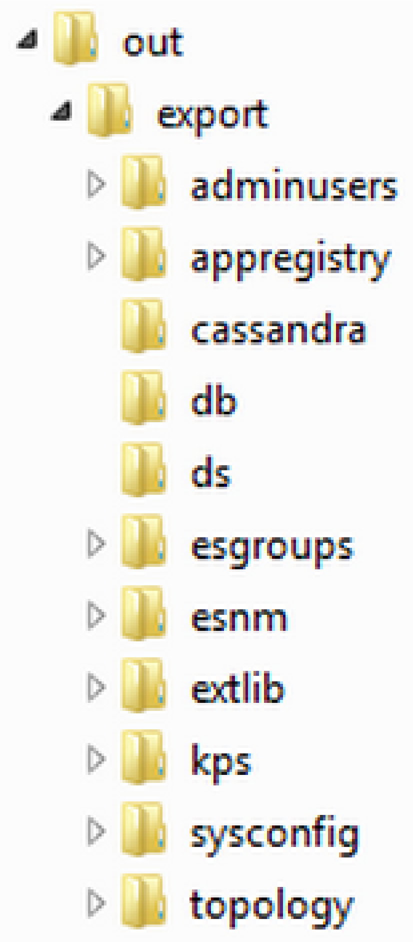
```
NEW_INSTALL_DIR\apigateway\Win32\bin
```

UNIX/Linux

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

This script is used for running all upgrade tasks. It supports four main tasks:

1. Export – Exports the data from the existing API Gateway into an `export` directory with a directory for each component's data.

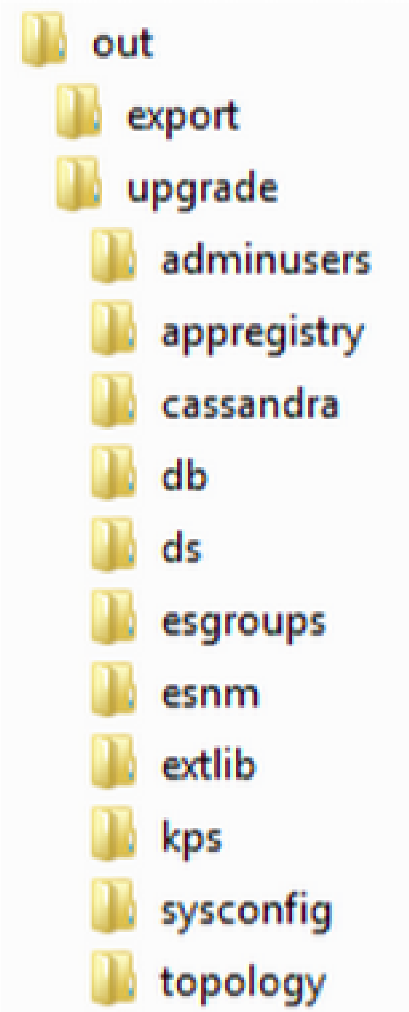
   

   ```
   out
     export
       adminusers
       appregistry
       cassandra
       db
       ds
       esgroups
       esnm
       extlib
       kps
       sysconfig
       topology
   ```

   ### Note

   Requires the old API Gateway installation to be running.

2. Upgrade – Upgrades the data in the export directory structure and creates an `upgrade` directory with the upgraded data in it.



```
out
  export
  upgrade
    adminusers
    appregistry
    cassandra
    db
    ds
    esgroups
    esnm
    extlib
    kps
    sysconfig
    topology
```

3. Apply DB – Applies any required database updates to the API Gateway 11.1.2.3.0 installation.

   Note

   If KPS or OAuth tables in your system are backed by a database this step must be run else it can be safely skipped.

4. Apply – Applies the upgraded data to the running API Gateway 11.1.2.3.0 installation.

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
System upgrade details:	

Option	Description
`--help`	Display available options and default settings.

`--component=COMPONENTS`
`-c COMPONENTS`
	Specify the components to execute the task on. The allowed values are:
	• adminusers – Administrator users
	• appregistry – Client application registry
	• db – Databases
	• ds – Directory services
	• esgroups – API Gateway instances and groups
	• esnm – Admin Node Managers
	• kps – Key property store
	• topology – Domain topology
	• cassandra – Cassandra databases
	• extlib – Contents of `ext/lib` directory
	• sysconfig – Configuration from `jvm.xml`

`--indir=INDIR`	Root directory of the API Gateway instance. Defaults to `INSTALL_DIR`.
`--outdir=OUTDIR`	Directory location in which the exported and upgraded data is stored. Defaults to `out`.
Node Manager details:	

`--scheme=SCHEME`
`-s SCHEME`
	Scheme for Node Manager (for example, `https`). The default is `https`.

`--host=HOST`	Host name for Node Manager (for example, `localhost`). The default is `localhost`.
`--port=PORT`	Port for Node Manager (for example, `8090`). The default is `8090`.
`--username=USERNAME`	User name for authenticating to the Node Manager (for example, `admin`). The default is `admin`.
`--password=PASSWORD`	Password for authenticating to the Node Manager (for example, `changeme`). The default is `changeme`.
Tracing details:	
`--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

Upgrade from version 11.1.1.x

Upgrade from 11.1.1.x overview

To upgrade from version 11.1.1.x of API Gateway to version 11.1.2.3.0 you must first upgrade to version 11.1.2.x, and then follow the procedures described in *Upgrade from version 11.1.2.x* to upgrade to version 11.1.2.3.0.

Upgrade API Gateway from 11.1.1.x to 11.1.2.3.0

To upgrade an API Gateway installation from version 11.1.1.x to 11.1.2.3.0, follow these steps:

1. Install API Gateway version 11.1.2.2.1 alongside your existing 11.1.1.x installation. Follow the instructions in the version 11.1.2.2.1 *API Gateway Installation and Configuration Guide*.
2. Create a managed domain for your deployment topology using the `managedomain` script. For more details on running `managedomain`, see the *API Gateway Administrator Guide*.
3. Upgrade your configuration to version 11.1.2.2.1 using the `upgradeconfig` script. Follow the instructions in the version 11.1.2.2.1 *API Gateway Installation and Configuration Guide*.
4. Install API Gateway version 11.1.2.3.0 alongside the 11.1.2.2.1 installation. Follow the instructions in the *Installation* topic.
5. Upgrade your version 11.1.2.2.1 installation to version 11.1.2.3.0 following the instructions in the *Upgrade from version 11.1.2.x* topic.

Additional upgrade steps

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.
- 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.
- RBAC – 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 using the `pdMigrate.py` script.

For more information on these steps, see the version 11.1.2.2.1 *API Gateway Installation and Configuration Guide*.

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.

iconmonstr:
This product includes graphic icons developed by iconmonstr [http://iconmonstr.com/].