webMethods API Portal Provider's Guide

Version 10.3

October 2018

WEBMETHODS

This document applies to webMethods API Portal Version 10.3 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: YAP-PG-103-20181015

Table of Contents

About this Guide

This guide describes how you can use webMethods API Portal and other webMethods components to effectively manage APIs for services that you want to expose to consumers, within your organization or outside to partners and third parties. In addition to describing the API management components and workflow, the guide explains configuring API Portal for use with CentraSite, webMethods Mediator, and API Gateway and how to manage API Portal and its users, and how to manage APIs published to API Portal.

To use this guide effectively, you should have an understanding of the APIs that you want to expose to the developer community and the access privileges you want to impose on those APIs.

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
Narrowfont	Identifies service names and locations in the format *folder.subfolder.service* , APIs, Java classes, methods, properties.
Italic	Identifies: Variables for which you must supply values specific to your own situation or environment. New terms the first time they occur in the text. References to other documentation sources.
`Monospace font`	Identifies: Text you must type in. Messages displayed by the system. Program code.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.

Convention	Description
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information and Support

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at "http://documentation.softwareag.com". The site requires credentials for Software AG's Product Support site Empower. If you do not have Empower credentials, you must use the TECHcommunity website.

Software AG Empower Product Support Website

If you do not yet have an account for Empower, send an email to "empower@softwareag.com" with your name, company, and company email address and request an account.

Once you have an account, you can open Support Incidents online via the eService section of Empower at "https://empower.softwareag.com/".

You can find product information on the Software AG Empower Product Support website at "https://empower.softwareag.com".

To submit feature/enhancement requests, get information about product availability, and download products, go to "Products".

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the "Knowledge Center".

If you have any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory at "https://empower.softwareag.com/public_directory.asp" and give us a call.

Software AG TECHcommunity

You can find documentation and other technical information on the Software AG TECHcommunity website at "http://techcommunity.softwareag.com". You can:

- Access product documentation, if you have TECHcommunity credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.

- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

Data Protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

1 General

Logging onto API Portal through the User Interface in a Browser

To open the API Portal user interface, open your browser and point it to the port on the host machine where the API Portal instance is running. By default, API Portal runs on port 18101.

All API Portal components must be started to open the API Portal user interface. If any of the components are not started, the browser displays an error. For example:

```
403 Forbidden You don't have permission to access / on this server.
```

To open the API Portal user interface

1. Start your browser, and then point it to the host and port where API Portal is running. For example:
   - If API Portal is running on the default port on the same machine where you are running the API Portal components, you would enter:

     ```
     http://localhost:18101
     ```
   - If the API Portal components are running on port 4040 on a machine called QUICKSILVER, you would enter:

     ```
     http://QUICKSILVER:4040
     ```
2. In the API Portal login screen, log on with your user name and password.

Logging onto API Portal Using a One-time Password

A user must provide an OTP along with the username and password to log onto API Portal. This option is available when multi-factor authentication is enabled in API Portal.

To log onto API Portal using an OTP

1. Open API Portal UI in a browser.
2. Provide user credentials.
3. Click **Login**.

   There is prompt asking you to provide an OTP.
4. You can do one of the following:
   - Click **Send OTP**.

     An OTP is sent to your registered email address.
   - If you are a registered user in API Portal you receive a secret token in an email upon on-boarding. Use this secret token to generate an OTP using an external

client. For details on generating an OTP using an external client, see "Generating an OTP Using the Secret Token" on page 15.

> **Note:** If you wish to change the secret token, you can do so in the User profile page in API Portal. For details on generating a secret token see. "Generating a Secret Token" on page 15

5. Type the OTP.
6. Click **Login**.

   You are now logged onto API Portal.

Changing the Password

Change your password in the user profile section after your first login or after a password reset by the administrator.

To change the password

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **<user name>**. Your profile is displayed.
3. Click **Change password**.
4. In the Change Password section, type the current password.
5. Type a new password.
6. Re-type the new password to confirm.
7. Click **Save Changes**.

The password is changed. The user receives a notification by e-mail.

Editing your Profile

You can modify your profile account settings in the My Profile section.

To edit your profile

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **<user name>**. Your profile is displayed.
3. Click the section you want to edit, for example **Account settings**.
4. Change the setting.
5. Click **Save Changes**.

You changed your profile data.

Configuring Display Settings

Change the display settings to view the display in a language of your choice.

To configure display settings

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **<user name>**. Your profile is displayed.
3. Click **Display settings**.
4. In the Display settings section, select a required language for display from the drop-down list for **Language**.

   The available languages are: **German (Germany)**, **English (United States)**, **Spanish (Spain)**, **French (France)**, **Italian (Italy)**, **Japanese**, **Dutch (Netherlands)**, **Polish**, **Portuguese (Portugal)**, **Russian (Russia)**, **Arabic (U.A.E)**.
5. Click **Save Changes**.

Scheduling Reports for Application Usage

You can schedule reports that provide periodic alerts on the usage of applications you own. The application usage metrics are collected and mailed to the configured email address.

To schedule reports

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **user name**.

   This displays your profile.
3. Click **Reports**.
4. In the Reports settings section, select a value for the frequency at which the report is generated and sent to the configured email. Select one of the following:
   - **Daily**: Specifies that the reports are generated daily and provides the usage of applications on daily basis. Reports are scheduled @12 PM every day.
   - **Weekly**: Specifies that the reports are generated every week and provides the usage of applications for the last seven days. Reports are scheduled @12 PM every Friday.

- **Monthly**: Specifies that the reports are generated every month and provides the usage of applications for a month. Reports are scheduled @12 PM on the first day of the month.

5. Click **Save Changes**.

   The reports are now scheduled and emailed to the configured email as per the frequency set. The report sent out has two sections.

   - **Summary**: Consists a summary in the form of a list of applications that the user owns and corresponding usage metric.
   - **Details**: Consists detailed information for each application, the API associated with the application, Resources used, and usage count.

Generating a Secret Token

You can generate a secret token from the user profile page.

Note:

- This option is available only if multi-factor authentication is enabled for API Portal.
- This option is not available for users registered in API Portal with social login.

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **<user name>**. Your profile is displayed.
3. Click **Generate secret token**.

   A secret token is sent to the registered email address. Using the secret token you can generate an OTP using an external client, such as Google Authenticator.

Generating an OTP Using the Secret Token

When multi-factor authentication is enabled, any user when on-boarded onto API Portal receives a secret token through an email. You can also generate a new secret token from the user profile settings page in API Portal.

You can use the secret token to generate an OTP using an external client. This procedure explains generating an OTP using the Google Authenticator.

To generate an OTP using the Google Authenticator

1. Start Google Authenticator.
2. Click the Pencil icon, in the top right corner.
3. Click **Add**.

4. Provide an account name in the Account name field.
5. Provide the secret token in the Secret key field.
6. Click **Add**.

   The one-time password is displayed. You can use this OTP to log onto API Portal.

Forwarding a Page of the Online Help

You can forward a link to the current page of the online help to others.

Prerequisite

The person you are sending the link to should have an access to the server on which the online help is located.

To forward a page of the online help

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click  . API Portal online help appears.
3. Open the required page of the online help.
4. Click  .
5. Type the email address of the recipient in the **To** field of email window that appears.

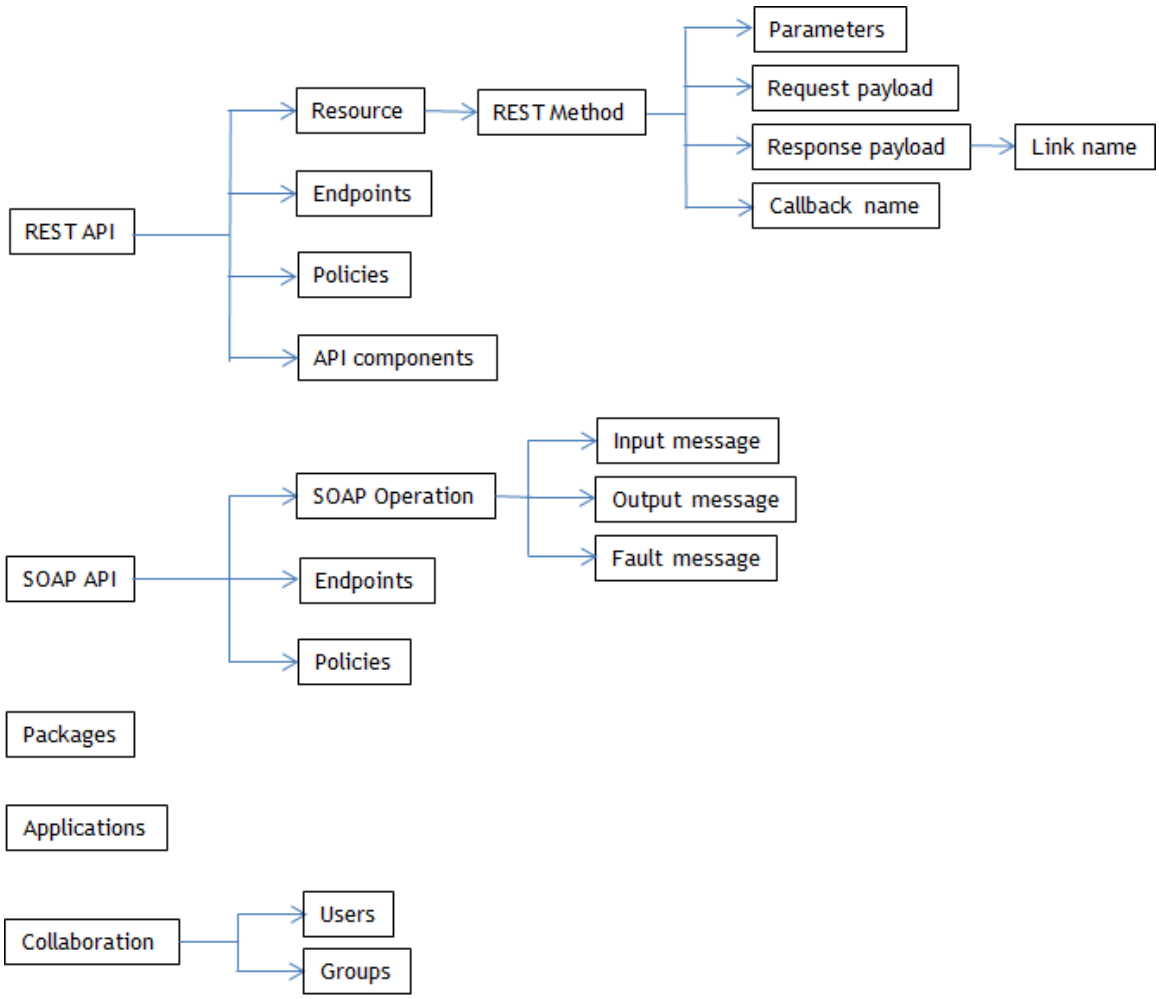
   Note: If the email window does not appear, check your browser settings and the settings of your local computer. You can also try a different browser, or copy the link from the browser's address bar and send it using the email program.

6. Click **Send**.

Searching in API Portal

The search feature in API Portal is a type-ahead search; a simple and easy to use search facility where you can type the text of interest to search. You can search for all items that contain one or more specified keywords (that is, text strings) in the item's properties. Some of the properties are name, description, version, key, value, tags, and so on.

This figure depicts the various items searchable in API Portal and the table lists the attributes that are searchable for each item type.



This table lists the attributes that are searchable for API-specific data:

Item	Attributes
REST API	■ Name ■ Short description ■ Description ■ Version ■ API group ■ Tags ■ Business term ■ Maturity state ■ Other attributes

Item	Attributes
	■ API component name
SOAP API	■ Name ■ Short description ■ Description ■ Version ■ API group ■ Tags ■ Business term ■ Maturity state ■ Other attributes
OData API	■ Name ■ Short description ■ Description ■ Version ■ API group ■ Tags ■ Business term ■ Maturity state
REST Resource	■ Name ■ Path ■ Description ■ Tags ■ Callback name
REST Method	■ Name ■ Description ■ HTTP Method ■ Tags

Item	Attributes
Parameter	■ Name ■ Description
Request payload	■ Schema ■ Sample request
Response payload	■ Schema ■ Sample response ■ Link name
SOAP Operation	■ Name ■ Description ■ Tags
SOAP message	■ Input message ■ Output message ■ Fault message
Endpoints	■ Base URL
Policies	■ Name ■ Description
Package	■ Name ■ Description
Applications	■ Name ■ Description
Entity	■ Name ■ Type ■ Container ■ Entity sets
Complex types	■ Name

Item	Attributes
	■ Type
Functions	■ Name
Actions	■ Name
Singleton	■ Name ■ Type
Properties	■ Name ■ Type

This table lists the attributes that are searchable for Collaboration data:

Item	Attribute
Users	■ First name ■ Last name ■ User name
Groups	■ Name ■ Description

To search for an object, type a string in the search box in the title navigation bar. A list of search result is displayed directly below the Search box. The number of matches found are displayed in two sections, APIs and Collaboration. A minimum of five search results are displayed in each category. The total number of matches across categories is listed at the bottom of the search box. If there are no results as per the search string typed, a message displays saying so.

If you find what you are searching for in the search result box, click on it to view the details. You are navigated to the specific page that displays more information. For example, if you are searching for a parameter in a REST method and click the displayed result, you are navigated to the parameters section in the corresponding API details page.

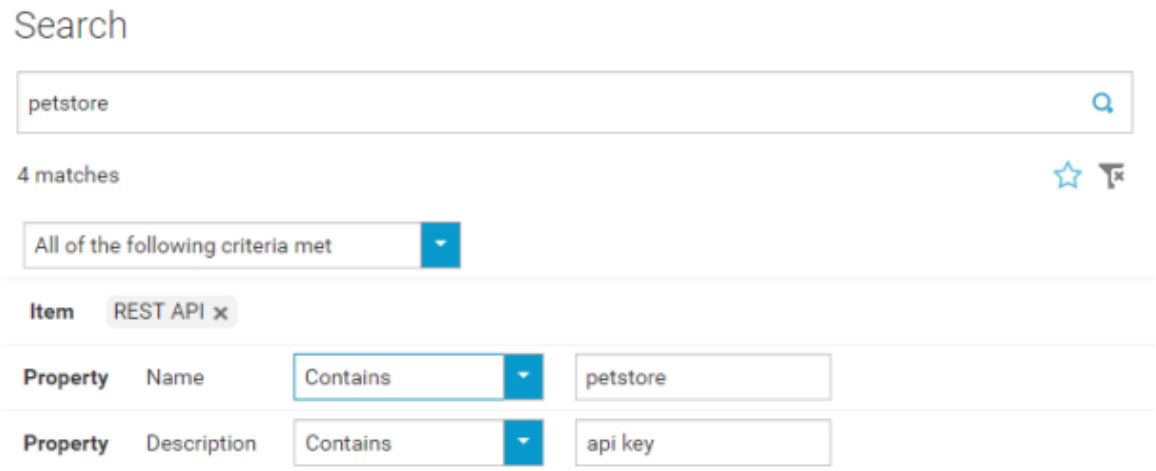
If you want to see all the search results click **Show all** in the search result box. The Advanced search page is displayed. This is a dedicated page that displays extensive search results. The search results are categorised in two tabs, APIs and Collaboration. You can select the respective tab to see search results pertaining to the category. A search

box is available in the Advanced search page; you can search for a particular string by typing the string in the search box and only results that contain the string are displayed.

You can filter the search results in the two tabs as follows:

- **APIs tab**: You can filter based on item types and include a subordinate filter of properties for each item type.

  For example, type a search string `swagger` in the search box on the title navigation bar. Click **Show all** to view all the search results that match the search string. This displays all the results in the advanced search page categorized under APIs and Collaboration tabs. In the APIs tab, you can now use a filter **REST API** in the list of filters for items; this filters the list to display only entries that have the specified item. You can further filter the list depending on the properties for the selected item; for example, select the properties **Name** and **Description**. You can provide one of the filtering criteria, **All of the following criteria met** or **One of the following criteria met**. Provide additional details for a string in the specified properties; **Name contains**`petstore` and **Description contains**`api key`. The figure displays the search criteria applied in this example.

  The search result list now displays only the search result items that are specified as per the filter.

- **Collaboration tab**: You can filter based on Users and Groups. For example, if you select the search result that describes the search item to be found for a User, it navigates to that particular user's page to display the occurrence.

You can clear the filters in each of the tabs by clicking and add new filters by clicking the required item or property.

You can save the filters as favourites by clicking and delete the saved favourites by clicking .

Note: When a backup taken from previous versions is restored in 10.1, the applications and its related properties are displayed as (Untitled). This is resolved by republishing the corresponding APIs to API Portal.

2 Managing API Providers

Manage API Providers

An API Provider has the privileges to enable an API Portal Administrator or Provider to manage APIs, and configure notification types that are used for API-related events. Notification configuration is required to notify the API Provider regarding any event for an associated API, like a token request. API Portal supports two types of notifications:

- **Email**. Email alias of a user group in UMC.
- **HTTP Callback**. The URL to which the notification event data is sent. The format of data is available in the API Portal Configurations page.

There are two types of API providers in API Portal:

- **Default Provider**. Any API that is imported and not associated with any other API provider is automatically associated with the Default Provider. When an imported API is associated with a new API provider, it gets disassociated from the Default Provider. The Default Provider has only the e-mail notification configured. By default, you will find the Default Provider in the Manage Providers page.

  Only the details in the email alias group is editable.
- **External Provider**. Any other provider falls under this category.

  Except CentraSite and API Gateway, the details of all other external providers are editable.

The details you can view and the actions you can perform in this page are listed in the following table:

Field	Description
Name	Name of the API Provider.
Description	Description of the API Provider.
APIs	The number of APIs associated with the API Provider. Hovering over the number displays the APIs that are associated.
Action	Actions that can be performed on the API Provider like Edit and Delete.
Create	Click to create an API Provider.

Creating an API Provider

You must have the privileges of an API Portal Administrator or an API Provider to create API Providers.

To create an API Provider

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **API provider**.
3. Click **Create** in the Manage API Providers page.
4. Type a name for the API Provider in the **Name** field.
5. Type a description for the API Provider in the **Description** field.
6. To associate APIs with the API Provider, click  and select the required APIs from the list.

   Only the APIs that are associated with the Default Provider are listed here.
7. To send an email notification select the email alias of the recipients group from the drop down. This is a user group in UMC.
8. To configure an HTTP callback notification, provide the required URL in the format `http://<host>:<port>/callbackurl`. This URL should accept HTTP POST call.

   a. If the HTTP callback is password protected, provide the **Username** and **Password**.
9. Click **Create**.

   The API Provider is created and listed in the Manage API Providers page.

Deleting an API Provider

You must have the privileges of an API Portal Administrator or an API Provider to delete API Providers.

You cannot delete providers created from CentraSite, API Gateway, and default API Provider in the system.

To delete an API Provider

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **API provider**.
3. Click  for the selected API Provider.
4. Click **Yes** in the confirmation dialog.

5. In the confirmation dialog box, select the option to delete the APIs along with the API provider.

   If you do not select the option only the API provider gets deleted and the APIs associated with this Provider get associated with the Default Provider.

6. Click **Yes**.

Modifying Details of an API Provider

You must have the privileges of an API Portal Administrator or an API Provider to modify the details of API Providers.

You can not modify the details of providers created from CentraSite, API Gateway. For the Default Provider you can update only the email notification group.

To modify details of an API Provider

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **API provider**.
3. Click the  for the API provider whose details are to be modified.
4. Modify the required details like name, description, associated APIs, and the notifications configured.
5. Click **Apply**.

   The API Provider is updated with the modified information and listed in the Manage API Providers page.

3 Managing APIs

Manage APIs

You can manage APIs from the Manage APIs page. The page lists all the APIs and their description. You can edit an API, delete an API, and import an API from this view.

Field	Description
Name	The name of the API.
Description	The description about the API.
Version	The version number of the API.
Operations	Operations performed on the API. Available options are: ■ Delete ■ Edit

Importing an API Directly through the API Portal User Interface

API Portal offers direct API importing facility for standalone scenarios when you do not have CentraSite or Mediator installed.

You can edit or delete the directly imported APIs as required. The supported API formats are **RAML**, **Swagger**, and **WSDL**.

You should have the API Provider or API Portal Administrator privileges to directly import an API. You can import the API in one of the following ways:

- "Importing an API by Uploading an API" on page 28
- "Importing an API by Providing an API URL" on page 30
- "Importing an API by Copying and Pasting API Content" on page 31

Importing an API by Uploading an API

API Portal offers direct API importing facility for standalone scenarios when you do not have CentraSite or Mediator installed.

Prerequisite

You must have the **API Provider** or **API Administrator** role.

To import an API by uploading an API

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Manage APIs**. The **Manage APIs** page that lists all the APIs is displayed.
3. Click **Import API**.
4. Click **Upload API**.
5. Click **Browse**.
6. Select the required file and click **Open**.

   The Swagger parser is a self-contained file with no external references and can be uploaded as is.

   If the RAML file, that is to be imported, contains external references, the entire set of files must be uploaded as a zip file with a structure as referenced by the RAML file.

   For WSDL, if it is a single .wsdl file, it can be uploaded as it is. If the wsdl file contains reference schema, the entire set of files must be uploaded as a zip file with a structure as referenced by the WSDL file. If there are multiple .wsdl files in the zip file, then you have to provide the root file name.
7. Select the type.

   The available types are **OpenAPI**, **RAML**, **WSDL**, or user-defined. By default, the options available are **RAML**, **OpenAPI**, and **WSDL**.
8. Type the API name you want the API to be displayed as.

   If you provide an API name, this overwrites the API name mentioned in the uploaded file and imported API is displayed with the name provided.

   If you do not provide an API name, the API name mentioned in the uploaded file is picked up and the API is displayed with that name.

   If you do not provide an API name and the uploaded file does not have an API name mentioned then the API is displayed as **Untitled**.
9. Select the API Provider.

   The imported API is associated with the API Provider selected. If a provider is not selected, by default the API is associated with the Default Provider.
10. Click **Import API**.
11. Click **Close**.

The imported API is now listed in the list of APIs.

You can use the **Delete** option to delete an API and the **Edit** option to update the API. The **Edit** option is available only for the directly imported APIs.

Importing an API by Providing an API URL

API Portal offers direct API importing facility for standalone scenarios when you do not have CentraSite or Mediator installed.

Prerequisite

You must have the **API Provider** or **API Administrator** role.

To import an API by providing an API URL

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Manage APIs**. The **Manage APIs** page that lists all the APIs is displayed.
3. Click **Import API**.
4. Click **API URL**.
5. Type the required URL.
6. Select the type.

   The available types are **OpenAPI**, **RAML**, **WSDL**, or user-defined. By default the options available are **RAML**, **OpenAPI**, and **WSDL**.
7. Type the API name you want the API to be displayed as.

   If you provide an API name, this overwrites the API name mentioned in the uploaded file and imported API is displayed with the name provided.

   If you do not provide an API name, the API name mentioned in the uploaded file is picked up and the API is displayed with that name.

   If you do not provide an API name and the uploaded file does not have an API name mentioned then the API is displayed as **Untitled**.
8. Select the API Provider.

   The imported API is associated with the API Provider selected. If a provider is not selected, by default the API is associated with the Default Provider.
9. Click **Import API**.
10. Click **Close**.

The imported API is now listed in the list of APIs.

You can use the **Delete** option to delete an API and the **Edit** option to update the API. The **Edit** option is available only for the directly imported APIs.

Importing an API by Copying and Pasting API Content

API Portal offers direct API importing facility for standalone scenarios when you do not have CentraSite or Mediator installed.

Prerequisite

You must have the **API Provider** or **API Administrator** role.

To import an API by copying and pasting API content

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Manage APIs**. The **Manage APIs** window that lists all the APIs is displayed.
3. Click **Import API**.
4. Click **API editor**.
5. Paste the required parser content in the text box.

   The content should not have any references to an external file.
6. Select the type.

   The available types are **OpenAPI**, **RAML**, **WSDL**, or user-defined. By default, the options available are **RAML**, **OpenAPI**, and **WSDL**.
7. Type the API name you want the API to be displayed as.

   If you provide an API name, this overwrites the API name mentioned in the uploaded file and imported API is displayed with the name provided.

   If you do not provide an API name, the API name mentioned in the uploaded file is picked up and the API is displayed with that name.

   If you do not provide an API name and the uploaded file does not have an API name mentioned then the API is displayed as untitled.
8. Select an API Provider.

   The imported API is associated with the API Provider selected. If a provider is not selected, by default the API is associated with the Default Provider.
9. Click **Import API**.
10. Click **Close**.

The imported API is now listed in the list of APIs.

You can use the **Delete** option to delete an API and the **Edit** option to update the API. The **Edit** option is available only for the directly imported APIs.

Deleting an API

You must have the **API Provider** or **API Administrator** role.

To delete an API

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Manage APIs**.

   The Manage APIs page that lists all the APIs is displayed.
3. Click  for the API you want to delete.

You deleted an API.

Updating an API

The **Update** option is available only for the directly imported APIs.

Prerequisite

You must have the **API Provider** or **API Administrator** role.

To update an API

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Manage APIs**. The **Manage APIs** window that lists all the APIs is displayed.
3. Click  for the API you want to update.
4. Update the API by uploading a new file or by providing a new URL or pasting new content.
5. Click **Update**.

   The API with the updated information is now available in the Manage APIs list.

API Versions

API Portal supports versioned APIs that are published from API Gateway and CentraSite. You can also create a new version of an API when you update an API in API Portal.

When you create a new version of an API and publish it to API Portal, the API Gallery page displays the latest version of the API with the indication that it is versioned. The Manage APIs page displays all the API versions. The API details page has a drop down

list that displays all the API versions present along with the maturity status of the API, if any. Selecting a version from the list displays the API details of that version.

If you have multiple versions of an API, the access token request is enabled only for the latest version. Access tokens of an earlier version can be used to test newer versions of the API.

Different versions of an API can be added to different communities and can be associated with different packages.

Creating a New API Version

You can create a new version of an API using the **Edit** option. This option is available only for the directly imported APIs.

Prerequisite

You must have the **API Provider** or **API Administrator** role.

To create a new API version

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Manage APIs**. The **Manage APIs** window that lists all the APIs is displayed.
3. Click  for the API you want to edit.
4. Update the API by uploading a new file or by providing a new URL or pasting new content.
5. Select **Create as new version**.
6. Click **Update**.

   The new version of the API created is now available in the API Gallery and the Manage APIs list.

4 Using and Testing APIs

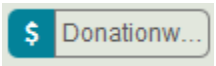
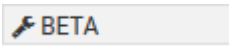
API Gallery

The API Gallery lists all the APIs that are present. If an API has multiple versions only the latest version is displayed. You can view the details of individual API or group the APIs as required.

The APIs listed in the API gallery are one of the following type:

- REST API
- SOAP API
- OData API (API Portal supports Version 2 and Version 4 of OData API.)
- Hybrid API (This is a REST API with the SOAP metadata displayed.)

In the API gallery view you can perform the following operations listed in the table.

Action	Description
	Group APIs as required. You can group them with the following options available: ■ **API group** ■ **Business term** ■ **Maturity status** The APIs that do not belong to the group specified are listed as Ungrouped.
	Displays the details of the selected API. The details such as API description, API Resources, API documents, Access API, API Version, and Latest posts are displayed.
	Indicates that the API is versioned and different versions of the API are available.
	Indicates the business term of the API.
	Indicates the maturity status of the API.

Finding APIs in the API Gallery

You can search for the required APIs in the API Gallery.

To find APIs in the API Gallery

- In the navigation bar, click **API Gallery**.

All APIs are displayed. APIs are structured in categories.

Alternatively, on the **Home** page, you can type the beginning of the API name in the search box. A list of relevant APIs is displayed.

APIs in development or deprecated APIs will be displayed only to API providers or administrators. Public APIs can be viewed by guest users without login.

Viewing API Details

You can view the details of an API in the API details page.

To view API details

1. Log in to API Portal.
2. Switch to the **API Gallery** page.
3. Click **View details** for an API.

The API Details page opens. The API Details page shows different entries depending on the API type (REST, SOAP, and OData API).

API Details View

The API details view displays the details of the selected API such as API description, API Resources, API documents, Access API and Latest posts. You can also look at the discussion on the support forum regarding this API, choose to follow this API, export the API, rate the API or view the list of followers of the selected API.

If the API is a Hybrid API, by default, it is displayed as a REST API and the REST resources are displayed in the API Details view. You can view the SOAP data by clicking the SOAP option.

Field	Description
API name	Displays the API name and the tags associated with the API.
About *API name*	Displays the name and description of the API.

Field	Description
	The API name and description of the API are editable. Hovering over the API name or the API description displays the edit icon, which you can click and edit them as required.
API resources (For a REST API)	Displays a list of resources available in the API sorted by resource/pathname. For the REST APIs, the list of resources are displayed in sorted order of the path names. Click each resource to view the corresponding HTTP methods, along with a summary. For each of these methods, details such as tags, parameters and status codes, schema definition, callback URLs, sample request, and sample response with links are displayed. If a method is protected by APIKey, OAuth2 or JWT, the same is indicated by a lock symbol.
API methods (For a SOAP API)	Displays a list of methods available in the API. For the SOAP APIs, methods are displayed along with their type of binding (SOAP 11 , SOAP 12, and other HTTP methods). Click each method to view details such as input, output, fault messages, and tags. If a method is protected by APIKey, OAuth2 or JWT, the same is indicated by a lock symbol.
API components For REST APIS created with Open API specifications	Displays a list of schema available in the API. Click each schema to view more details You can click on each schema to view the schema details, such as name, description, type, example, whether it is required and array information in the Table tab and the schema format in the JSON tab
Other attributes	Displays a list of any other attributes associated with the API. For example, Contact ame, License URL, License name, Cntact email, and so on.
Entity sets (For an OData API)	An Entity Set element represents a single entity or a collection of entities of a specific entity type in the data model. Type of the entity and the container name are displayed.

Field	Description
Singletons (For an OData API)	Singletons are single entities which are accessed as children of the entity container. Type of the singleton and the container name are displayed.
Entity types (For an OData API)	Entity Types (for example, Person, Airline and so on) are structured records consisting of named and typed properties and key properties whose values (for example, UserName, AirlineCode and so on) uniquely identify one instance from another. Here the list of available entity types and the parameters are displayed.
Complex types (For an OData API)	Complex Types are structured types (for example, City, Location, Airport Location and so on) consisting of a list of properties (for example, CountryRegion, Name, Address, and so on) but with no key, and thus can only exist as a property of a containing entity or as a temporary value. List of available complex types and the parameters are displayed.
Functions (For an OData API)	The Function element represents a parameter to the function. Function renders the parameters that are accepted by the function and return type of the function.
Actions (For an OData API)	The Action element denotes if the action is bound to a specific entity type in an entity model. Displays the parameter section that is rendered in functions.
API documents	Displays the list of all documents for the API.
Access API	Displays the list of endpoints for the API.
API scopes (For a SOAP and REST API)	A scope represents a logical grouping of REST resources, methods, or both, and SOAP operations in an API. You can then enforce a specific set of policies on each individual scope in the API. Displays the scopes associated with the API and the corresponding details such as name of the scope, description of the scope and the methods included in the scope.

Field	Description
	If the scope has policies associated, the policies are displayed under a subsection Policies.
Latest posts	Opens a text editor where you can type in your comment, tag the post, attach a link or a file and post it.
Try API	Click this option to test the API. It opens the Try API page. You can provide the various parameters required for the API and test it. For a REST API, the REST resources that can be tested are displayed in the left panel. For a SOAP API, the API methods that can be tested are displayed in the left panel. For a Hybrid API, you can click the REST toggle option, in the left panel, to display the REST resources to be tested and click the SOAP toggle option to display the SOAP methods that can be tested.
Version	Displays the version of the API along with the maturity status, if any, and lists all the versions of the API from the latest to the least in the drop-down list. Selecting a version from the list displays the API details of that version.
Support forum	Clicking this option navigates you to the Collaboration > My feed view where you can view the recent posts or activity. You can also post it to your feeds.
Get access token	Clicking this option you can request an access token to access and use the API. This option is available only for the latest API version.
Follow this API	Click to follow this API. If you are already following this API you will see the option Unfollow this API, in which case you can click it to unfollow the API.
Export API as (For a REST API)	Click to export the API in the JSON or YAML format. The schemas of the API must comply with at least Draft 4 version of JSON Schema.

Field	Description
Download Client SDK (For a REST API)	Click to download the Client SDK for the API in the specified language. **Supported languages** - Akka-Scala, Android, ASP.NET5, Async-Scala, Clojure, C++Rest, C#, C#.NET2, Cwiki, Dart, Dynamic-Html, Flash, Go, Go-Server, Groovy, Haskell, HTML, HTML2, Inflector, Java, Javascript, Javascript-Closure-Angular, JAXRS, JAXRS-CXF, JAXRS-Rest, JAXRS-Spec, JMeter, Lumen, Nancyfx, Nodejs-Server, Objective C, Perl, Php, Python, Python-Flask, Qt5 C++, Rails5, Ruby, Scala, Scalatra, Silex-Php, Sinatra, Slim, Spring, Swagger, Swagger-Yaml, Swift, Tizen, Typescript-Angular, Typescript-Angular2, Typescript-Fetch, Typescript-Node. The schemas of the API must comply with at least Draft 4 version of JSON Schema. This is available only for REST APIs.
Advanced edit	Click to modify the icon representing the API, API documents and API category for the selected API.
Rate this API	Click the number of stars depending on how you want to rate this API. Rating is specific to an API version.
List of followers	Displays the number of followers who are following this API. Followers of a previous API version automatically follow any subsequent higher versions. **Note:** The list of followers is not persisted in the following cases : ■ A SOAP API republished as REST API or a Hybrid API. ■ A REST API or a Hybrid API republished as a REST API.
Associated packages	Displays the associated packages with the API.

Editing APIs

You can edit an API from the API Details page. There are two types of edits you can apply to an API:

- Basic: Involves modifying API name, API description, resource description, method description, method parameter description, and additional attributes.
- Advanced: Involves modifying the icon, supporting documents, and categories of an API.

Modifying the Basic Attributes of an API

You can modify the basic attributes of an API, in the API Details page, in the view mode as well as by clicking the **Edit** button.

To modify the basic attributes of an API

1. Log in to API Portal.
2. Click **API Gallery**.
3. Click **View details** for an API.
4. In the API Details page, you can do one of the following:
   - Hover over the basic attributes and click the edit icon that appears.
   - Click **Edit**. All the editable fields display the edit icon ; click for the required field.

     On clicking **Edit**, the **Advanced edit** option appears under the What's Next? section, which can be used to edit the advanced attributes of an API.
5. Modify the information as required.
6. click to save the changes.

   You can click to discard the changes.

Modifying the Advanced Attributes of an API

You can modify the advanced attributes of an API using the Advanced edit option.

To modify advanced attributes using Advanced edit

1. Log in to API Portal.
2. Click **API Gallery**.
3. Click **View details** for an API.

4. In the API Details page, click **Edit**.

   The **Advanced edit** option appears in the What's Next? section.

5. Click **Advanced edit**.

6. In the Advanced API editing dialog box you can modify any or all the following:

   - Click  (API icon). Click **Browse...**, select the required icon, click **Open**, and click **Save**.

     Note: Supported filed types are JPG, JPEG, GIF, SVG, and PNG and maximum image size is 1MB.

   - Click  (API documents). Click **Add**, select the required documents, and click **Open**.

     Note: Supported files types are PDF, DOC, ZIP, JPG, JPEG, DOCX, XLS, XLSX, PNG, PPT, and PPTX and maximum file size is 2 MB. The supported file type and maximum size parameters are configurable in the Configuration Settings page.

     If you want to delete the existing document you can click the delete icon for the corresponding API document listed.

   - Click  API category. Provide the **Tags**, **Business term**, **Maturity state**, and **API group** as required and click **Save**.

Markdown Support

Markdown is a lightweight language that is used to render HTML content using plain text formatting syntax.

Markdown support is available for the following attributes in API details page:

- API short description
- API long description
- Resource description
- Method short description
- Method long description
- Values in Other Attributes section

Note: Addition of authentic and valid markdown content is recommended for security reasons.

Testing a REST API

The fundamental concept in any RESTful API is the resource. A resource is an object with a type, associated data, relationships to other resources, and a set of methods that operate on it. Only a few standard methods are defined for the resource (in line with the standard HTTP GET, POST, PUT, and DELETE methods).

To test a REST API

1. Switch to the **API Gallery** page.

   Alternatively go to the **Home** page and type the beginning of the API name into the search box.

2. Click **View details** for an API.

3. Click **Try API** in the API details page.

   The resources that can be tested are displayed in the left panel.

4. Select a resource.

   The methods associated with the resource that can be tested are displayed. If a method is protected by APIKey, OAuth2 or JWT, the same is indicated by a lock symbol.

   Note: The HTTP PATCH support is available in API Portal 9.12 onwards.

5. Click a method.

6. Provide the following required values:

   - **Path parameters**: Type a value for the Path parameters.
   - **Query parameters**: Type a query parameter and its corresponding value. You can add multiple entries by clicking +.
   - **Header parameter > Headers**: Type in the required Header name and corresponding value. You can add multiple entries by clicking +.
   - **Header parameters > Security**: You can select any of the following authentication types
     - **No Auth**: Specifies that no authentication is required.
     - **Basic authentication**: Specifies basic authentication of user credentials is required. Type the username and password for authentication and click **Update**.
     - **Oauth 2.0**: Specifies OAuth authentication is required. Provide the required information to fetch a OAuth token to use for authentication. For details on how to generate a OAuth token and use it see, "OAuth 2.0 Support" on page 47.

- **JWT**: Specifies a JSON Web token is required for authentication. Type a token or select one of the available tokens in the list and click **Update**. For details on how to generate a JSON web token and use it see, "Testing a JWT protected API" on page 49.

7. Click **Test**.

The request and the response of the API are displayed.

To clear all data, click **Clear**.

Testing a SOAP API

To test a specific SOAP API proceed as follows.

To test a SOAP API

1. Log in to API Portal.
2. Switch to the **API Gallery** page.

   Alternatively go to the **Home** page and type the beginning of the API name into the search box.
3. Click **View details** for an API.
4. Click **Try API** in the API details page.

   The methods that can be tested are displayed in the left panel. If a method is protected by APIKey, OAuth2 or JWT, the same is indicated by a lock symbol.
5. Select a method.

   The methods associated with the resource with the corresponding SOAP versions that can be tested are displayed.
6. Provide the following required values:
   - **Web service security**: Type the username and password.
   - **Header parameter > Headers**: Type in the required Header name and corresponding value. You can add multiple entries by clicking +.
   - **Header parameters > Security**: You can select any of the following authentication types
     - **No Auth**: Specifies that no authentication is required.
     - **Basic authentication**: Specifies basic authentication of user credentials is required. Type the username and password for authentication and click **Update**.
     - **Oauth 2.0**: Specifies OAuth authentication is required. Provide the required information to fetch a OAuth token to use for authentication. For details

on how to generate a OAuth token and use it see, "OAuth 2.0 Support" on page 47.

- **JWT**: Specifies a JSON Web token is required for authentication. Type a token or select one of the available tokens in the list and click **Update**. For details on how to generate a JSON web token and use it see, "Testing a JWT protected API" on page 49.

- **API Method request**: Provide the required request payload. For example, it can be xml content or json content.

7. Click **Test**.

The request and the response of the API are displayed.

To clear all data, click **Clear**.

Testing an OData API

To test a specific OData API proceed as follows.

To test an OData API

1. Switch to the **API Gallery** page.

   Alternatively go to the **Home** page and type the beginning of the API name into the search box.

2. Click **View details** for an API.

3. Click **Try API** in the API details page.

   The resources that can be tested are displayed in the left panel.

4. Select a resource.

   The methods associated with the resource that can be tested are displayed. If a method is protected by APIKey, OAuth2 or JWT, the same is indicated by a lock symbol.

5. Click a method for the listed **Entity sets** in the left navigation paths and select the method for the entities listed under **Entity sets**.

6. Provide the following required values:

   - **Path parameters**: Type a value for the Path parameters. This field is applicable only for the entity methods listed under the **Entity sets**.

   - **Query parameters**: Type a query parameter and its corresponding value. You can add multiple entries by clicking +.

   - **Header parameter > Headers**: Type in the required Header name and corresponding value. You can add multiple entries by clicking +.

- **Header parameters > Security**: You can select any of the following authentication types
  - **No Auth**: Specifies that no authentication is required.
  - **Basic authentication**: Specifies basic authentication of user credentials is required. Type the username and password for authentication and click **Update**.
  - **Oauth 2.0**: Specifies OAuth authentication is required. Provide the required information to fetch a OAuth token to use for authentication. For details on how to generate a OAuth token and use it see, "OAuth 2.0 Support" on page 47.
  - **JWT**: Specifies a JSON Web token is required for authentication. Type a token or select one of the available tokens in the list and click **Update**. For details on how to generate a JSON web token and use it see, "Testing a JWT protected API" on page 49.

7. Click **Test**.

The request and the response of the API are displayed.

To clear all data, click **Clear**.

OAuth 2.0 Support

The OAuth 2.0 Authorization Framework (OAuth) facilitates the sharing of private resources (data or services) with a third-party client application (client). In an OAuth session, private resources are stored on a resource server and the owner of the resources, or resource owner, grants the client application permission to access them. In this case the resource owner is typically an application. When a resource owner grants permission, the OAuth authorization server issues an access token to the client application. When the client application passes the access token to the resource server, the resource server communicates with the authorization server to validate the token and, if valid, provides access to the resources.

Note: Extensive OAuth2 support is available from API Portal 10.1 and higher versions.

Authorization grant types supported in API Portal

The flow of authorization requests and responses between the resource owner, client application, authorization server, and resource server depends on the authorization grant type defined by the OAuth session. API Portal supports the following authorization grant types:

- Authorization code
- Implicit

- Client credentials

Note:

- For an OAuth2 protected API published from CentraSite, only Client credentials grant type is supported.
- All 3 grant types are supported only if the OAuth2 protected API is published from API Gateway 10.1 or higher versions.

Authorization Code Grant

The authorization code grant type is used to authenticate and provide access to clients that have credentials on the authorization server. This grant type requires the client to authenticate to the authorization server before obtaining an access token. The user is prompted to log on to the authorization serve and to authorize or deny the client (application) access to their account. Once authorized, the Authorization provides an authorization code. This authorization code is provided to the Access token URL, which in turn provides the required access token to access the resource.

Implicit Grant

The implicit grant flow is similar to the authorization code grant flow with a distinct difference that the Authorization server provides the access token instead of authorization code. The Client ID and Client secret is passed on to the Authorization URL, for validation. The user is prompted to log on to the authorization server and approve the client. On approval, the required access token is provided to access the resource.

Client Credentials

The simplest of all of the OAuth 2.0 grants, this grant is suitable for machine-to-machine authentication where a specific user's permission to access data is not required. The Client ID and Client secret is passed on to the Access token URL, which in turn provides the required access token to access the resource.

Testing an OAuth Protected API

When an OAuth protected API is published from API Gateway to API Portal you require an OAuth2 access token to test the API. The Authorization server can be configured to use either HTTP or HTTPS connection to authorize requests. For information on enabling HTTPS mode for Authorization server in API Gateway see, *API Gateway Administrator's Guide* and *webMethods Integration Server Administrator's Guide*.

To test an OAuth2 protected API

1. Switch to the **API Gallery** page.

   Alternatively, go to the **Home** page and type the beginning of the API name in the search box.

2. Click **View details** for an API.

   The API Details page opens.

3. Click **Get access token** if you are accessing the API for the first time, else proceed to step 6.
4. In the Request API access token dialog box, provide the **Application name** and **Application description**.

   The application is created and listed in the Applications page.
5. Click **Request token**.
6. In the API details page, click **Try API**.

   The application is listed in the Try API page.
7. Click **Get new token**.

   This option is available if the API is OAuth protected and you have requested an application to access the API.
8. In the Get OAuth token dialog box provide the following information:
   - **Token name**: Type a name for the token.
   - **Grant type**: Select the grant type to be used to authenticate the API. Available values are **Authorization code**, **Implicit**, **Client Credentials**.

   The **Authorization URL**, **Access token URL**, **Client Id**, and **Client secret** are pre-populated depending on what grant type is selected.
9. Click **Get token**.
10. In the API Gateway Resource access approval page, click **Approve**.

    This page lists all the APIs that are added as part of the application.

    A token is generated and is listed under the available token list. An Authorization header is added along with the access token value.
11. Select the access token and click **Test**.

    The response is displayed.

Testing a JWT protected API

JSON Web Token (JWT) is an open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed.

When a JWT protected API is published from API Gateway to API Portal you require a JWT access token to test the API.

To test a JWT protected API

1. Switch to the **API Gallery** page.

Alternatively, go to the **Home** page and type the beginning of the API name in the search box.

2. Click **View details** for an API.

   The API Details page opens.

3. Click **Get access token** if you are accessing the API for the first time, else proceed to step 6.

4. In the Request API access token dialog box, provide the **Application name** and **Application description**.

   The application is created and listed in the Applications page.

5. Click **Request token**.

6. In the API details page, click **Try API**.

   The application is listed in the Try API page.

7. Click **Get JSON Web token**.

   This option is available if the API is JWT protected and you have requested an application to access the API.

8. Type the API Gateway Administrator credentials in the Basic Authentication dialog box

9. Click **OK**.

   A token is generated and is listed under the available token list. An **Authorization header** is added along with the access token value.

10. Select the access token and click **Test**.

    The response is displayed

Following an API

You can follow an API on a social network.

To follow an API

1. Search for APIs or find one in the API Gallery.
2. Click the API to view the API Details page.
3. Click **Follow this API**.

   The list of followers increases by 1. The option now changes to **Unfollow this API**. You can click this to unfollow the API.

You will receive a corresponding notification for any event involving the API.

Sharing an API

You can share an API to let your contacts know about anything interesting you found about the API.

To share an API

1. Search for APIs or find one in the API Gallery.
2. Click the API to view the API Details page.
3. You can share the API in one or more of the following ways:
   - Click to share the API through facebook. This opens the browser where you have to login into your facebook account and share the API.
   - Click to share the API through Google. This opens the browser where you have to login into your Google account and share the API.
   - Click to share the API through email. This opens the compose new mail screen where you type the receivers email address and send the mail to share the API.

The API is now shared.

Downloading Client SDK for an API

You can download the Client SDK for an API in a specified language as a zip file. The zip file contains necessary code package that can be used for testing and communicating with the API. This is available for REST APIs.

To download the client SDK for an API

1. Search for APIs or find one in the API Gallery.
2. Click the API to view the API Details page.
3. Click **Download Client SDK**.
4. Select the required language.

   Supported languages - Akka-Scala, Android, ASP.NET5, Async-Scala, Clojure, C++Rest, C#, C#.NET2, Cwiki, Dart, Dynamic-Html, Flash, Go, Go-Server, Groovy, Haskell, HTML, HTML2, Inflector, Java, Javascript, Javascript-Closure-Angular, JAXRS, JAXRS-CXF, JAXRS-Rest, JAXRS-Spec, JMeter, Lumen, Nancyfx, Nodejs-Server, Objective C, Perl, Php, Python, Python-Flask, Qt5 C++, Rails5, Ruby, Scala, Scalatra, Silex-Php, Sinatra, Slim, Spring, Swagger, Swagger-Yaml, Swift, Tizen, Typescript-Angular, Typescript-Angular2, Typescript-Fetch, Typescript-Node.

5. Click **Download**.

The Client SDK is now downloaded.

5 Managing Applications

Applications

An application defines the precise identifiers by which messages from a particular consumer application is recognized at run time. The identifiers can be, for example, user name in HTTP headers, a range of IP addresses, such that API Portal can identify or authenticate the applications that are requesting an API.

The ability of API Portal to relate a message to a specific application enables it to:

- Control access to an API at run time (that is, allow only authorized applications to invoke an API).
- Monitor an API for violations of a Service-Level Agreement (SLA) for a specified application.
- Indicate the application to which a logged transaction event belongs.

Field	Description
Name	The name of the application.
Description	The description of the application.
Purpose	Specifies the purpose of the application. For example API subscription, Package subscription.

Viewing List of Applications and Application Details

You can view the list of applications in the Applications page from where you can select an application to view its details. In the Application details page you can see the list of associated APIs and renew or revoke access tokens for those APIs.

To view the application list and application details

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Manage applications**.

   A list of all registered applications is displayed.
3. Select an application.

   The application details page displays the basic information, access tokens, and APIs registered for that application.

Application Details View

The application details view displays the details of the selected application such as application description, purpose for which the application is created, access tokens, and associated APIs. You can also renew or revoke the access token for an associated API.

Field	Description
Basic information	Provides the basic information of the selected application such as description and purpose for which the application is created.
Access tokens	Provides the list of access tokens available for the associated APIs for the application. It displays the following details of the access token: ■ **API access key**: The access for using the access token for the associated API. ■ **Expiration date**: The date when the access token expires.
OAuth2 credentials	Provides the OAuth2 credential details available for the application. It displays the following details of the OAuth2 credentials: ■ **Client Id**: Specifies the client identifier issued to the client to identify itself to the authorization server. ■ **Client secret**: Specifies the client secret that is matching to the client identifier. ■ **Token life time (sec)**: Specifies the time for which the access token is available. ■ **Refresh count**: Specifies the number of times the access token can be refreshed. ■ **Authorization URLs**: Specifies the Authorization URL to which the Client ID and Client secret is passed on for validation. ■ **Access token URLs**: Specifies the Access token URL to which the Client id and Client secret is passed on to and which in turn provides the required access token to access the resource.

Field	Description
	■ **Redirect URLs**: Specifies the URIs that the authorization server uses to redirect the resource owner's browser during the grant process. You can add more than one URI at a time using the **Add** button.
JWT properties	Provides the Access token URL details used to get the access token. ■ **Access token URLs**: Specifies the Access token URL that is used, along with the App ID to get an access token from the API provider to access the resource.
Associated APIs	Lists the associated APIs for the selected application. It displays the following information for the associated APIs: ■ **API name**: Specifies the name of the API. ■ **Version**: Specifies the version of the API. ■ **Action**: Displays the following actions that can be performed for the specified API ■ **Renew**: Click to renew the access token for the required API. ■ **Revoke**: Click to revoke an access token for the required API.

Renewing Access Tokens

The renew option is available only for the APIs that are published from CentraSite with an expiry date.

To renew an access token

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Applications**.
3. Click **Renew**, in the Associated APIs section, for the required API.

   The access token is renewed for the specified time.

Revoking Access Tokens

To revoke an access token

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Applications**.
3. Click **Revoke**, in the Associated APIs section, for the required API.

   The access token is revoked and the application is removed from the applications list page, if there is only one API associated to the application.

6 Managing API Packages and Plans

API Packages and Plans

API Package refers to a logical grouping of multiple APIs from a single API provider. A package can contain one or more APIs and an API can belong to more than one package. You should have the API Administrator or Provider privileges to manage an API Package. As a consumer you can only view the API package details. Once a package is deprecated, it will no longer be visible to an API Consumer.

An API Plan is the contract proposal presented to consumers who are about to subscribe APIs. Plans are offered as tiered offerings with varying availability guarantees, SLAs or cost structures associated to it. An API Package can be associated with multiple plans at a time. This helps the API Providers in providing tiered access to their APIs to allow for different service levels and pricing plans. Though you can edit or delete a plan that has subscribers Software AG recommends you not to do so.

Viewing API Packages and Associated Plans

You can view the API Packages and the associated plans in the Packages page.

To view API Packages

1. Log in to API Portal.
2. Click **API Packages** in the title bar.

   A list of API packages is displayed. Additional information on the number of APIs and Plans associated with the package are also present.
3. Click **View details** for an API Package.

   A list of APIs and Plans associated with the API Package are displayed. You can click an API to view details of the associated API. Click **Subscribe** to subscribe a Plan. This opens Request Access Token dialog where you can request for one and subscribe to the plan.

API Package details

You can view the associated APIs and Plans from the Package details page. You can view details of a Package, details of the API, and subscribe for a plan from the API Package details view.

Field	Description
About	A brief description of the API Package

Field	Description
APIs	A list of APIs associated with the API Package. Click on individual APIs to view details of the API.
Plans	List of Plans associated with the API Package. Click **Subscribe** to request access token and subscribe to the particular Plan.

7 Managing Apps

App Gallery

The App gallery in API Portal acts as a market place in which API Portal users post their solution built on top of APIs published in the Portal; the market place can be used for establishing ecosystems for engaging partners and customers. Users who create these solutions can document them by providing descriptions and linking to other documents, features and screen shots of the app, and provide a link to external sources such as Apple Store or Google Play store. Other users can access the solutions available in the market place and download any assets posted in them.

The App gallery lists all the Apps that are present. Click an App to view its details.

App Details View

The App details view displays the details of the selected App such as App description, App features, and additional information about the App. You can also look at the discussion on the support forum regarding this App, choose to follow this App, rate the App or view the list of followers of the selected App.

Field	Description
Features	Displays a list of features available in this app. The features are categorised as the basic features and the advanced features that can be availed with an upgrade of the app.
Additional information	Displays additional information about the app as to when it was created, when it was last updated, the version of the app and the organization it belongs to.
Developed using	Lists the APIs that were used to build this app. Click on an API in the list to view the API details.
Screenshots	Displays the screen shots of the App.
Comments	Displays the comments that were added by the users. The comment text box allows a user to include a comment for the App. You can attach a tag, link or a file as part of the comment. In addition you can bookmark a comment, edit it, tag it, flag it, or delete it.

Field	Description
Developed by	Displays the names of the developers who developed the app.
Support forum	Click this option to navigate you to the Collaboration > My feed view where you can view the recent posts or activity. You can also post it to your feeds.
Follow this App	Click to follow this App. If you are already following this App you see the option Unfollow this App, in which case you can click it to unfollow the App.
List of followers	Displays the number of followers who are following this App.
Rate this App	Click the number of stars depending on how you want to rate this App.

Manage Apps

You can manage Apps from the Manage apps page. The page lists all the Apps and their description. You can edit an App, or delete an App from this view.

Field	Description
Name	The name of the App.
Description	The description about the App.
Version	The version number of the App.
Actions	Actions that can be performed on the App. Available options are: ■ Delete ■ Edit . This option is available only if you are the creator of the app.

Creating an App

You must have the privileges of an API Portal Administrator, an API Provider or a Consumer to create Apps.

To create an App

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Manage apps**.
3. Click **Create** in the Manage apps page.
4. In the Overview section, provide the following information:
   a. In the **Name** field, provide a name for the app to identify it.
   b. In the **Description** field, provide a short description about the app.
   c. In the **Features** field, elaborate the features of the app.
   d. In the **Icon** field, attach a image that is displayed as an icon for the app in the app gallery. Click Browse through the available icons and upload it.

      Note: The format and size is as mentioned in the configuration settings page.

   e. In the **Version** field, provide a version for the app. If no version is mentioned, it automatically gives the version number 1.0.
   f. In the **Company** field, provide the name of the company developing the app.
   g. In the **Tags** field, provide tags for the app.

      Tags are used as keywords to denote the app, such as an app predicting the weather could have tags like weather, and so on.
5. In the APIs section, perform the following to associate APIs to the app:
   a. Click **+ Add**.
   b. Select the required APIs
   c. Click **OK**.

      The selected APIs are displayed as a list. If you want to remove the APIs, click **Unlink** for the corresponding API and it gets deleted from the App.
6. In the Screenshot section, do the following:
   a. Click **+ Add**.
   b. Select the required image.
   c. Click **Open**.

The screenshot is uploaded and is listed. The format and size is as mentioned in the configuration settings page.

7. In the Platforms section, type the URL to your App available in the respective platforms.

   The URL provided is that of your app in the App Store, like https://play.google.com/store/apps/details?id=com.whatsapp&hl=en

8. Click **Save**.

   The App is created and listed in the Manage apps page.

Deleting an App

You must have the privileges of an API Portal Administrator or you must be the creator of the App to delete an App.

To delete an App

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Manage apps**.
3. Click  corresponding to the App that is to be deleted.
4. Click **Yes** in the confirmation dialog.

Modifying Details of an App

You must be the creator of the App to modify its details.

To modify details of an App

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Manage apps**.
3. Click the  corresponding to the App whose details are to be modified.
4. Modify the required details.
5. Click **Save**.

   The App is updated with the modified information and listed in the Manage apps page.

8 Managing Collaboration

Collaboration

Collaboration is the platform for cooperation across teams. With Collaboration information can be exchanged faster, knowledge can be shared and cooperation across borders is improved.

Group Coordinators and Collaboration Administrators manage the activities under Collaboration.

A Group Coordinator manages the group profile, edits requests to join private groups, privileges, and facilitates access and feed activity. Group Coordinators can delete their groups. As the creator of a group you are automatically the coordinator. You can grant user administrator privileges or revoke them from the members.

A Collaboration administrator has the same privileges as a coordinator. In addition, the Collaboration Administrator manages the posts that users have flagged, view all posts, delete them, and check activities reported as inappropriate.

Groups can be created for teams, departments, interest groups, topics, projects, and so on. There are public and private groups. Public groups are open to all users. For private groups, a coordinator decides who is to be granted access privileges to the group.

These are the five steps that are an optimal start to Collaboration:

1. “Modifying a User Profile” on page 73
2. “Finding Users and Groups and Following their Feeds” on page 74
3. “Defining Filters” on page 75
4. “Commenting on, Sharing, and Flagging Posts” on page 75
5. “Inviting other Users to Collaboration” on page 77

Collaboration View

You can manage the activities from the Collaboration view if you are a Coordinator or a Collaboration Administrator. You can click the  in the right top corner of the API Portal window and click Collaboration to navigate to this view.

From the collaboration view you can manage the group profile, edit requests to join private groups, privileges, facilitate access and feed activity, manage the posts that users have flagged, view all posts, delete them, and check activities reported as inappropriate. Various sections in this view and what operations you can perform from each of them is described in the table.

Field	Description
4	Specifies the number of new notifications. Click to view the notifications. If there are more than 3 notifications the Notifications dialog opens. You can click a notification message to see the details. Once you select a notification it is marked as read and the number of new notifications changes. Click **Unread** to see a list of all unread notifications. Click **Read**. A list of read notifications is displayed. You can click individual notifications or you can click **Delete all** to delete all the read messages. Click **Mark all as read** to mark all the unread messages as read. Click **Change your notifications changes** to change the settings to define how the notifications are displayed.
<user>	Specifies the user name with which you have logged in. It displays Administrator System if you have logged in as a Portal Administrator. Click to view the <user> profile view This view lists the posts that were published and categorised as Recent, Popular, and Active. You can search the required post by typing the characters in the search box. Click Edit profile to edit the user profile settings. Click **Followers** to view the users that are following you Click **Following** to list the users you are following.
My feed	Lists all my feed categorised as Recent, Popular, and Active. You can search the required post by typing the characters in the search box.
All company feeds	Lists all the company feeds categorised as Recent, Popular, and Active. You can search the required post by typing the characters in the search box.
My portal feed	Lists all feed from my portal categorised as Recent, Popular, and Active. You can search the required post by typing the characters in the search box.

Field	Description
Administration	You can manage your portal feeds from here. **Check flagged activities** - displays a list of flagged content. **Manage portal feeds** - displays a list of portal feeds alphabetically sorted. You can modify or delete a feed. Clean up activities- Select a date and click Delete to clear all activities that are older than the date specified. **Sync** - Click **Sync** to synchronize the permissions of Portal items.
Find groups	You can search a group from All Groups or My Groups section. **Statistics** - Displays the most active feed data. **All groups** - You can search a group from All Groups or My Groups section. ■ Click **Create group** to create a new group. ■ Click **Follow** to follow a particular group. **My groups** - Lists the group created by you or where you are a member of. Click **Create group** to create a new group.
Create group	Click to create a new group.
My bookmarks	Lists all the bookmarks you have saved.
My liked items	Lists all the items you have liked.
Create filter	Click to create custom filters to find interesting posts quickly and easily using keywords or to gain a better overview.
Check flagged activities	Click to check the flagged activities from the list.
Manage portal feeds	Click to manage the portal feeds. You can also synchronize access privileges.

Field	Description
Manage announcements	Click to manage announcements
Configure document user	Click to configure the ARIS document storage user
Dashboards	Click to view the dashboards.
Cleanup and export	
Configure notifications	Click to configure notification and customize them

Modifying a User Profile

Modify your user profile to provide other users with information about your areas of activity and interests.

To modify a user profile:

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Collaboration**.
3. Click *<user name>*.
4. Click **Edit profile**. The Edit profile page is displayed.
5. Upload a photo in JPG, PNG, or GIF format, with a maximum size of 4 MB. A square photo fits best.
6. After uploading, you can select the picture detail that you want to use. To do this, click **Edit**.
7. Use the frame to select the required picture detail.
8. Click **OK**.
9. In the **Title** field, provide your title that describes your position in the company.
10. In the **Description** field, provide a brief description of your job responsibilities.
11. In the **Keywords** field, specify keywords that will enable colleagues looking for particular information or expertise to find you. Use a comma as the separator.
12. In the **Phone** field, type your telephone number.

13. Select **Allow others to post to my feed** if you want your colleagues to be able to post information on your feed. and submit comments in your feeds.
14. Select **Allow others to comment on activities in my feed** if you want your colleagues to be able to submit comments in your feeds.
15. Click **OK**.

Your profile is now modified accordingly. The information is now available to other users.

Finding Users and Groups and Following their Feeds

You can look for colleagues or groups to find interesting contacts and information and follow their feeds.

To find users and groups and follow their feeds:

1. Type the name of the user or the group in the global find box at the top right. The search results are displayed dynamically. Continue typing characters until the relevant user or group is displayed.
2. Click the name you are looking for.

   The profile of the user or the group is displayed with all posts.
3. Do one of the following:
   - For users and public groups, click **Follow**.
   - For private groups, click **Send request**.

     Private groups are marked with a padlock icon.

When you follow users, you have access to the posts that they publish in their feeds. In private groups, a coordinator needs to confirm your request before you are allowed access to this group's posts, comments, and so on. In public groups you have immediate access to the group. The feeds you follow are displayed under **My feed** and the groups you follow under **Groups**. To stop following a user or group, click **Unfollow** in the user or group profile.

Users who are following your feeds are displayed under **Followers** in your profile.

Tip:

- To find groups, you can also use the group search function (**Groups > Find groups**). Alternatively, you can display the profile of another user to find out which groups that user belongs to.
- You can also use the global search to search for keywords, in order to find interesting feeds, users, and groups.

Defining Filters

You can define custom filters to find interesting posts quickly and easily using keywords or to gain a better overview.

To create a filter

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Collaboration**.
3. Click **Create filter**. The Create/edit filter page opens.
4. Select the relevant filter criteria, for example, whether you want all feeds or only feeds you follow to be included in the filter.
5. Type a name for the filter.
6. Specify the keywords that can be used to find relevant posts. Use a space to separate the keywords.
7. Click **OK**.

The filter is saved and is displayed under **Filters**. Click the filter name to display the posts that contain the specified keywords.

To change a saved filter, click **Edit filter**. To delete filters that you no longer require, click **Delete filter**.

Commenting on, Sharing, and Flagging Posts

Depending on whether a post is your own or from another user, you can perform different actions.

To comment on, share and flag posts

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Collaboration**.
3. Open the page containing the relevant post.
4. You can do one of the following:
   - Click **Like** to show other users what interests you. The user who wrote the post receives a notification, if they have made the relevant notification setting. The post is also flagged accordingly and added to your filter. To cancel your Like, click **Unlike**.

- Click **Comment** to type a comment or to add additional information for a post. You can also add a link to a Web site.
- Click **Share** to comment on a post by another user and publish it in your own feeds.

  To remove the post from your feeds, click **Delete**.
- Click **Bookmark** to add a post to your filters so that you can easily find it again later (**Filter > My bookmarks**).
- Click **Tag** to tag the post or a comment.
- Click **Delete** to delete a post or a comment.
- Click **Flag** to send a post to the Collaboration Administrator for review because you think it is inappropriate.
- Click the timestamp, for example, **2 hours ago** to display a post with all un-abbreviated comments, and so on.

Depending on the selected action, the affected users receive a message by email.

Creating a Group

Create your own group if you cannot find any interesting groups or you need a group for your team. Groups enable users to collaborate in a team and to participate in a special interest group or a particular topic.

To create a group

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Collaboration**.
3. Click **Create group**.

   The Create group page opens.
4. In the **Name** field, type a name for the group.
5. In the **Short name** field, type a short name you would want the group to be displayed as.
6. In the **Description** field, type information that describes the purpose of the groups feed.
7. In the **Keywords** field, type keywords that describe your group so that the group is easily found in search results. You can type in multiple keywords separated by comma.
8. In the **Web address** field, type the URL of the website if your group has one.

9. Click **Add coordinator** to add an additional coordinator, if required, who will manage the group profile and privileges. You can type in the search string for the user you are trying to find to add as a coordinator in the Search boxProvide As the creator of the group, you are automatically the coordinator.
   a. In the Search dialog that appears, type in the search string for the user you are trying to find to add as a coordinator
10. Enable the relevant privacy option.
11. Click **OK**.

Your group is created. It is displayed under **Groups**. Using tags, other users can find the group and follow its posts. In private groups, only members are able to read the posts. The group's name and description will, however, be visible in search results for non-members, as well.

Inviting other Users to Collaboration

You can invite other users to become a member in a specific group.

To invite other users to a group:

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Collaboration**.

   The Collaboration page appears.
3. Click the group to which you want to issue an invitation for.
4. In the **Add colleagues** box, enter the name of the person you want to invite.
5. Click **Add**.

The user receives a notification and can log in to Collaboration. Initially only read privileges are assigned, until the user becomes a member of the group .

Group coordinators can add more users to a group directly (**Add colleagues**). That user immediately becomes a member of the group and receives the posts, and comments by the group.

Accepting or Denying Requests to join Private Groups

You can accept or deny requests to join private groups of which you are a coordinator.

To accept or deny a request to join private groups:

1. Click  in the right top corner of the API Portal window to display the menu options.

2. Click **Collaboration**.
3. Click the private group.
4. Click **Requests**. The user requests are displayed.
5. Click **Accept** to accept the request.

   You can click **Deny** to deny the request.

If the user was accepted as a group member the user will be notified accordingly and displayed in the list of followers. If the user was denied membership the user and all other group coordinators receive a corresponding notification.

Granting or Revoking Group Coordinator Privileges

You can grant group coordinator privileges to additional group members or revoke them from the members on a need basis.

To grant or revoke group administrator privileges:

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Collaboration**.
3. Open a private group.
4. Click **Followers**. The members of this group are displayed.
5. In the row of the group member you can grant or revoke the administrator privileges by clicking **Grant** or **Revoke**.

The user is granted privileges or they are withdrawn. The user receives a notification. If a user is granted coordinator privileges all other coordinators of the group receive a notification, as well.

A coordinator can cancel group membership only if another coordinator withdraws the coordinator privileges from the user first.

Checking Activities Reported as Inappropriate

As a Collaboration Administrator, you can check content reported as inappropriate and decide if the content needs to be deleted.

To check activities reported as inappropriate

1. Open the notification you received for activities reported as inappropriate.
2. Click the link. The content reported is shown.
3. Verify whether the content violates the Collaboration terms of use.

4. Do one of the following:
   - Click **Approve** if the content is acceptable.
   - Click **Delete** if the content violates the terms of use.

The content reported was checked and depending on the result it is deleted or continues to be shown.

Modifying Notification Settings

You can specify the situations when you want to receive a notification about activities in API Portal and modify the settings accordingly.

To modify notification settings

1. Click  on the top left corner of the collaboration page to view notifications. The **Notifications** dialog is displayed.
2. Click **Change your notification settings**. The notification settings are displayed.
3. Specify the situations when you want to be informed about activities by other users or activities on groups. In each case, decide whether you want to receive the notification as an internal notification in API Portal(internal) or as an **e-mail**.
4. Click **Save**.

Your settings are saved. In the future, you will be notified in the selected situations.

Commenting on Portal Content

You can add comments to APIs and post information that could be of interest to your colleagues.

To comment on portal content

1. Click **API Gallery**.
2. Click **View details** for an API.
3. Click **Latest Posts**.
4. Type a comment. The text may have up to 250 characters.

   Note: If you want to add a link in the comment, the characters in the link are counted towards the 250 available characters.

5. Add links if required, by typing the required link and click **Add link**.

   The link is checked and added.

   If you add a link to a Web site , the link must start with http://.

6. Add tags, if required, by typing the required tags in the tag field.
7. Add a document, if required, by clicking .
8. Click **Post**.

Your comment is posted.

Publishing Posts

You can post information that could be of interest to your colleagues, or start a discussion on a particular topic.

To publish a post

1. Click in the right top corner of the API Portal window to display the menu options.
2. Click **Collaboration**.
3. Click **My feed**.
4. Type or copy the text into the input field. Up to 2000 characters are available.

   If you want to add a link the characters in the link are counted. To create a link to another user in the text, type '@' at the relevant point in the text, immediately followed by the name of the user.
5. You can attach a Tag, Link, and a File while publishing a post as follows:
   - To attach a Tag:
     i. Click <tag>.
     ii. Add the tag.
     iii. Press **Enter**.
   - To attach a Link:
     i. Click <link>.
     ii. Add the Link. The link must start with http://
     iii. Press **Enter**.
   - To attach a File:
     i. Click <File>.
     ii. In the Select Document dialog, select a file by browsing in the left hand panel and click **OK**.

     Alternatively you can also search for the file by clicking search and typing the required text in the search box.
6. Click **Post**.

Your post is published. If you have published something in your feed, the text is also displayed in the company feeds. If you have posted something in another user's feed, this information is also displayed in your feed and in the company feed, and is indicated by **<user name A> for <user name B>**. If you published a post in a private group you are a member of, the post is shown only to group members.

Using Hashtags

You can use hashtags to categorize posts using keywords or topics. This enables other users to find posts on interesting topics more easily. A hashtag consists of the **#** character followed by a keyword or phrase. There is no space after the # and the phrase does not contain any punctuation marks.

Examples

#BPM

#Optimize your processes using social collaboration

To use a hashtag

1. Type your post or comment in the relevant feed (your feeds, company feeds, group feeds).
2. Type the word to be used as a keyword, preceded by a # symbol, for example, #BPM, or enter a sentence. Alternatively, select an existing hashtag from the list.
3. Publish the post.

Your post is published and the keyword entered as a hashtag is highlighted in color as a link. Additionally, a tag is automatically created for the hashtag.

If a user clicks the hashtag, all post and comments subsequently entered are displayed on a separate page. A hashtag can be saved as a filter. You can then use the same hashtag in the filter definition, for example, #BPM.

Following API Portal content as a Group

You can follow any interesting content in API Portal as a group. This enables the group, for example, a project team, to jointly discuss and edit relevant processes.

Prerequisite

- You must be the coordinator of the group.
- The item from API Portal must either be followed as a portal feed or have comments in Collaboration.

To follow API Portal content as a group

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Collaboration**.
3. Activate the group that has to follow portal feeds.
4. Click **Edit group**.
5. Click **Follow portal feeds**. The dialog opens.
6. Type a search term for finding the portal feed. Ensure that the spelling is correct.
7. Select the required portal feed in the search result.
8. Click **OK** in both the dialog and the group.

Using the **Following** button, all members of the group can now view the portal feed.

The portal feeds a group is following are displayed in the group under **Following**. Comments are shown directly in the group. To stop following a portal feed, the coordinator removes the feed from the list of portal feeds being followed (by clicking **Delete**).

Users of the group are notified when the portal feed changes or comments are added to it.

Finding Help

In addition to this online help, there are various ways you can find support in Collaboration.

To find help

- Publish a post containing your question and use the hashtag**#Help**.

  This keyword enables other users to find and reply to your question. Alternatively, contact your system administrator.

9 Analytics

Dashboard

Dashboard displays a variety of charts to provide an overview of API Portal and it's API usage. Dashboard can be accessed by clicking the **Dashboard** option in the user action menu. Select the type of dashboard in the dashboard drop down list to view the particular dashboard.

The different types of dashboards available are:

- **API audit log** - used to view the lifecycle and access token events for an API, the API audit log, and monitor the subscriptions per package.
- **Runtime dashboard** - used to study the API's invocations and its performance during runtime.
- **API trends dashboard** - used to study the API invocation trends by response time, success and failure rates.
- **Consumer dashboard** - used to track the total API requests over a period of time, requests over time per API, and API request log.

You can create time based filters to view the statistics in the selected time range.

Select...	To...
Quick Time	You can select a time range from a defined list. For example, **Last 24 hours**, **Previous week**, and so on. The data displayed would be the data captured in the time range specified. By default, the time range selected is **Last 24 hours**.
Relative Time	You can select a time relative to the current time. The range can be specified in minutes, hours, days, weeks, and months. For example: Selecting **10 days ago** in the **From** field and **Now** in the **To** field displays the data in the time interval chosen.
Absolute Time	You can specify an absolute time range, by selecting the required dates in the date picker. For example, selecting specific dates in the **From** and **To** fields displays data in the time interval chosen.

Note: Localization is not supported in API Portal dashboards.

API Trends Dashboard

The API trends dashboard is used to study the API invocation trends by response time, success and failure rates. You can filter the data as required and view the required data by hovering the cursor over the legend in each of the charts.

The KPIs can be monitored in each of the charts displayed.

KPI	Purpose
API trends by response	Tracks and compares the total successful invocations with total failed invocations for APIs present in the API Portal in the specified interval. The failure and the successful events are depicted by different colors in the graph.
API trend by success	Tracks the invocation trends for top 5 APIs based on most successful invocation in API Portal in the specified interval. The invocation trends from 5 different APIs are depicted by different colors.
API trend by failure	Tracks the invocation trends for top 5 APIs based on most failed invocation in API Portal in the specified interval. The invocation trends from 5 different APIs are depicted by different colors.
Overall average response time	Tracks the overall average response time for all APIs in API Portal over time in the specified interval.
Average Response time by API	This chart depicts the average response time for top 5 APIs inAPI Portal over time in the specified interval.

You can use the following options to resize the view and view the legend of the required KPI.

Settings	Description
	Click to view the legend of the chart. Hovering the cursor over any of the elements in the legend highlights the section pertaining to the legend chosen.

Settings	Description
⌟	Use this to resize the chart.

Runtime Dashboard

The Runtime Dashboard is used to study the API's invocations per user and its performance during runtime. You can filter the data as required and view the required data by hovering the cursor over the legend in each of the charts.

The KPIs can be monitored in each of the charts displayed.

KPI	Purpose
Top 10 APIs	Tracks the top 10 APIs based on the API requests.
Requests per user	Depicts the distribution of API requests across users.
Top APIs by consumption	Tracks the top 10 APIs based on API's consumption. The different colors in the chart represents different consumer application name.
Overall events	Depicts the total number of events that are generated for the API published in API Portal for the specified time interval. The data is displayed in the form of a donut chart. The chart is sliced based on the distribution of event types.
Requests over time by API	Tracks the number of API requests over time.
Runtime events	The table displays the information of all generated events, sorted by the descending order of creation date. Details include: ■ **Time** – time when the event was logged. ■ **eventType** – type of event . ■ **apiName** – name of the API for which the event was triggered. ■ **apiVersion** - version of the API.

KPI	Purpose
	■ **operationName** – name of the operation that triggered the event. ■ **applicationName** - name of the application that generated the event. ■ **applicationIP** - IP address of the application. ■ **request** – description for the alert generated. ■ **response** – source that triggered the alert. ■ **responseCode** - response code for the event. ■ **providerTime** - time interval in milliseconds from when a request is forwarded to a native provider until a response is received from the provider. ■ **totalTime** - time interval in milliseconds from when a request is received by the virtual service runtime until the response is returned to the caller.

You can use the following options to resize the view and view the legend of the required KPI.

Settings	Description
	Click to view the legend of the chart. Hovering the cursor over any of the elements in the legend highlights the section pertaining to the legend chosen.
	Use this to resize the chart.

API Audit Log

The API audit log dashboard is used to used to view the lifecycle and access token events for an API, monitor the subscriptions per package, and access token requests per API. You can filter the data as required and view the required data by hovering the cursor over the legend in each of the charts.

The KPIs can be monitored in each of the charts displayed.

KPI	Purpose
API life cycle events	Tracks events of an API like Publish, RePublish, and UnPublish over time. The different coloured lines in the line graph depict the different categories of events.
Access token events	Tracks all access token related activities like RequestAaccessToken, RenewAccessToken, and RevokeAccessToken over time.
Access token event distribution	Displays the distribution of access token events like RequestAaccessToken, RenewAccessToken, and RevokeAccessToken.
Access token requests per API	Tracks the number of access token requests for an API. Displays the top 5 APIs.
Subscriptions per package	Tracks the number of subscriptions per package package. Each package can have multiple plans associated with it. So the subscriptions of a package are displayed as a stacked bar chart depicting the subscriptions of each associated plan. It displays the top 5 packages.
Audit log	The table lists information of all the events sorted by the descending order of creation date. Details include: ■ **Time** – time when the event was logged. ■ **eventType** - the type of event that was generated. ■ **userName** – user who initiated the event. ■ **apiName** – name of the API. ■ **apiVersion** – version of the API. ■ **applicationName** – name of the application for which the event was generated. ■ **domainName** – name of the package. ■ **planName** - name of the plan.

You can use the following options to resize the view and view the legend of the required KPI.

Settings	Description
	Click to view the legend of the chart. Hovering the cursor over any of the elements in the legend highlights the section pertaining to the legend chosen.
	Use this to resize the chart.

Consumer Dashboard

Consumer dashboard captures the KPIs specific to the visitors who access API Portal. It is used to track the total API requests over a period of time, requests over time per API, and API request log.

You can filter the data using the two filters:

- **Application filter** - The Applications drop-down list displays all the applications of the user. You can select any application and the dashboard displays data for the application selected.
- **API filter** - On selecting an application, the APIs corresponding to that application are displayed in the APIs drop-down list. If there are multiple APIs associated with an application (in case of subscription tokens), you can choose an API from the APIs list.

The data displayed are based on the selected application and API combination. All the charts in this dashboard represent the data of the logged in user. You can view the required data by hovering the cursor over the legend in each of the charts.

The KPIs can be monitored in each of the charts displayed.

KPI	Purpose
Total requests (Today)	Tracks the total number of API requests made by the logged in user, for the day. This is independent of the time chosen in the time filter.
Total requests (Last 7 days)	Tracks the total number of API requests made by the logged in user, in the last 7 days. This is independent of the time chosen in the time filter.
Total requests (Last one month)	Tracks the total number of API requests made by the logged in user, in the last month.

KPI	Purpose
	This is independent of the time chosen in the time filter.
Total requests (Chosen interval)	Tracks the total number of API requests made by the logged in user, for the time interval chosen in the time filter.
Requests per API	Tracks the number of requests for each API. For a versioned API, this chart is displayed in a stacked bar format for different versions of that API.
Requests over time by API	Tracks the number of API requests over time.
Average response time	Depicts the average response time of the top 5 APIs over time in the specified time interval.
API request log	Displays the information of all the transactions of the logged in user, sorted in the descending order of creation date. The table displays information such as time when the event was created, API Name, API version, name of the application that generated the event, IP address of the consumer, request and response details.

You can use the following options to resize the view and view the legend of the required KPI.

Settings	Description
	Click to view the legend of the chart. Hovering the cursor over any of the elements in the legend highlights the section pertaining to the legend chosen.
	Use this to resize the chart.

Viewing Dashboards

Dashboards display a variety of charts to provide an overview of the API usage.

Prerequisite

You must have the **API Administrator** role.

To view a dashboard

1. Click  in the right top corner of the API Portal window to display the menu options.
2. Click **Dashboard**.
3. Select the dashboard type.

The Dashboards page opens and different charts are displayed.