



Informatica® API Center
October 2025

Introducing API Center

Informatica API Center Introducing API Center
October 2025

© Copyright Informatica LLC 2022, 2025

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

Informatica, Informatica Cloud, Informatica Intelligent Cloud Services, PowerCenter, PowerExchange, and the Informatica logo are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at <https://www.informatica.com/trademarks.html>. Other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties. Required third party notices are included with the product.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2025-10-03

Table of Contents

- Preface 4**
- Chapter 1: Introducing API Center..... 5**
 - API Center user roles. 6
 - API Center tools 7
 - Explore page. 7
 - API Policies page. 8
 - API Console page. 9
 - API Groups page. 9
 - API Monitor page. 9
 - My Import/Export Logs page. 9
 - Configuration page. 9
- Index..... 13**

Preface

Read *Introducing API Center* to learn about Informatica Intelligent Cloud Services™ API Center. You can use API Center to design, manage, and monitor the APIs in your organization.

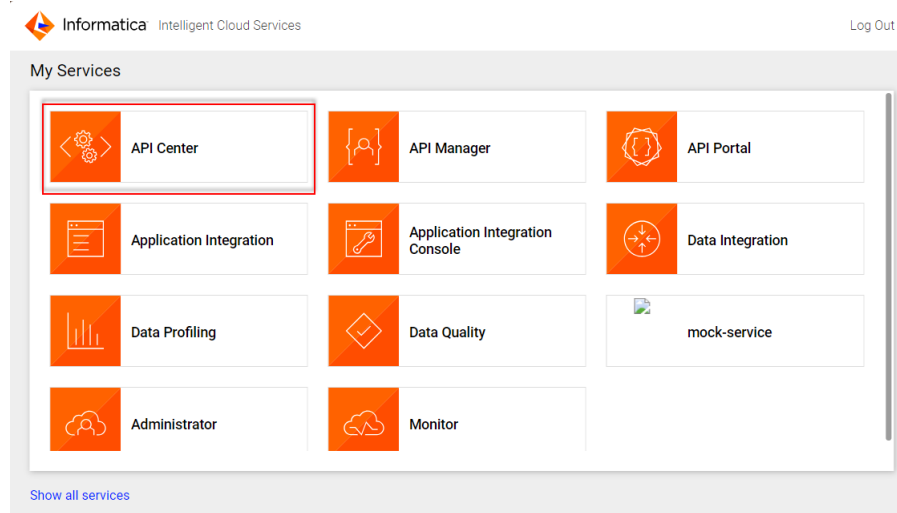
CHAPTER 1

Introducing API Center

API Center is a service in Informatica Intelligent Cloud Services™ that you can use to design, publish, manage, and monitor APIs in the organization. You can provide API consumers with access to the APIs for enterprise services and processes that you create with API Center.

When you log in to Informatica Intelligent Cloud Services, the **My Services** page displays the API Center service and services that apply to API Center. The **My Services** page might also include other services that you subscribe to and trial versions of other services.

The following image shows the **My Services** page:



You can choose the domain name when you log in to API Center the first time, and then provision the domain. For more information about, see [“API domain name” on page 10](#).

Use API Center to perform the following tasks:

Create REST APIs

To create and define REST APIs, you can create API operations or import existing API definitions.

Assign API policies to APIs and API operations

You can create policies and assign them to APIs and to API operations. Policies are rules that you use to enforce API security and control access to APIs.

Publish APIs

You create a published API using either a top-down approach or a bottom-up approach. Using the top-down approach, you can create a REST API with at least one operation and then publish the API. Using the bottom-up approach, you can create a published API from an existing Application Integration process.

Group APIs

API groups are collections of APIs that organization administrators and developers can consume. You can group your published REST APIs across your organizational and business boundaries by adding them to API groups. You can then share the API group endpoint URLs with API consumers so that they can easily access the related operations in a managed API group.

Manage APIs

You create managed APIs from published APIs. You can then share the API endpoint URLs with API consumers so that they can access the operations of the managed APIs.

Monitor API usage

You can view and monitor the invocations of managed APIs in the organization.

API Center user roles

A role is a collection of privileges that you can assign to users. To ensure that every user can access assets and perform tasks in an organization, assign at least one role to each user.

API Center uses pre-defined roles to define access privileges for different types of assets and service features. For example, users with the Designer role can create assets, but don't have access to the **API Console** page and to policies.

You can assign the following types of roles to API Center users in Administrator:

API Center Role	Role Name Mapping	Access Privileges
API Administrator	Admin	Has full access to the service, including all asset privileges, and can provision tenants. Can access the following pages: <ul style="list-style-type: none">- New Asset- Explore- Policies- API Console- Import/Export- API Monitor- Configuration
API Deployer	<ul style="list-style-type: none">- Deployer- Service Consumer	Can view and deploy assets, provision tenants, assign policies, manage organization settings, and add OAuth 2.0 clients when assigned with the Service Consumer role. Can access the following pages: <ul style="list-style-type: none">- Explore (read-only)- API Console- Configuration Deployer can also create a published API from the Services tab in the API Console page.

API Center Role	Role Name Mapping	Access Privileges
API Designer	<ul style="list-style-type: none"> - Designer - Service Consumer 	Has full access to all asset privileges and can assign policies when assigned with the Service Consumer role. Can access the following pages: <ul style="list-style-type: none"> - New Asset - Explore - Import/Export
API Monitor	Monitor	Can monitor assets and view API invocation logs. Can access the following pages: <ul style="list-style-type: none"> - Explore (read-only) - API Monitor
API Policy Manager	API Policy Manager	Can define policies and access the following pages: <ul style="list-style-type: none"> - Explore (read-only) - Policies - Import/Export

You can create and configure individual user accounts to allow access to your organization on the **Users** page in Administrator. You can create groups of users that can perform the same tasks on the **User Groups** page in Administrator.

API Center tools

API Center provides the following tools that you can use to satisfy your business needs:

- Explore page
- Policies page
- API Console page
- API Groups page
- API Monitor page
- My Import/Export Logs page
- Configuration page

Explore page

Use the **Explore** page to work with your API Center projects and assets.

Finding projects and assets on the Explore page

Use any of the following methods to find your projects and assets on the **Explore** page:

- Explore by projects and folders. View all projects or select a particular project.
- Explore by asset types. View all assets or view assets of a particular type.
- Explore by tags. View assets associated with a particular tag.

- Search for projects or assets. To search all projects, folders, and assets in the organization, view the **Explore** page by **All Projects**, and then enter a name or description in the Find box. Or, to narrow your search, in the **Find** box, enter a name or description in full or part.
- Sort the search results. Sort the **Explore** page by name, asset type, last update date, create date, or description.
- Filter the objects on the page. To filter objects, click the **Filter** icon. To apply a filter, click **Add Filter**, select the property to filter by, and then enter the property value. The filters available depend on how you view the page. You can specify multiple filters.

You can see projects, folders, and assets for all of the services that you use. If you select an Application Integration process to open or to perform an action, the Application Integration service opens in a new browser tab.

Working with projects and assets on the Explore page

Perform actions on projects, folders, and assets on the **Explore** page. To see what actions you can perform on an object, in the row that contains the object, click the **Actions** icon.

The Actions menu lists the actions you can perform based on your user role privileges and the permissions specified for the selected object. For example, your user role might have privileges to view objects, but not to edit and delete objects.

You can also delete multiple objects at one time. Select the check box to the left of each object, or select the Select All check box to select all of the objects that are displayed on the current page. After you select the objects, click **Actions** in the row of any of the selected objects and then click **Delete**.

Alternatively, you can use the Selection menu to choose the action.

Customizing the Explore page

You can display or hide columns on the **Explore** page. To display or hide columns, right-click the column heading area and select or clear the column headings in the list. The headings in the list depend on whether projects, assets, or tags are in view on the **Explore** page.

Importing assets

You can import all or selected assets from an export file into your chosen projects, deciding whether to overwrite existing assets and merge tags in case of name conflicts. To import assets, ensure your user role has the necessary privileges and permissions, including create, update, and read rights depending on whether you add new assets or overwrite existing ones. Use the **Import Assets** page to view, select, and assign assets to projects, creating new projects in the target organization automatically if needed.

API Policies page

API policies are rules that you can create to enforce API security and control access to APIs.

You can use API Center to define and assign different types of policies, such as IP filtering, security policies, operational policies, and privacy policies.

You can choose to export individual assets, entire projects, or folders. To export assets, your user role must have export privileges.

API Console page

Use the **API Console** page to view the published APIs and managed APIs in your organization.

The **API Console** page includes the following tabs:

- **Services.** Lists all the processes that you published in Application Integration. You can use the **Services** tab to create published APIs.
- **Published APIs.** Displays the published APIs in your organization. You can use the **Published APIs** tab to create managed APIs, view published APIs detail and history, unpublish published APIs, and publish custom APIs.
- **Managed APIs.** Displays the managed APIs in your organization. You can use the **Managed APIs** tab to view, edit, test, activate, share, deprecate, deactivate, and delete managed APIs. You can generate JWT tokens and manages contacts of managed APIs. You can also copy the endpoint URLs for API operations, and download the API specification for a managed API, and send it to API consumers.

API Groups page

Use the **API Groups** page to view the API groups and managed API groups in your organization.

The **API Groups** page includes the following tabs:

- **API Groups.** Lists the published API groups in your organization. You can use the **Create API Group** to add more groups.
- **Managed API Groups.** Displays the managed API groups in your organization. You can use the **Managed API Groups** tab to edit, view, activate, and delete managed API groups. You can generate JWT tokens to override all other authentication policies applied to the APIs in a particular managed API group. You can also download the API specification for a managed API group, and send it to API consumers.

API Monitor page

Use the **API Monitor** page to monitor the invocations of managed APIs in your organization.

The **API Monitor** page displays details of the API invocations according to the time frame you select. You can download the details as a ZIP file from the page.

My Import/Export Logs page

Use the **My Import/Export Logs** page to view and track the history of your import and export jobs.

This page provides detailed logs of your import and export jobs, including their status, timestamps, and any errors or warnings encountered during the process. Use this page to efficiently monitor and troubleshoot your data migration and asset transfer tasks within the organizations.

Configuration page

Use the **Configuration** page to configure third-party authentications, OAuth 2.0 clients, the organization response timeout, change your domain name, and use a vanity domain name of your choice for the organization domain.

The **Configuration** page includes the following tabs:

- **Third-party Authentication.** You can leverage external identity providers, such as Okta or Azure Active Directory (AAD), to handle user authentication and authorization processes.

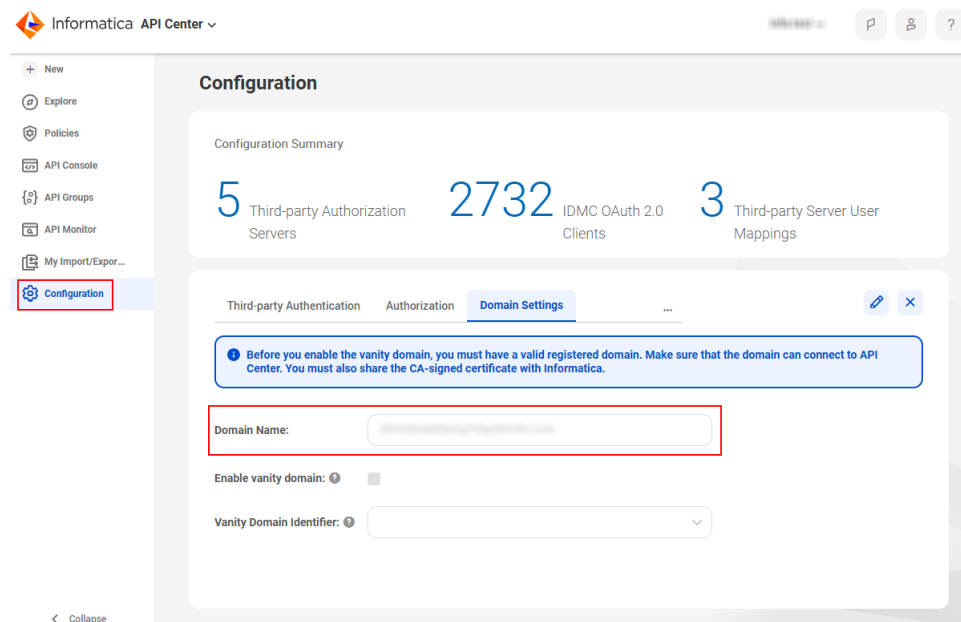
- **Authorization.** Displays the OAuth 2.0 clients in your organization and the third-party server user mappings. You can use the **Authorization** tab to do the following:
 - Create and manage OAuth 2.0 clients. You can also download an OAuth 2.0 clients list and copy the access token URL to send to API consumers.
 - Define user permissions for authorization server of third-party identity providers.
- **Organization Settings.** You can use the **Organization Settings** tab to configure the organization response timeout for API requests. You must enter a timeout value from 1 through 180 seconds. Operation response timeouts take precedence over the organization response timeout.
- **Domain Settings.** Displays the **Domain Name** and the option to enable a vanity domain name for your domain.
- **Domain IP Filtering.** You can use the **Domain IP Filtering** policy to manage IP-based access control for all managed APIs, managed API groups, and custom APIs within your organization. This policy defines access rules that either allow or deny IP addresses permission to invoke any API in your organization.

API domain name

The API domain name identifies the organization and is used in the URLs created for the managed APIs of an organization. You can also use a sub-domain of the organization domain.

When you access API Center for the first time, API Center automatically provisions an organization.

The default format of the API domain name is the `<organization ID.com>`. You can change the domain name on the **Domain Settings** tab on the **Configuration** page as shown in the following image:



Edit the domain name to enter a name of your choice. After you change the domain name, all existing managed API URLs are seamlessly updated with the new domain name. Any new managed API created after the API domain name change will have the new domain name.

Domain name sample URL

A managed API URL has the following format.

```
{protocol}://{Informatica_URL}/{domain_name}/{context}/{api_version}/{operation_path}
```

Consider that your organization API domain is `myorg.com`, and the given operation path is `Customers`. When you change the API domain name, the managed API URL changes to the following API URL format:

`https://na1.dm-us.informaticacloud.com/myorg.com/urlcontext/v1/Customers`

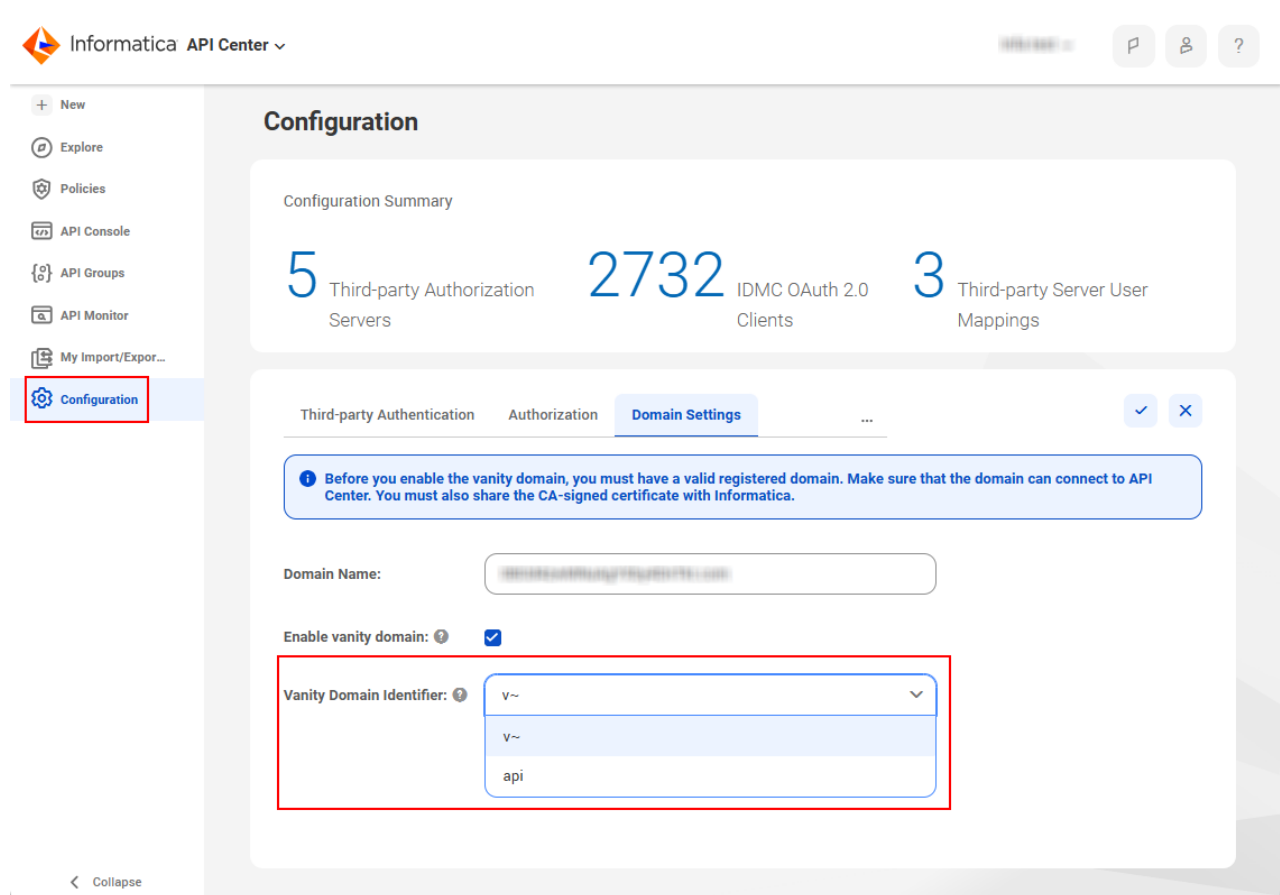
Vanity domain

Use a vanity domain to personalize your API Center domain name and URL, and enhance your personal brand, user experience, and the accessibility of the domain.

A vanity domain is a personalized domain name that you can choose to reflect your particular brand, product, or service. Using a vanity domain makes it easier for visitors to remember your domain name and to be redirected to your primary website, facilitating repeated visits to the site.

Before enabling the vanity domain, you must possess a valid registered domain. Ensure that the domain can connect to API Center. You must also share the CA-signed certificate with Informatica. After you enable the vanity domain for your APIs, all API URLs will be dynamically changed to the vanity domain API URL format. However, redeployment of the APIs is not necessary after enabling the vanity domain. Contact [Informatica Global Customer Support](#) if you want to enable a vanity domain.

You can enable a vanity domain for your organization on the **Domain Settings** tab on the **Configuration** page. The following image shows the option to enable a vanity domain in API Center:



Complete the following steps to enable a vanity domain:

1. On the **Domain Settings** tab, click the edit button on the right-hand side of the tab.
2. Optionally, add a domain name of your choice.

3. Enable the vanity domain option to personalize your API Center domain name and URL.
4. Select the vanity domain identifier. After you enable this option, the API URL uses one of the following formats based on your selection:
`https://YourDomainName.com/v~/context/v1/...`
`https://YourDomainName.com/api/context/v1/...`
Default is `v~`.
5. Save the changes for the domain settings to take effect.

Vanity domain URL example

After you enable the vanity domain option, the vanity domain uses the following format:

`{protocol}://{domain_name}/v~/context/{api_version}/{operation_path}`

For example, consider the following managed API URL:

`https://na1.dm-us.informaticacloud.com/myorg.com/urlcontext/v1/Customers`

After you enable the vanity domain, the managed API URL changes to the following format:

`https://myorg.com/v~/urlcontext/v1/Customers`

Here, `v~` denotes that the domain name uses a vanity domain name.

You can't use the **Test Managed API** option to test a managed API or its operations on a vanity domain URL. Use the following URL format to check if your vanity domain can connect to API Center:

`https://myorg.com/v~`

INDEX

A

Actions menu [Z](#)
assets [Z](#)

E

Explore page [Z](#)

F

filtering [Z](#)

finding assets and projects [Z](#)

P

project folders [Z](#)
projects [Z](#)

S

searching for assets and projects [Z](#)