



Informatica® API Center
October 2025

What's New

© Copyright Informatica LLC 2023, 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 5**
 - Informatica Resources. 5
 - Informatica Documentation. 5
 - Informatica Intelligent Cloud Services web site. 5
 - Informatica Intelligent Cloud Services Communities. 5
 - Informatica Intelligent Cloud Services Marketplace. 5
 - Data Integration connector documentation. 6
 - Informatica Knowledge Base. 6
 - Informatica Intelligent Cloud Services Trust Center. 6
 - Informatica Global Customer Support. 6
- Chapter 1: October 2025..... 7**
 - New features and enhancements. 7
 - Changed behaviors. 8
- Chapter 2: July 2025..... 9**
 - Important notices. 9
 - New features and enhancements 9
 - Changed behaviors. 10
- Chapter 3: May 2025..... 12**
 - New features and enhancements. 12
 - Changed behaviors. 13
- Chapter 4: April 2025..... 14**
 - New features and enhancements. 14
 - Changed behaviors. 16
- Chapter 5: November 2024..... 17**
 - Changed behaviors. 17
- Chapter 6: October 2024..... 18**
 - New features and enhancements. 18
 - Changed behaviors. 18
- Chapter 7: August 2024..... 20**
 - New features and enhancements. 20
- Chapter 8: July 2024..... 21**
 - New features and enhancements. 21

Changed behaviors.	22
Index.	23

Preface

Read *What's New* to learn about new features, enhancements, and changed behaviors in API Center for the October 2025 release.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit <https://docs.informatica.com>.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Intelligent Cloud Services web site

You can access the Informatica Intelligent Cloud Services web site at <http://www.informatica.com/cloud>. This site contains information about Informatica Cloud integration services.

Informatica Intelligent Cloud Services Communities

Use the Informatica Intelligent Cloud Services Community to discuss and resolve technical issues. You can also find technical tips, documentation updates, and answers to frequently asked questions.

Access the Informatica Intelligent Cloud Services Community at:

<https://network.informatica.com/community/informatica-network/products/cloud-integration>

Developers can learn more and share tips at the Cloud Developer community:

<https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers>

Informatica Intelligent Cloud Services Marketplace

Visit the Informatica Marketplace to try and buy Data Integration Connectors, templates, and mapplets:

<https://marketplace.informatica.com/>

Data Integration connector documentation

You can access documentation for Data Integration Connectors at the Documentation Portal. To explore the Documentation Portal, visit <https://docs.informatica.com>.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit <https://search.informatica.com>. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Intelligent Cloud Services Trust Center

The Informatica Intelligent Cloud Services Trust Center provides information about Informatica security policies and real-time system availability.

You can access the trust center at <https://www.informatica.com/trust-center.html>.

Subscribe to the Informatica Intelligent Cloud Services Trust Center to receive upgrade, maintenance, and incident notifications. The [Informatica Intelligent Cloud Services Status](#) page displays the production status of all the Informatica cloud products. All maintenance updates are posted to this page, and during an outage, it will have the most current information. To ensure you are notified of updates and outages, you can subscribe to receive updates for a single component or all Informatica Intelligent Cloud Services components. Subscribing to all components is the best way to be certain you never miss an update.

To subscribe, on the [Informatica Intelligent Cloud Services Status](#) page, click **SUBSCRIBE TO UPDATES**. You can choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

Informatica Global Customer Support

You can contact a Global Support Center through the Informatica Network or by telephone.

To find online support resources on the Informatica Network, click **Contact Support** in the Informatica Intelligent Cloud Services Help menu to go to the **Cloud Support** page. The **Cloud Support** page includes system status information and community discussions. Log in to Informatica Network and click **Need Help** to find additional resources and to contact Informatica Global Customer Support through email.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at <https://www.informatica.com/services-and-training/support-services/contact-us.html>.

CHAPTER 1

October 2025

The October 2025 release of API Center includes the following updates.

New features and enhancements

The October 2025 release of API Center includes the following new features and enhancements.

[Export and import assets](#)

You can now export API Center assets, such as, APIs and policies, from an organization and import them into another organization. This enhancement gives you the flexibility to transfer assets across organizations without needing to re-create them.

For more information, see *Asset Management*.

[View asset dependencies](#)

You can view object dependencies for an asset. You can view the objects that the selected asset uses and the objects that use the selected asset.

You might want to view object dependencies before performing certain operations on an asset. For example, you can't delete an asset if another object depends on the asset.

For more information, see *Asset Management*.

[Domain-level 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.

For more information, see *API Policies*.

[New Consumer column added to the Activity Log tab on the API Monitor page](#)

The **Activity Log** tab on the **API Monitor** page now includes a new column named **Consumer**. Using the **Consumer** column, you can get insights into the users who invoked the APIs.

For more information, see *Monitor APIs*.

Changed behaviors

The October 2025 release of API Center includes the following changed behaviors.

Editing policies of active managed APIs and managed API groups

You can now update the policies of your managed APIs and managed API groups that are in the active, shared, and deprecated state.

Previously, to edit a managed API's policies, you had to deactivate it, causing token invalidation and downtime.

For more information, see *Manage APIs*.

CHAPTER 2

July 2025

The July 2025 release of API Center includes the following updates.

Important notices

The July 2025 release of API Center includes the following important notice:

Preview initiated

Effective in the July 2025 release, import of Data Quality rule specifications directly into API Center is available for preview. All Data Quality operations must use a session ID based authentication policy.

For more information, see *REST API Assets*.

Preview functionality is supported for evaluation purposes but is unwarranted and is not supported in production environments or any environment that you plan to push to production. 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.

New features and enhancements

The July 2025 release of API Center includes the following new features and enhancements.

New session ID authentication method

You can assign the new session ID authentication method to APIs and operations. If you create an API by importing a Data Quality asset, use only the session ID authentication method.

For more information, see *API Policies*.

Ability to view published API details

If you are assigned the Admin or Deployer role, you can view and verify the details of a published API before you create a managed API from it. You can view the API-level rate limit policies and operation-level policies in read-only mode. You can view the API-level security and privacy policies under the operational-level policies if the operational-level policies inherit the API-level policies.

You can view the details of the following types of published APIs:

- REST APIs that were published using the top-down approach or bottom-up approach

- SOAP APIs that were published using the bottom-up approach
- Custom REST and SOAP APIs

For more information, see *Manage APIs*.

Changed behaviors

The July 2025 release of API Center includes the following changed behaviors.

OAuth 2.0 security authentication for API groups

When you create or edit an API group or managed API group, you can enable OAuth 2.0 authentication at the API group level. You can then invoke the APIs in the managed API group with OAuth 2.0 or third-party authorization access tokens.

When you enable API-level authentication for an API group, all the operation-level authentications are overridden. However, this behavior doesn't apply to custom API operations.

Previously, you couldn't enable OAuth 2.0 authentication at the API group level. You could enable OAuth 2.0 authentication only at the operation level.

For more information, see *Manage APIs*.

Naming convention changes

To include OAuth 2.0 authentication at the API group level, a field has been renamed as described in the following table:

Page or Tab Name	Old Field Name	New Field Name
API Groups page > API Groups tab > <Create or edit an API group> > Policies tab	JWT Access Token	Security
API Groups page > Managed API Groups tab > <Create or edit a managed API group> > Policies tab	JWT Access Token	Security

For more information, see *Manage APIs*.

Inclusion of query parameters in managed and custom managed API endpoint URLs

When your REST API operation endpoint includes query parameters, API Center now automatically displays the complete endpoint URL with those parameters for both managed APIs and custom managed APIs. This enhancement ensures consistency between your endpoint definitions and query parameter configurations.

In a managed API, you can use the following formats for query parameters:

- Query key (?param)
- Query key with equals (?param=)
- Query key and value (?param=value)

In a custom managed API, you can use the following format for a query parameter:

Query key and value (?param=value)

Previously, query parameters were not displayed in the managed API endpoint URL, even when they were defined during the creation of the managed API.

For more information, see *Manage APIs*.

[Distinct tabs for APIs and API groups while configuring OAuth 2.0 clients and defining user permissions for third-party authentication](#)

When you configure an OAuth 2.0 client or third-party user permission, you'll now see the managed APIs and managed API groups categorized under the following tabs:

- Managed APIs
- Managed API Groups

With this enhancement, the APIs are now organized into distinct tabs, making it easier to locate and interact with the specific resources you need.

Previously, you could view both API types in a single, combined view requiring you to scroll to reach the next section. This made navigation inefficient and time-consuming.

For more information, see *Manage APIs*.

CHAPTER 3

May 2025

The May 2025 release of API Center includes the following updates.

New features and enhancements

The May 2025 release of API Center includes the following new features and enhancements.

[Federated or third-party authorization server support with OAuth server 2.0](#)

You can implement OAuth 2.0 authentication using federated or third-party providers such as, Okta and Azure AD, to secure your APIs effectively. This configuration enhances API security by leveraging external OAuth identity providers. You can streamline the authentication process, making it easier for developers to integrate secure access controls.

You can enable your API consumers to access protected resources using tokens generated from their preferred OAuth provider without pre-provisioning all API consumers through the IDMC identity provider.

For more information, see *API Policies*.

[Custom SOAP API support](#)

You can create, manage, and govern unique custom SOAP APIs that aren't based on Informatica service endpoints. The API URL that you specify must conform to the W3C standards.

For more information, see *Manage APIs*.

[API groups and Managed API groups for SOAP and custom APIs](#)

You can categorize published SOAP and custom APIs and their operations into logical API groups to easily manage the APIs in your organization. To create an API group, you must be assigned the Deployer or Admin role.

You can create subsequent managed API groups from an API group. You can add a URL context to a managed API group, create an IP filtering policy for a managed API group, and generate a JSON web token for a group of managed APIs. You can assign a rate limit policy to a managed API group.

For more information, see *Manage APIs*.

Changed behaviors

The May 2025 release of API Center includes the following changed behaviors.

Ability to edit API-level JSON web token of a managed API group

You can now add or remove an associated JSON web token authentication from a managed API group if the managed API group is in the created or inactive state.

Previously, after you created a managed API group that contained an API-level JSON web token, you couldn't add or remove the API-level JSON web token authentication. If you wanted to add or remove a JSON web token authentication, you had to create a new managed API group again.

Ability to edit the context of a managed API or a managed API group

You can now edit the context of a managed API or a managed API group if the managed API or the managed API group are in the created or inactive state.

Previously, you couldn't change the context of a managed API or a managed API group after you created it.

New keyword for vanity domain identifier

When you enable a vanity domain to personalize your API Center domain name and URL, you can now use `v~` and `api` as the vanity domain identifiers in the URL.

Previously, you used only `v~` as the vanity domain identifier in the URL.

Increase in API policy description length

You can now enter 512 characters in the **Description** field of all API Center policies.

Previously, you could enter only 255 characters in the `Description` field of all API Center policies.

Increase in API operation description length at design time

You can now enter 4000 characters for an API operation description when you create a REST API.

Previously, you could enter only 1025 characters for an API operation description.

CHAPTER 4

April 2025

The April 2025 release of API Center includes the following updates.

New features and enhancements

The April 2025 release of API Center includes the following new features and enhancements.

Real-time monitoring of APIs

You can gain real-time visibility into API health, including response times, latency, errors, and traffic. Additionally, you can access detailed analytics on API usage patterns, user behavior, and performance trends over time. You can use this data to optimize API operations, identify bottlenecks, and ensure compliance effectively.

API Center now provides various visual charts to help you.

For more information, see *Monitor APIs*.

Enhanced OAuth 2.0 support

You can now assign multiple managed APIs and managed API groups to a single OAuth 2.0 client. This improvement enhances API security and management by eliminating the need for multiple OAuth 2.0 clients. You can create a single OAuth 2.0 client to grant access to specific API sets, simplifying authorization control.

With this enhancement, disabling or deleting an OAuth 2.0 client will immediately invalidate its authorization token, preventing API access and enhancing security.

For more information, see *API Policies*.

Import of Application Integration processes to API Center

You can import all the Application Integration processes to API Center. The processes on the **Service Name** corresponds to the **API Name** and the **Source Name** corresponds to the **Name** in Application Integration.

This import capability helps you easily transition the REST APIs of published Application Integration processes into API Center. You can easily design, publish, and create managed APIs in API Center.

For more information, see *REST API Assets*.

Multibyte character support

You can use multibyte characters, including Japanese characters for the following API Center fields:

- Operation name

- API name
- Published API name
- Managed API name
- Policy name
- OAuth client 2.0
- Context
- API group name
- Managed API group name
- Custom API name
- Projects
- Application Integration process

For more information, see *Manage APIs*.

Date and Date Time data type support

When you define the request and response body of an API operation, you can select the Date and Date Time data types. You can also create an array type of the Date and Date Time data types.

Ability to edit operation policies in API groups

You can edit policies that are in created and inactive states of a Managed API group. Editing such policies enables you to reuse API groups with the same operations while applying different policies and context names.

You can reuse the same operation in multiple APIs with an API group but assign different policies and context names to the operations

You can also attach different policies to different operations when creating active managed API groups and hence ensures that you can reuse Published APIs directly from the API Console.

For more information, see *Manage APIs*.

API-level rate limit policy at operation level for API groups

If you associate an API-level rate limit policy with an API, but do not assign policies to individual API operations, the API-level rate limit policy is automatically applied to the operations when you add the published API operation to an API group. The active managed API groups will also enforce the applied rate limit.

This enhancement does not apply to the existing operations you previously added to a managed API group.

For more information, see *Manage APIs*.

Support for octet-stream content type

API Center now stores API responses that contain content types such as multipart/form-data and application/octet-stream. These new content types apply only when you include the file datatype in the request and response body fields during REST API creation.

Previously, API Center stored only application/json and XML content types.

For more information, see *REST API Assets*.

Array data type support in path and query parameters of an API operation

When you define the path and query parameters of an API operation, you can select the array type of the primitive data types. You can pass multiple values in the CSV format as default values for query parameters.

For more information, see *REST API Assets*.

Changed behaviors

The April 2025 release of API Center includes the following changed behaviors.

Automated domain provisioning

API Center now automatically provisions a domain with the default domain as `<organization ID.com>`. Automatic provisioning of a domain doesn't depend on your user role.

You can change the domain name on the **Domain Settings** tab on the **Configuration** page.

Previously, when you access API Center for the first time with the Admin or Deployer, you were prompted to select an API domain name and provision the domain. If the domain provisioning failed, you couldn't access API Center.

For more information, see *Introducing API Center*.

Support for multiple HTTP response codes

When you import an API definition with multiple response codes, you can view all the response codes on the **Response** tab of the operation panel. You can edit the response codes.

Previously, you could see only the one response code.

For more information, see *Introducing API Center*.

Conflict resolution during import of API definition

When you import an API definition with duplicate operation names, API Center adds the imported assets without replacing the existing assets. API Center doesn't show conflicts during import, but validates the unique endpoints when you publish the API.

Previously, when you imported a duplicate operation, the existing operation was replaced by the new operation.

For more information, see *REST API Assets*.

Synchronization of request and response between Application Integration and API Center

After you generate a new process in API Center and publish the API, the changes reflect in Application Integration. When you update the **Input Mapping** or **Output Mapping** fields in Application Integration and publish the process, the data synchronizes in API Center. Refresh the mapping in the process **Implementation** tab in API Center to view the synchronized data between Application Integration and API Center. The updates appear in the **Request** and **Response** tabs in API Center.

Previously, you updated and refreshed every field in API Center manually. Also, the **Transformation** section in the **Implementation** tab is removed as the data synchronizes automatically with each refresh.

For more information, see *REST API Assets*.

CHAPTER 5

November 2024

The November 2024 release of API Center includes the following updates.

Changed behaviors

The November 2024 release of API Center includes the following changed behaviors.

Custom time frame to view API invocation details

You can now view the API invocation details for a custom time frame. You can retrieve API detail logs for a maximum of 30 days.

Previously, you could select only one of the following pre-defined time frame values:

- Last 1 hour
- Last 2 hours
- Last 3 hours
- Last 4 hours

For more information, see *Manage APIs*.

New filters for published APIs and managed APIs

On the **Managed APIs** tab, you can now filter the managed APIs based on the **Context Name** field and **Managed API Name** field in addition to the existing **Published API Name** filter.

For more information, see *Manage APIs*.

New filters for viewing API activity logs

On the **API Monitor** tab, you can filter the API activity logs based on the **Provider**, **IP Address**, and **Duration** fields in addition to the existing **API Context** and **Method** filters.

For more information, see *Manage APIs*.

CHAPTER 6

October 2024

The October 2024 release of Informatica Intelligent Cloud Services™ API Center includes the following updates.

New features and enhancements

The October 2024 release of API Center includes the following new features and enhancements.

[Unpublish an API](#)

You can unpublish an API that was published using a top-down approach or a bottom-up approach. You can also unpublish a custom API or any API published through an Application Integration process. If you no longer need a published API, you can unpublish the API and permanently delete the unpublished API from API Center.

The API that you want to unpublish must not contain any managed API in created, active, shared, deprecated, or inactive state.

Unpublishing an API doesn't impact any API group.

For more information, see *Manage APIs*.

[Cross-origin Resource Sharing \(CORS\) policy](#)

You can define a cross-origin resource sharing (CORS) policy and associate the CORS policy with a CORS group. You can specify the allowed origins, HTTP methods, and headers that require CORS support.

CORS support helps API providers to control the invoking of the managed APIs and managed API groups.

For more information, see *API Policies*.

Changed behaviors

The October 2024 release of API Center includes the following changed behaviors.

[Dynamically update the path parameter and query parameter values of a custom managed API](#)

When you create and activate a custom managed API, you can choose to dynamically change the path parameter and query parameter values.

Previously, you could provide an absolute URL for each path parameter or query parameter. Thus, you had to create multiple custom APIs with the same URL with different path parameters and query parameters.

For more information, see *Manage APIs*.

CHAPTER 7

August 2024

The August 2024 release of API Center includes the following update.

New features and enhancements

The August 2024 release of API Center includes the following new feature and enhancement.

[API Groups and Managed API Groups](#)

You can categorize published REST APIs and operations into logical API groups to easily manage the APIs in your organization. To create an API group, you must be assigned the Deployer or Admin role.

You can create subsequent managed API groups from an API group. You can add a URL context to a managed API group, create an IP filtering policy for a managed API group, and generate a JSON web token for a group of managed APIs. You can assign a rate limit policy to a managed API group.

For more information, see *Manage APIs*.

CHAPTER 8

July 2024

The July 2024 release of Informatica Intelligent Cloud Services™ API Center includes the following updates.

New features and enhancements

The July 2024 release of API Center includes the following new features and enhancements.

Vanity domain

You can enable 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. After you enable this option, the vanity domain uses the following format:

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

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 dynamically include the vanity domain name. 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.

For more information, see *Introducing API Center*.

User-level rate limit policy

When you create a managed API, you can associate a user-level rate limit policy with a managed API to control the number of times a specific API consumer can access an API and its operations within a designated timeframe. In a specific organization, you can associate an active user with only one user-level rate limit policy.

You can configure a user-level rate limit policy only after you migrate to the new API gateway.

For more information, see *API Policies*.

SOAP APIs

In addition to the REST APIs for the Application Integration processes, you can now see the SOAP APIs also in API Center. Use the **Services** tab to view a list of all the SOAP API implementations that are available in Application Integration. You can create a published API from an available SOAP API. The steps to create a managed API and activate the managed API remain the same. You can download a WSDL file of the SOAP API and share it with API consumers.

You can see the SOAP APIs on the **Services** tab only after you migrate to the new API gateway.

For more information, see *Manage APIs*.

Custom APIs

You can create, manage, and govern unique custom APIs that aren't based on Informatica service endpoints.

The name that you assign to the custom API is part of the API URL. When you create a custom API, the API URL that you specify must not be a URL that is restricted by Informatica and must not contain any potential vulnerability or malicious script. The URL must use a certificate that is signed by a well-known Certificate Authority.

The API URL that you specify must conform to the W3C standards.

For more information, see *Manage APIs*.

Published APIs from Application Integration

After you save and publish a process in Application Integration, you can publish the process to API Center. The API of the published process appears on the **Published APIs** tab in API Center. You can then create a managed API, apply policies, and monitor the API in API Center.

For more information, see *Manage APIs*.

Changed behaviors

The July 2024 release of API Center includes the following changed behaviors.

API domain name change

You can now change the domain name even after provisioning a domain. You can change the domain name on the **Domain Settings** tab on the **Configuration** page.

Previously, you could choose the domain name when you logged in to API Center the first time. After you provisioned the domain, you could not change the domain name.

For more information, see *Introducing API Center*.

INDEX

C

Cloud Application Integration community
URL [5](#)
Cloud Developer community
URL [5](#)

D

Data Integration community
URL [5](#)

I

Informatica Global Customer Support
contact information [6](#)
Informatica Intelligent Cloud Services
web site [5](#)

M

maintenance outages [6](#)

S

status
Informatica Intelligent Cloud Services [6](#)
system status [6](#)

T

trust site
description [6](#)

U

upgrade notifications [6](#)

W

web site [5](#)