Informatica® Intelligent Cloud Services
Summer 2019 September

API Manager Guide

Informatica Intelligent Cloud Services API Manager Guide
Summer 2019 September
September 2019

Publication Date: 2019-09-11

Table of Contents

Chapter 1: Introduction to API Manager. 5

Workflow for Creating and Using a Managed API. 5
Before You Start. 6
API Domain Name. 6
Authentication for Managed APIs. 6
Accessing API Manager. 7

Chapter 2: Administration. 8

Custom API URLs. 9
Before you start. 9
Configuring API URL customization. 9
Viewing services and managed APIs. 9
API Registry Properties. 10
Creating and Deleting a Managed API. 11
Viewing managed API details and metadata. 11
Interactively Testing a Managed API. 12
Generating and Exporting an SDK Package. 13
Disabling and Enabling API Portal View for a Managed API. 13
Renaming a Managed API. 14
Deactivating and Activating a Managed API. 14
Searching for a Service or Managed API. 14
Configuring an API-specific rate limit policy. 15
Configuring an API-specific IP filtering policy. 15
Configuring a privacy policy for a managed API. 16
JSON Web Token Authentication for Managed APIs. 16
JSON Web Token Authentication Tasks. 17
JSON Web Token Expiration. 18
Prerequisites. 18
Configuring JSON Web Token Authentication. 18
Generating JSON Web Tokens for Multiple Managed APIs Simultaneously. 20
API Invocation based on the Authentication Method. 21
Managing API Groups. 21
Adding Managed APIs to a Managed API Group. 22
Viewing and editing Managed API groups. 22
Generating JSON Web Tokens for Managed API Groups. 23
Deleting a Managed API Group. 23

Chapter 3: Organization policies. 24

Updating the Rate Limit Policy. 24
Configuring an IP filtering policy. 25

Searching for an IP Filtering Policy. 25

Chapter 4: Analytics. 26

Overview Reports. 26

Overview Reports Properties. 26

Activity Log. 27

Activity Log Properties. 27

Exporting an Activity Log. 28

Event log. 28

Event log properties. 28

Exporting an event log. 29

Searching for a log. 29

Index. 30

CHAPTER 1

Introduction to API Manager

API Manager is a cloud-based service that an organization uses to manage the APIs for enterprise services and processes built in Informatica Cloud Application Integration. With API Manager, your organization can deploy, manage, and control the use of APIs.

API Manager provides the following functionality:

- Seamless integration with Informatica Cloud Application Integration to manage APIs for Informatica Cloud Application Integration services using REST and SOAP protocols
- Rapid integration of managed APIs into organization applications through software development kit (SDK) packages
- API lifecycle management, including activating, deactivating, and deleting APIs
- Access to API metadata and description
- Enforcement of a rate limit policy, IP filtering policy, and privacy policy for a managed API
- Management of organization API policies, including global rate limit and IP filtering policies
- API analytics, including dashboard, activity log, and event log

With API Manager, your organization ensures that internal or external users can safely and securely use the organization APIs. Administrators use API Manager to create managed APIs from Application Integration services, and to set policies and access authorization that control the usage of managed APIs.

Administrators can monitor and analyze managed API usage with the API Analytics dashboard, and with activity and event logs. The Analytics dashboard provides a visual summary information about APIs, which includes trends in usage over time, APIs with the most invocations, and the most frequent users. The activity log includes a comprehensive report of all API access attempts. The event log allows administrators to quickly identify and analyze unauthorized API access attempts, rate limit and IP filtering policy exceptions, and privacy policy leakages.

Workflow for Creating and Using a Managed API

To create and use a managed API, perform the following steps:

1. Select an Informatica Cloud Application Integration service.
2. Create a managed API for the service. When API Manager creates a managed API, it activates the managed API.
3. Optionally, set rate limit and privacy policies for the managed API.
4. Optionally, update the default organization rate limit and IP filtering policies.

5. Copy the managed API URL and provide the URL to API consumers. Alternatively, API consumers can use API Portal to access managed APIs. For more information about the API Portal, see the *API Portal* help.

Before You Start

Before you use API Manager, ensure that you have an active Informatica Intelligent Cloud Services account, have assigned user roles through the Administrator, and have an API Manager license. To access API Manager, the user must be assigned both the **Admin** and **Service Consumer** roles, or both the **Deployer** and **Service Consumer** roles. If a new role is assigned, it is populated to the API gateway within 5 minutes.

For more information about registration and roles, refer to the *Informatica Cloud Administrator Guide*.

Note: A trial subscription includes access to API Manager with a trial license during the trial period.

API Domain Name

When you access API Manager for the first time, you are prompted to select an API domain name.

The domain name identifies the organization and is used in the URLs created for the managed APIs of an organization. For example, the URL of the managed API of a service named `GetEmployee` might be `https://<base-url>/<API-domain-name>/t/GetEmployee`. You might want to use a subdomain of the organization domain.

Select the domain name carefully. You can change the domain name at any time, but any change of the domain name after you start to use the system will result in the deletion of your organization API Manager settings, including managed APIs, policies, and analytics data.

Tip: You can customize the URLs of managed APIs so that the API domain name replaces the Informatica domain name as the base URL of the API. For more information, see "Custom API URLs" on page 9.

Authentication for Managed APIs

You can configure basic authentication and JSON Web Token (JWT) authentication for managed Informatica Cloud Application Integration APIs.

If you configure basic authentication, the user groups and users that are provided access to the API in Informatica Cloud Application Integration can invoke the API.

If you configure JWT authentication, you can generate a token using API Manager or API Portal and use the generated token to invoke the API. JWT is an open standard that helps in the secure transmission of information between API consumers and REST web services such as Informatica Cloud Application Integration service APIs. For more information about configuring JWT authentication, see "JSON Web Token Authentication for Managed APIs" on page 16.

You can create groups of managed APIs and then generate a token for the group to use when invoking any JWT authenticated API in the group. You can add or remove APIs from the group. For more information about managing API groups see "Managing API Groups" on page 21.

Accessing API Manager

Access API Manager through the Informatica Intelligent Cloud Services **My Services** page.

1. In the Informatica Intelligent Cloud Services login page, enter your user name and password.
2. Click **Log In**.
3. In the **My Services** page, select **API Manager**.

   API Manager appears.
4. If you are accessing API Manager for the first time, select an API domain name. On the **API Domain Name** window, define a unique domain name and click **Save**.

CHAPTER 2

Administration

Use API Manager to manage APIs for your organization. To manage an API, you select an Informatica Intelligent Cloud Services service and create a managed API for the service. When API Manager creates the managed API, it activates it. You can copy the managed API URL and provide it to your API consumers.

You can customize the URLs of managed APIs so that the API domain name replaces the Informatica domain name as the base URL of the API.

After API Manager activates the managed API, you can make the API available API Portal. API consumers can use API Portal to access detailed information about APIs so that they can incorporate APIs into their applications. API consumers can also use API Portal to test and debug API execution. For more information about API Portal, see the *API Portal* help.

If you want to temporarily make a managed API unavailable, you can deactivate the managed API. Alternatively, you can hide an active managed API from API Portal without deactivating it. For example, during an API test phase, you can remove the display of the managed API from the portal until you are ready to release it to API consumers. When testing is complete, you can display the managed API in the portal again.

To stop running the service as a managed API, you can delete the managed API. When you delete the managed API, the Informatica Intelligent Cloud Services service is not affected.

Use API Manager to generate SDK packages for rapid integration of managed APIs into organization applications. You can generate SDK packages that provide a set of resources to enable integration for Java, Android, Javascript, Nodejs, Python, Ruby-on-Rails, C#.NET, ASP.NET5, or C# applications.

You can define API-specific policies to enforce security and access rules. For each managed API, you can configure a rate limit policy, an IP filtering policy, and a privacy policy.

You can configure basic authentication or JSON Web Token (JWT) authentication for managed Informatica Cloud Application Integration APIs. With basic authentication, the user groups and users that are provided access to the API in Informatica Cloud Application Integration can invoke the API. With JWT authentication, you can generate a token using API Manager or API Portal and use the generated token to invoke the API.

You can create groups of managed APIs and then generate a token for the group to use when invoking any JWT authenticated API in the group. A managed API can belong to one group only.

Custom API URLs

You can customize the URLs of managed APIs so that the API domain name replaces the Informatica domain name as the base URL.

For example: Your organization API domain is `org-subdomain.com`, and the name of the managed API is Customers. When you create a managed API, API Manager creates one of the following API URLs, based on whether or not you configured API URL customization:

- If you don't customize the API URLs, API Manager creates the following URL:

  ```
  https://apigw-pod1.dm-us.informaticacloud.com/t/org-subdomain.com/Customers
  ```

- If you customize the API URLs, API Manager creates the following URL:

  ```
  https://org-subdomain.com/Customers
  ```

Before you start

Before you configure API URL customization, provide Informatica with a certificate for the organization API domain.

Perform the following tasks:

1. In your DNS, define routing from the organization API domain to the Canonical Name record of the following URL:

   ```
   https://apigw-pod1.dm-us.informaticacloud.com
   ```

   For more information about API domain names, see "API Domain Name" on page 6.
2. Generate a certificate for the organization API domain.
3. Contact Informatica Global Customer Support and provide them with the certificate.

Informatica Global Customer Support will inform you when you can configure the customization.

Configuring API URL customization

1. In the **API Registry** page, click the Settings icon.
2. In the **API Domain Name** page, select **Use the API domain name as the default API URL**.
3. Click **Save**.

Viewing services and managed APIs

Use the **API Registry** page of API Manager to view and select Informatica Cloud services and create and handle managed APIs.

The **API Registry** page shows services and managed APIs in alphabetical order. You can view service details and managed API details. To sort the services and managed APIs, click the title of the column to sort. To view services only, select **All Services**. To view managed APIs only, select **Managed Services**.

To create and use a managed API, you perform the following actions in the **API Registry** page:

1. Create a managed API for the service.

2. Copy the managed API URL and provide the URL to API consumers. Alternatively, API consumers can use API Portal to access managed APIs.

   Tip: You can customize the URLs of managed APIs so that the API domain name replaces the Informatica domain name as the base URL of the API. For more information, see "Custom API URLs" on page 9.

In the **API Registry** page you can also perform the following actions:

- Deactivate and delete a managed API
- Add a managed API to a group or remove the managed API from a group.

Note: By default, all managed APIs can be accessed through API Portal. You can select to disable portal access.

If a managed API exists for a service that is unavailable or has been deleted, the managed API is greyed out in the display.

API Registry Properties

The following table describes the **API Registry** page properties:

Property	Description
Icon	Icon identifies whether the entity is a service or managed API: -  : Designates a service. -  : Designates a managed API.
Name	Name of the managed API. The name must be unique in the organization. The name can contain up to 50 characters, including any letter on the ASCII table, any digit, and the special characters . _ and -. The name cannot contain spaces and any of the following characters: "~!@#;:%^. &*+={}()|<>,'/\$ The name is part of the API URL.
Protocol	The protocol of the service or the managed API: - REST - SOAP Informatica Cloud Application Integration services are published with both REST and SOAP endpoints.
Status	Status of a managed API: - Active  : The managed API is active. - Inactive  : The managed API is currently not available. - Service not available  : This status indicates a managed API for a service that is unavailable or deleted. If the service for which a managed API has been created is unavailable or deleted, the managed API is greyed out.

Property	Description
Authentication Method	API authentication method: - Anonymous: The API does not require the API consumer to authenticate. - Basic: The API consumer must provide an Informatica Intelligent Cloud Services user name and password for authentication. - JWT - JSON Web Token: The API consumer must pass the JWT token as a bearer token in the HTTP Authorization header for authentication. For example: `Authorization: Bearer aF…mk` - JWT and Basic: The API consumer can either pass the JWT token as a bearer token in the HTTP Authorization header or provide the login credentials of the allowed user groups or users for authentication.
Rate Limit	An individual rate limit policy for a managed API.
Group	The group to which the API belongs.
Description	Description of the service.

Creating and Deleting a Managed API

You can create a managed API for any Informatica Intelligent Cloud Services service. By default, the managed API is active and API Portal view for the API is enabled. The name that you assign to the API is part of the API URL.

1. In the **API Registry** page, select a service.
2. Click to open the Actions menu, and then select **Create Managed API**.
3. In the **Create Managed API** window, enter a name for the API or accept the default name, and click **OK**. The name must be unique in the organization. The name can contain up to 50 characters, including any letter on the ASCII table, any digit, and the special characters . _ and -. The name cannot contain spaces and any of the following characters: "~!@#;:%^. &*+={}()|<>,'/\$

   To delete a managed API, in the **API Registry** page, select the API, click to open the Actions menu, and select **Delete Managed API**. The Informatica Intelligent Cloud Services service on which the API was based is not affected.

Viewing managed API details and metadata

After you create a managed API, you can view API details, including the API URL and the Swagger or WSDL URL, depending on the type of service from which you create the managed API.

Copy the URL of the managed API and provide it to API consumers to invoke the API. Copy the Swagger or WSDL URL and use it to view API metadata.

Tip: You can customize the URLs of managed APIs so that the API domain name replaces the Informatica domain name as the base URL of the API. For more information, see "Custom API URLs" on page 9.

1. In the **API Registry** page, click to select a managed API, or click to open the Actions menu and select **View API Details**.

   The **API details** window appears and displays relevant details.

   Note: API Manager **Service Name** is the Application Integration Process **Unique Name**, not the process name. The unique name differs from the process name when there are spaces or special characters in the process name, or when the same process name is given to processes in different folders in the Informatica Cloud organization.

2. To obtain the URL of the API, click **Copy URL**.

   Alternatively, you can obtain the API URL directly from the **API Registry** page. Perform the following actions:

   1. Select a managed API.
   2. Click to open the Actions menu, and select **Copy URL**.

   The URL is copied to the clipboard.

3. To obtain the URL to view metadata details for the managed API, in the **API details** window, select the available option:

   - For a REST API, click **Copy Swagger URL**.
   - For a SOAP API, click **Copy WSDL URL**.

   The URL is copied to the clipboard. You can paste the URL in your browser to view the metadata results.

Interactively Testing a Managed API

You can interactively test a managed API created for a REST API in a Swagger interface. You can view the API URL, the HTTP status codes, the request parameters, and the response parameters. You can also execute the API for testing purposes, or get a sample cURL command.

1. In the **API Registry** page, click to select a managed API, or click to open the Actions menu and select **View API Details**.

   The API details window appears.

2. Select the **Swagger** tab.
3. If the API requires authentication, the **Authorization** dialog box appears. Enter the username and password of a user who is authorized to access the API.
4. To expand the view in the **Swagger** tab, click the arrows in the upper right corner.
5. To view the API request body and response codes, click any button that displays an API method.

   For example, for an API with a POST method, a **POST** button is displayed. Click the **POST** button to view the API request body.

6. To view the request body in JSON format, select **application/json**. To view the request body in XML format, select **application/xml**.
7. To test the API semantics, in the request body panel, perform the following steps:

   a. Click **Try it out**.

   b. Edit the request body. Replace any parameter type with a value.

c. To test the updated request body, click **Execute**.

   The **Server response** panel displays the response body, response headers, and request duration time.

d. To clear the server response, click **Clear**.

e. To cancel the request body changes, click **Cancel**. To change the request body again, click **Edit**.

8. To view the request or response syntax, in the **Models** panel, click the right arrow near the request or response entry.

   The model request or response body is displayed. A red asterisk next to an element indicates a required element.

Generating and Exporting an SDK Package

You can generate and export an SDK package for a managed API. You can use the SDK package to integrate the managed API into your applications.

1. In the **API Registry** page, click to select a managed API.

   The API details window appears.

2. Select the type of client SDK package that you want to generate.

3. Click **Download**.

   The **API Registry** window appears.

4. Enter your API Manager user authorization details.

   The SDK package downloads to your host machine. To obtain information about the SDK package, read the `readme.md` file.

Disabling and Enabling API Portal View for a Managed API

API Portal view for a managed API is enabled by default. When you disable API Portal view for a managed API, the managed API does not show on the API Portal. API consumers can access the managed API with the Managed API URL.

1. In the **API Registry** page, click to select a managed API, or click to open the Actions menu and select **View API Details**.

   The API details window appears.

2. To disable API Portal view for the managed API, clear **Available on API Portal**, and then click **Save**.

   To re-enable API Portal view, open the API details window, select **Available on API Portal**, and then click **Save**.

Renaming a Managed API

When you rename a managed API, the API URL changes accordingly. Be sure to inform API consumers of the new URL.

1. In the **API Registry** page, verify that the status of the managed API to rename is Inactive. If the status is Active, click to open the Actions menu, and then select **Deactivate**.
2. Click the managed API.

   The API details window appears.
3. Click in the **API Name** field, name the API, and then click **Save**. The name must be unique in the organization. The name can contain up to 50 characters, including any letter on the ASCII table, any digit, and the special characters . _ and -. The name cannot contain spaces and any of the following characters: "~!@#;:%^. &*+={}()|<>,'/\$

   API Manager saves the managed API with the new name. In the API URL field, the URL changes accordingly.
4. Click **Copy URL**. Send the new URL to API consumers.
5. To reactivate the API, in the **API Registry** page, click to open the Actions menu, and then select **Activate**.

Deactivating and Activating a Managed API

To disable a managed API, you can deactivate it. To use the API again, reactivate it.

1. In the **API Registry** page, select a managed API.
2. Click to open the Actions menu, and then select **Deactivate** to deactivate the API, or select **Activate** to activate the API.

Searching for a Service or Managed API

You can search for a managed API or for an Informatica Cloud service by sorting columns or searching for specific text.

1. To sort the services or managed APIs according to a specific property, in the **API Registry** page, click the column picker icon to the left of the **Find** field and then select the column to sort.

   Managed APIs and the services are sorted accordingly.
2. To search for managed APIs and services based on specific text, in the **Find** field, type the text by which to search. The search is performed on all columns.

   The APIs table shows the relevant managed APIs or services.

Configuring an API-specific rate limit policy

Create a rate limit policy for a specific managed API. The rate limit policy controls the number of times API consumers can invoke the API during a designated time period.

The API-specific rate limit overrides the organizational rate limit policy. For example, if the organizational rate limit is 10 invocations per second, and the API-specific rate limit is 20 invocations per second, API Manager rejects attempts to access the API after the 20 invocations per second limit is reached.

If a rate limit policy is not defined for a managed API, or if the API-specific rate limit policy is disabled, API Manager applies the organizational rate limit policy to the API.

When an API consumer attempts to access a managed API and access is denied due to a rate limit policy, the HTTP response includes a `429 Too Many Requests` status code and the description `API rate limit reached`. API Manager logs an access exception in the event log. For more information about the event log, see "Event log" on page 28.

1. In the **API Registry** page, click to select a managed API, or click to open the Actions menu and select **View API Details**.

   The API details window appears.
2. Select the **Policies** tab.
3. Select **Enable API-specific rate limit policy**, enter the number of requests and the number of milliseconds that define the rate limit policy, and then click **Save**.

   To disable the API-specific rate limit policy for the API, clear the option **Enable API specific rate limit policy**, and then click **Save**.

Configuring an API-specific IP filtering policy

Create an IP filtering policy for a managed API. The IP filtering policy designates the range of computer IP addresses that are allowed or denied permission to invoke the API.

If an IP filtering policy is not defined for a managed API, or if API Manager doesn't find any matches with the API-specific policy, API Manager applies the organizational IP filtering policy to the API.

When the policy is breached, API Manager logs an event in the even log. For more information about the event log, see "Event log" on page 28.

1. In the **API Registry** page, click to select a managed API, or click to open the Actions menu and select **View API Details**.

   The API details window appears.
2. Select the **Policies** tab.
3. In the **IP Filtering Policy** section, select to allow or deny a range of addresses, then fill in the IP range.
4. Add a description of the rule and click **Add**.

   The rule appears in the **IP Filtering Rules** list.
5. Add as many rules as required to define the policy. The order of the rules determines the precedence. The higher the rule is in the list, the higher the precedence.
6. To move a rule up or down the list and change the precedence, rest on a row to move and click the Action menu at the right end of the line. From the menu select **Move Up** or **Move Down**.

7. To delete a rule, rest on a row to delete and click the Action menu at the right end of the line. From the menu select **Delete**.

Configuring a privacy policy for a managed API

Configure a privacy policy for a managed API to protect private information that is contained in API data.

API Manager logs a privacy policy leakage in the event log if an API request or response payload contains the following information:

- Credit card number
- Email address
- IP address
- United States address
- United States phone number
- United States Social Security number

For more information about the event log, see "Event log" on page 28.

Preview Notice: Effective in version Winter 2019 June, privacy policy is available for preview. Preview functionality is supported for evaluation purposes but is unwarranted and is not production-ready. Informatica recommends that you use in non-production environments only. Informatica intends to include the preview functionality in an upcoming release for production use, but might choose not to in accordance with changing market or technical circumstances. For more information, contact Informatica Global Customer Support. To use the functionality, your organization must have the appropriate licenses.

1. In the **API Registry** page, click to select a managed API, or click to open the Actions menu and select **View API Details**.

   The API details window appears.
2. Select the **Privacy Policy** tab.
3. Select **Enable privacy policy**.
4. Select the type of information to protect, and whether to apply protection of each information type to requests, responses, or both.
5. Click **Save**.

   To disable the privacy policy for the API, clear **Enable privacy policy** and then click **Save**.

JSON Web Token Authentication for Managed APIs

You can configure JWT authentication for a managed Informatica Cloud Application Integration API that meets all of the following criteria:

- The associated process uses HTTP/SOAP binding.
- The associated process uses basic authentication and defines the user groups and users who can access the process service URL at run time.
- The associated process is published and exposed as a service.

You can configure a managed API to use one of the following authentication methods for JWT authentication:

JWT - JSON Web Token

Use this authentication method to configure JWT authentication with tokens. You can generate a token and set an expiration date for it.

You can invoke the API by passing the token as a bearer token in the HTTP Authorization header. For example:

```
Authorization: Bearer aF…mk
```

JWT and Basic

Use this authentication method when you want to use both the following options:

- Configure JWT authentication with tokens. You can generate a token and set an expiration date for it.
- Allow the API to be accessed by the user groups and users who have been provided access to the API in Informatica Cloud Application Integration.

You can invoke the API by both the following methods:

- Passing the token as a bearer token in the HTTP Authorization header
- Providing the login credentials of the allowed user groups or users

Note: You cannot configure JWT authentication if you select the authentication method as **Basic**.

JSON Web Token Authentication Tasks

After you publish an Informatica Cloud Application Integration process, Informatica Cloud Application Integration automatically exposes the service API to API Manager. You can then create a managed API for the Informatica Cloud Application Integration service API and make it available in API Portal.

Based on the role and privileges you are assigned, you can use API Manager or API Portal to perform JWT authentication tasks.

JWT Authentication Tasks in API Manager

Use API Manager to perform the following tasks for JWT authentication:

1. Configure JWT authentication for the managed API.
2. Generate a token and set an expiration date for the token. You can generate tokens for up to 15 APIs simultaneously. Optionally, you can make the managed API available in API Portal so that API Portal users can discover available APIs and view their authentication method.
3. Invoke the managed API by using the generated token.

JWT Authentication Tasks in API Portal

Use API Portal to perform the following tasks for JWT authentication:

1. View a list of managed APIs available in API Portal and view their authentication method.
2. Generate a token and set an expiration date for the token. You can generate tokens for up to 15 APIs simultaneously.
3. Invoke the managed API by using the generated token.

For more information about the JWT authentication tasks you can perform in API Portal, see the *API Portal* help.

JSON Web Token Expiration

API Manager uses the Coordinated Universal Time (UTC) time zone for the JWT token expiration and uses the current time on your computer as the baseline time for the token expiration. The token expires on the expiration date you configure and a minute earlier than the time at which you generated the token.

For example, if you generate the token on January 10 at 2:30 p.m. and set the expiration date as January 11, the token expires on January 11 at 2:29 p.m. If you set the expiration date as January 15, the token expires on January 15 at 2:29 p.m.

After a token expires, you cannot refresh it. You must generate a new token.

Prerequisites

Before you configure JWT authentication in API Manager, you must perform the following prerequisite tasks in Informatica Cloud Application Integration:

1. Create a process and enable HTTP/SOAP binding for the process.
2. Configure basic authentication for the process by defining the user groups and users who can access the process service URL at run time.

   Note: You can configure JSON web token authentication for a managed API only if the associated process uses basic authentication in Informatica Cloud Application Integration. You cannot configure JWT authentication if the associated process allows anonymous access.
3. Publish the process to expose it as a service.

Configuring JSON Web Token Authentication

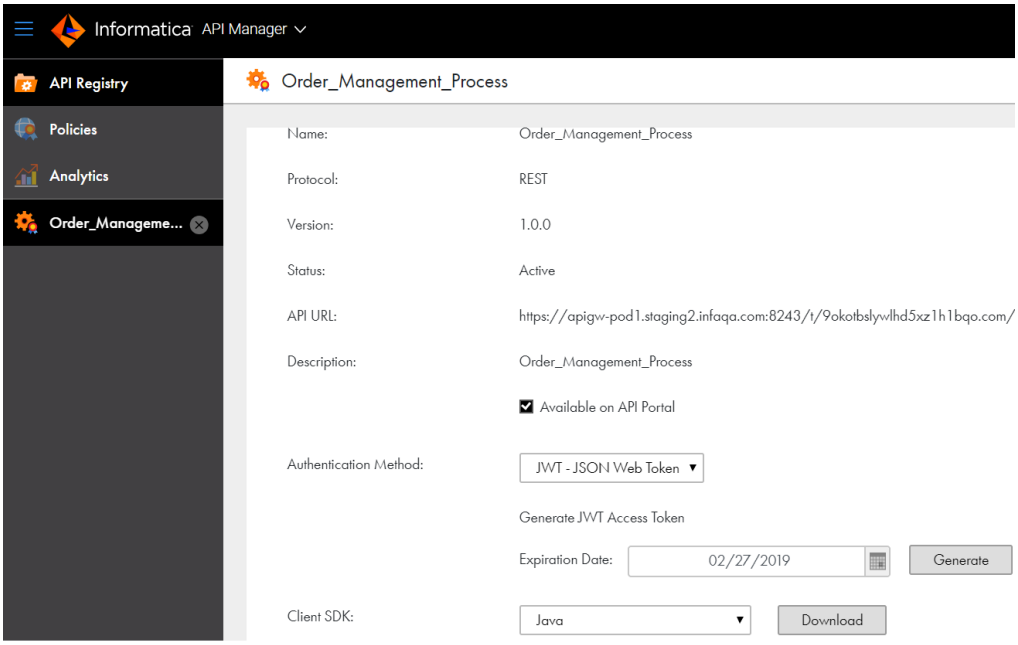
After you create a managed API for a service that you published in Informatica Cloud Application Integration, you can configure JWT authentication, generate a token, and set an expiration date for the token. Optionally, you can make the managed API available in API Portal so that API Portal users can discover it in API Portal and invoke it.

1. On the **API Registry** page, click the managed API for which you want to configure JWT authentication.
2. On the **General** tab, from the **Authentication Method** list, select one of the following values:

Value	Description
JWT - JSON Web Token	Select to configure JWT authentication with tokens. You can generate a token and set an expiration date for it. You can invoke the API by passing the token as a bearer token in the HTTP Authorization header. For example: `Authorization: Bearer aF…mk`
JWT and Basic	Select to configure JWT authentication with tokens and allow basic authentication for the managed API. You can generate a token and set an expiration date for it. When you select this option, you also allow the API to be accessed by the allowed user groups and allowed users defined for the API in Informatica Cloud Application Integration. If you select this option, you can invoke the API by both the following methods: - Passing the token as a bearer token in the HTTP Authorization header - Providing the login credentials of the allowed user groups or users

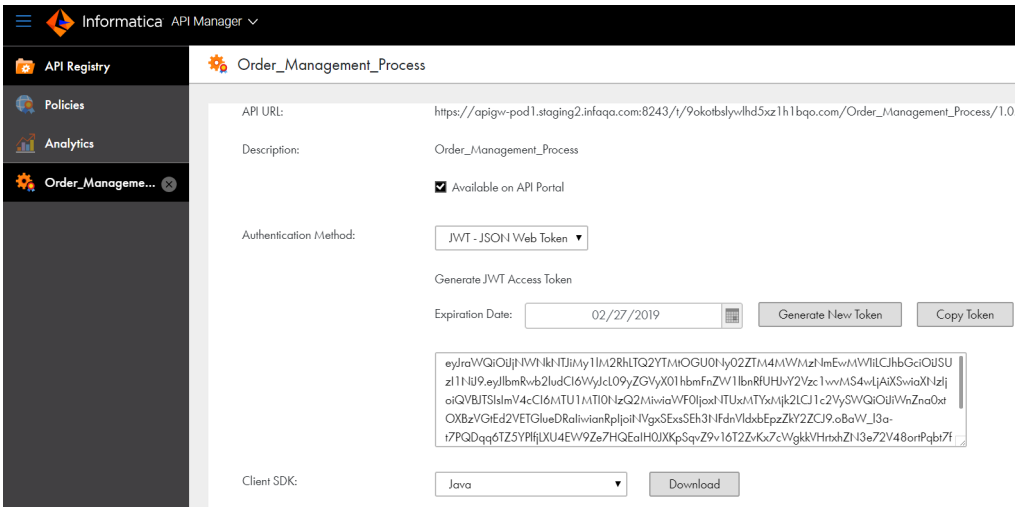
Note: You cannot configure JWT authentication if you select the **Basic** option.

After you select the **JWT - JSON Web Token** option or the **JWT and Basic** option, the **Expiration Date** field and the **Generate** button become available as shown in the following image:



3. Save the changes.
4. Select an expiration date for the token.
5. Click **Generate** to generate a token.

   API Manager creates a token for the managed API as shown in the following image:



Note: After you generate a token for the first time, the **Generate New Token** button appears. You can click this button to generate a new token if your earlier token has expired. After you generate a token, you cannot revoke the token.

6. Click **Copy Token** to copy the token.
7. Optionally, you can click the **Swagger** tab to view the generated Swagger definition.

Note: You cannot view the Swagger definition or WSDL URL from a browser as the browser does not contain the token details.

8. Optionally, you can make the managed API available in API Portal so that API Portal users can discover it in API Portal and invoke it. Click the managed API and verify that the **Available on API Portal** option is selected.

You can then invoke the API based on the authentication method it uses.

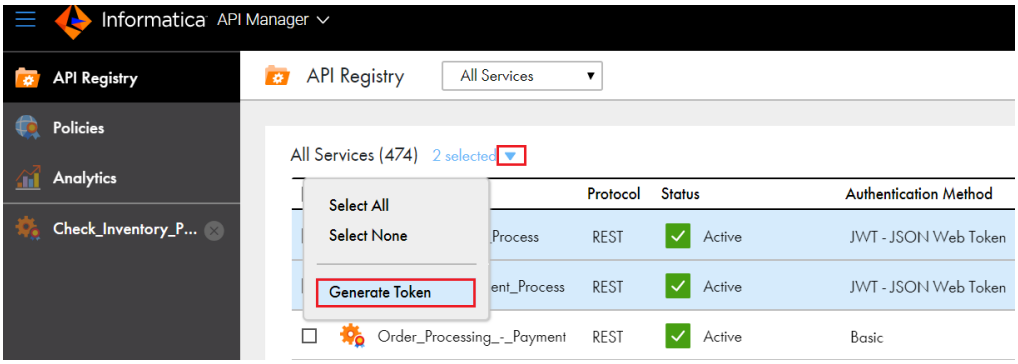
Generating JSON Web Tokens for Multiple Managed APIs Simultaneously

You can generate tokens simultaneously for up to 15 managed APIs that have been configured to accept tokens.

1. On the **API Registry** page, select the managed APIs for which you want to generate tokens.

   Note: All the selected APIs must have the authentication method set to **JWT - JSON Web Token** or **JWT and Basic**. You cannot configure JWT authentication if the authentication method is set to **Basic**.

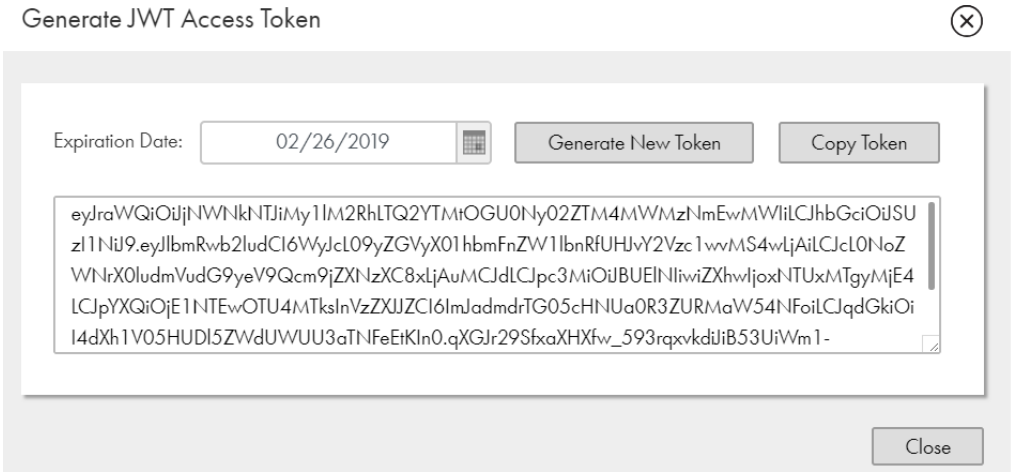
2. Click the down arrow above the list of APIs and select **Generate Token** as shown in the following image:



   The **Generate JWT Access Token** dialog box appears.

3. Select an expiration date for the token.
4. Click **Generate** to generate a token.

   API Manager creates a token for the selected APIs as shown in the following image:



Note: After you generate a token for the first time, the **Generate New Token** button appears. You can click this button to generate a new token if your earlier token has expired. After you generate a token, you cannot revoke the token.

5. Click **Copy Token** to copy the token.

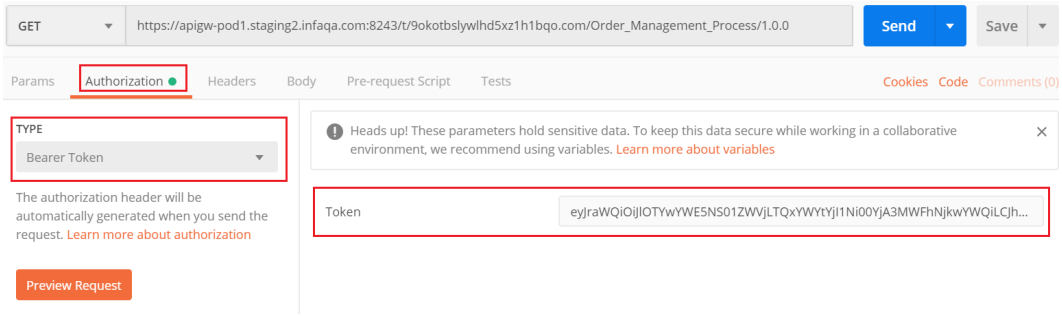
You can then invoke the API based on the authentication method it uses.

API Invocation based on the Authentication Method

You can invoke an API based on the authentication method that it uses.

If a managed API uses the **JWT - JSON Web Token** authentication method, you can invoke the API by passing the token as a bearer token in the HTTP Authorization header.

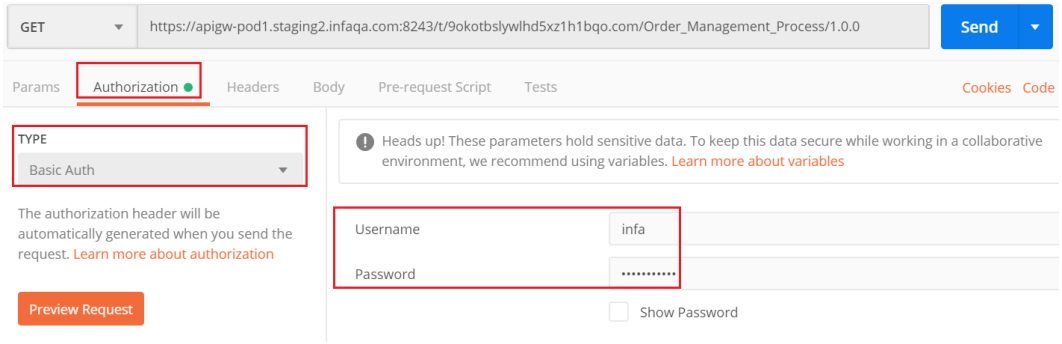
The following image shows an API invoked through Postman with the authorization type set to **Bearer Token** and the token specified:



If a managed API uses the **JWT and Basic** authentication method, you can invoke the API by one of the following methods:

- Passing the token as a bearer token in the HTTP Authorization header
- Providing the login credentials of the allowed user groups or users

The following image shows an API invoked through Postman with the authorization type set to **Basic Auth**, and the user name and password specified:



Managing API Groups

Use the **API Registry** page to add APIs to a group or remove APIs from the group. Use the **API Groups** page to view and edit managed API groups, to generate a JSON web token for the group, or to delete the group.

Adding Managed APIs to a Managed API Group

You can add managed APIs to a new or existing managed API group.

1. In the **API Registry** page, select managed APIs.
   - To add a single managed API to a group select the API, click to open the Actions menu, and select **Add to Group**.
   - To add multiple APIs to a group, select the APIs, click the down arrow above the list of APIs, and select **Add to Group**.

   If there are existing groups the **Add to Group** dialog box appears.
   If there are no existing groups, the **New Group** dialog box appears. Skip to step 3.
2. If there are existing groups, perform the following steps to add the APIs to a group:
   a. Select a group from the **Group Name** list.
   b. Click **Add to Group**.

   API Manager adds the managed APIs to a group.
3. Perform the following steps to add the APIs to a new group:
   a. Click **New Group**.

      The **New Group** dialog box appears.
   b. In the **Name** field enter a group name.
   c. Click **Save**.

Viewing and editing Managed API groups

Use the **API Groups** page to view and edit managed API groups.

The **API Groups** page shows managed API groups in alphabetical order. To sort the groups, click the title of the column to sort. To search for API groups based on specific text, in the **Find** field, type the text by which to search.

To view or edit details of a managed API group, double-click the group name. The **Group Details** window appears and shows the managed APIs in the group in alphabetical order. The following table describes the API attributes that appear in the **Group Details** window.

Property	Description
Name	Name of the managed API.
Protocol	The protocol of the managed API: - REST - SOAP

Property	Description
Status	Status of the managed API: - Active : The managed API is active. - Inactive : The managed API is currently not available. - Service not available : This status indicates a managed API for a service that is unavailable or deleted. If the service for which a managed API has been created is unavailable or deleted, the managed API is greyed out.
Description	Description of the API.

To sort the APIs, click the title of the column to sort. To search for APIs based on specific text, in the **Find** field, type the text to search by.

Generating JSON Web Tokens for Managed API Groups

Use the **API Groups** page to generate JSON web tokens for a managed API group.

The managed API group can contain APIs with any authentication method. You can invoke any JWT or JWT and Basic authenticated managed API that is in the group, using the generated token.

Perform the following steps to generate a token for the group:

1. In the **API Groups** page click to select an API group.
   The **Group Details** window appears.
2. Double-click the group name to view the details.
3. Select an **Expiration Date** for the token.
4. Click **Generate**.

A token is created for the group.

Note: For details of configuring JWT tokens, see "JSON Web Token Authentication for Managed APIs" on page 16.

Deleting a Managed API Group

1. In the **API Groups** page, select a managed API group.
2. Click to open the Actions menu, and select **Delete Group**.
3. Confirm that you want to delete the group

   API Manager deletes the managed API group.

CHAPTER 3

Organization policies

Organization policies are rules that the organization creates to enforce security and access rules on all managed APIs. The organization can enforce IP filtering access policies and determine the rate at which managed API requests can be made.

The IP filtering policy designates the range of computer IP addresses that are allowed to invoke or are denied permission to invoke managed APIs. The rate limiting policy controls the number of times any managed API can be invoked during a designated time period.

In the **Policies** page, you can change the default rate limit policy settings, and add, edit, or delete an IP filtering policy. IP filtering policies are applied according to the order of the policies. The order of the policy determines its precedence.

You can also create a rate limit policy and an IP filtering policy for specific managed APIs. For more information, see "Configuring an API-specific rate limit policy" on page 15 and "Configuring an API-specific IP filtering policy" on page 15.

When an API consumer attempts to access a managed API and is denied due to an IP filtering policy, the HTTP response includes a `403 Forbidden` status code and the description `Invocation is prohibited due to organization policies`.

When an API consumer attempts to access a managed API and access is denied due to a rate limit policy, the HTTP response includes a `429 Too Many Requests` status code and the description `API rate limit reached`.

When an API consumer attempts to access a managed API and is denied due to a rate limit policy or an IP filtering policy, API Manager logs an event in the event log. For more information about the event log, see "Event log" on page 28.

Updating the Rate Limit Policy

You can change the rate limit policy for managed APIs. The rate limit policy controls the number of times a managed API can be invoked during a designated time period, for all the organization's managed APIs. The rate limit rule cannot be deleted, but can be updated. The default rate limit for a managed API is 1000 requests per minute.

- In the **Policies** page, in the Rate Limit Policy panel, enter the number of requests and the number of milliseconds that define the rate limit policy, then click **Update**.

Configuring an IP filtering policy

You can create an IP filtering policy to applies to all the managed APIs in the organization. The IP filtering policy designates the range of computer IP addresses that are allowed or denied permission to invoke managed APIs. The order of the policy rules determines the precedence. The first relevant rules in the rules table is applied to the managed API. You can change the order of the rules by selecting to move them up or down.

1. In the **Policies** page, in the **IP Filtering Policy** panel, select to allow or deny a range of addresses, then fill in the IP range.

   Note: The IP range applies to a Class C network. Only the last octets in the range can differ from each other. Thus the range can contain different client hosts in the same network.
2. Add a description of the policy.
3. Click **Add**.

   API Manager creates an IP filtering policy for all the managed APIs of the organization and adds the policy to the **IP Filtering Rules** list. The order of the rules determines the precedence.
4. To move a policy up or down the list and change the precedence, rest on a row in the table to move and click the Action menu at the right end of the line. From the menu select **Move Up** or **Move Down**.

   The higher the policy is in the list, the higher the precedence.
5. To chance a policy from allowing an IP address range access to denying it access, or from denying access to allowing access, rest on a row in the table to move and click the Action menu at the right end of the line. From the menu select **Change to Deny All** or **Change to Allow All**.
6. To delete a policy, in the right-most column of the IP filtering policy row, rest on a row in the table to move and click the Action menu at the right end of the line. From the menu select **Delete**.

Searching for an IP Filtering Policy

You can search for an IP filtering policy by searching for specific text.

- In the **Policies** page, in the **IP Filtering Policy** panel, in the **Find** field, type the text for which you want to search.

  The IP Filtering Policy table shows the relevant policies.

CHAPTER 4

Analytics

API analytics provide a graphical overview of activity and API usage, as well as the ability to drill down to specific activities and events. The Overview dashboard offers a collection of panels that contain reports about managed APIs. Use the dashboard to view visual summary information about APIs, such as trends in usage over time, APIs with the most invocations, and the most frequent users.

When users invoke API calls, the organization can track general API usage activity for API access instances and access exceptions. The organization may need to track access exceptions to accommodate business or legal needs. API Manager creates an activity log for all API access instances, and an event log to track any access exceptions that users create when invoking managed APIs.

The organization can create IP filtering, rate limiting, basic authentication, and privacy policies. If an API call breaches a policy, API Manager logs the incident in the event log.

Overview Reports

You can use the **Overview** page in the **Analytics** page to view graphical summary information about APIs, including trends in usage over time, APIs with the most invocations, and the most frequent users.

The **Overview** page shows API usage trends for a selected period, for 7, 30, or 90 days. You can refresh the data by clicking the refresh icon. The last time that you refreshed the data is displayed near the icon.

Note: Data from the current day appears after a delay of half an hour.

You can also view the APIs that were most frequently invoked in the selected period, ranked by number of invocations. To sort the display, click the title of the column by which to sort the display.

You can view the users who most frequently invoked APIs in the selected period, ranked by number of invocations. To sort the display, click the title of the column by which to sort the display.

Overview Reports Properties

The following table describes the properties of the Top APIs report in the **Overview** page:

Property	Description
API Name	Name of the managed API.
API URL	Identifies the URL of the managed API that was invoked.

Property	Description
Protocol	Identifies the protocol of the managed API: - REST - SOAP
Invocations	Number of times that the managed API was invoked during the selected period.

The following table describes the properties of the Top Users report in the **Overview** page:

Property	Description
Username	Name of the user who invoked the managed API, if known.
Invocations	Number of times that the user invoked URLs for managed APIs during the selected period.

Activity Log

You can use the **Activity Log** tab in the **Analytics** page to view managed APIs access requests for a selected date range.

The **Activity Log** tab shows API access attempts in chronological order. To sort the access logs, click the title of the column to sort. The last time that you refreshed the data is displayed beside the **Find** field.

Note: The timestamp displayed is based on the local time zone setting of your browser.

Activity Log Properties

The following table describes the **Activity Log** tab properties:

Property	Description
Timestamp	Time that the access occurred. The timestamp displayed is based on the local time zone settings of your browser.
API Name	Name of the managed API.
API URL	Identifies the URL of the managed API that was invoked.
Protocol	Identifies the protocol of the managed API: - REST - SOAP
Method	Identifies the API call method.
HTTP Response	The HTTP response to the managed API invocation.
Username	Name of the user who performed the managed API call, if known.

Property	Description
Consumer IP	Identifies the IP address that accessed the API.
Duration	The duration of access measured from the moment the API request reaches API Manager until the moment API Manager provides a response.

Exporting an Activity Log

You can export an activity log for a managed API.

1. In the **Analytics** page, in the **Activity Log** tab, select a activity log from the API Invocations table.
2. Click the **Export** icon.

   The activity log downloads to your host machine.

Event log

You can use the **Event Log** tab in the **Analytics** page to view policy breaches on managed APIs for a selected date range.

The **Event Log** tab shows the logged incidents in chronological order. To sort the incidents based on a different criterion, click the title of the column by which to sort the display. The last time that you refreshed the data is displayed beside the **Find** field.

Note: The timestamp displayed is based on the local time zone setting of your browser.

Event log properties

The following table describes the **Event Log** tab properties:

Property	Description
Timestamp	Time that the access exception or privacy policy leakage occurred. The timestamp displayed is based on the local time zone of your browser.
API URL	URL of the managed API that was invoked.
HTTP Response	HTTP response to the managed API invocation.
Description	Description of the access exception or privacy policy leakage.
Username	Name of the user who performed the managed API call, if known.
Consumer IP	IP address of the host machine that created the access exception or privacy policy leakage.

Exporting an event log

You can export an event log for a managed API.

1. In the **Analytics** page, in the **Event Log** tab, select an event log from the API Access Exceptions table.
2. Click the **Export** icon.

   The event log downloads to your host machine.

Searching for a log

You can search for an event or activity log by date of creation or by searching for specific text in the display columns.

1. To search for logs that were created during a specific time period, in the relevant tab, select a range of dates in the **Select date range** fields, and then click **Show Log**. Ensure that you select dates based on the local time zone setting of your browser.

   Logs for the selected time period are displayed.
2. To sort the logs according to a specific property, click the column picker icon to the left of the **Find** field and then select the column by which to sort the logs.
3. To search for logs based on specific descriptive text, in the **Find** field, type the text for which to search.

   The log table shows the relevant logs.

INDEX

A

activity log
  API access 27
  view 27
Activity Log
  properties 27
Administration
  description 8
Analytics
  API access 26
  description 26
  overview 26
API domain name
  description 6
API Manager
  API Registry page 9
  description 5
API Registry page
  description 9
  properties 10
authentication overview
  API Manager 6, 9
  Managed APIs 6, 9

C

custom URLs
  API Manager 6, 9
  Managed APIs 6, 9

E

event log
  API access exceptions 28
event log *(continued)*
  privacy policy leakages 28
  view 28
Event Log tab
  properties 28

J

JWT authentication
  configuring 18
  generating tokens 18
  generating tokens simultaneously for multiple APIs 20
  invoking an API 21
  overview 16
  prerequisites 18
  tasks 17
  token expiration 18

O

organization policies
  description 24
Overview Reports
  properties 26

R

registration
  description 7