



Informatica® API Center
October 2025

Monitor APIs

Informatica API Center Monitor APIs
October 2025
April 2025

© Copyright Informatica LLC 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: Monitor APIs..... 5

Overview tab. 5

Activity logs tab. 8

Preface

Read Monitor APIs to learn how to view and monitor APIs that are running or have run in your Informatica Intelligent Cloud Services organization.

CHAPTER 1

Monitor APIs

Use the **API Monitor** page to track the availability and performance of your managed APIs and managed API groups.

If you are assigned the API Monitor or Admin role, you can use the API Monitor page to monitor the invocations of managed APIs and managed API groups in an organization.

The API Monitor page displays the following two tabs:

Overview

The **Overview** tab provides a graphical overview of activity and API usage. You can gain real-time visibility into API health, including API invocation rate, response times, latency, errors, and traffic on the **Overview** page. 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.

Activity Log

The **Activity Log** tab provides a tabular view of the activity logs of the API invocations. You can download API activity log entries as a text file from this tab.

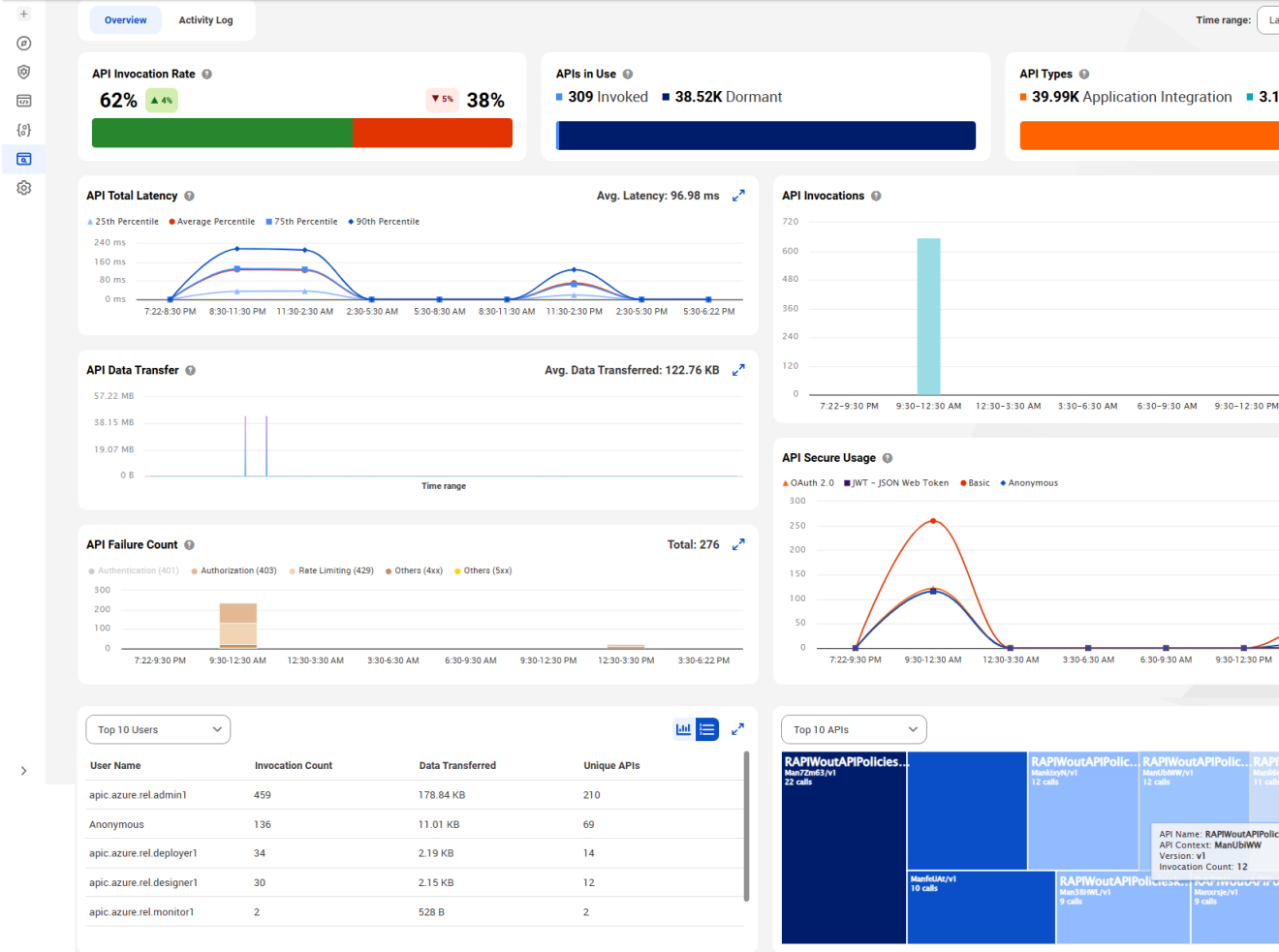
Overview tab

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

The **Overview** tab shows API usage trends for a selected period, for last 24 hours, 7, or 30 days. You can refresh the data by clicking the refresh icon.

API Monitor displays chart-boards in both concise and expanded views. The data representation varies between these views. For certain charts, such as top users and top APIs, you can also view the data in a tabular format.

The following image shows the different visual charts available on the **Overview** tab:



The following table explains the different API metrics available in the **Overview** tab:

Metric	Description
API Invocation Rate	<p>Evaluate API invocation success and failure rates, and track changes over time using trend indicators. Utilize this metric to assess the success and failure rates of API calls and their variations over time.</p> <p>This graph displays API invocation rates as success and failure percentages of the total requests sent to the gateway. Successful requests are displayed as green bars, while failed requests appear as red bars.</p> <p>The following indicators illustrate changes over time:</p> <ul style="list-style-type: none"> - Green arrows indicate an increase in number - Red arrows indicate a decrease in number - Neutral markers indicate no change in number <p>The trend is calculated based on the selected time range. For instance, if the selected time range is 24 hours, the trend is determined using the data from the previous 24 hours. If the range is 7 days, the trend is calculated using the previous 7 days of data. If no historical data is available, a neutral marker with 0% is displayed.</p>
APIs in Use	<p>Evaluate the frequency of API invocations within your organization.</p> <p>APIs are categorized as Dormant if they were not invoked during the selected time period, or as Invoked if they have been used at least once.</p> <p>This chart displays metrics for both managed APIs and managed API groups.</p>
API Types	<p>Identify the different types of APIs in your organization based on the implementation provider.</p> <p>The implementation provider can be Application Integration or a third-party custom provider. Each operation is considered as an API.</p>
API Total Latency	<p>Understand API latency through percentiles, offering insights into request completion time and performance. You can view the total API latency as a percentile and average latency time in milliseconds.</p> <p>For example, 75th percentile in the chart means that API Center completes 75% of all API requests within a certain amount of time, while the remaining 25% take longer. This metric provides a more comprehensive understanding of API performance compared to average latency, as it shows how quickly most of the requests are handled.</p> <p>You can refer the average percentile to understand the general speed of API requests overall. You can refer the other specific percentile, such as 25th or 90th percentile to understand the latency experienced by most users or the tail-end of slower requests.</p>
API Invocations	<p>Measure the incoming traffic to the gateway.</p> <p>This chart displays the API invocation counts over a specified time range, regardless of the invocation status. You can also view the total API invocations for a selected time range.</p>
API Data Transfer	<p>Measure the total amount of data received or transferred as part of the request and response body of all API invocations.</p>
API Failure Count	<p>Assess the overall health of API invocations.</p> <p>This chart displays the number of API invocation failures due to policy enforcement, service unavailability, or connectivity issues. The following causes of API failures are considered:</p> <ul style="list-style-type: none"> - Authentication - Authorization - Rate limits - Client errors (4xx HTTP status codes) - Server errors (5xx HTTP status codes)

Metric	Description
API Secure Usage	<p>Evaluate API invocations based on the supported authentication types to gain insights into the security posture of your APIs.</p> <p>The following authentication types are analyzed for security:</p> <ul style="list-style-type: none"> - OAuth 2.0 - JWT - JSON Web Token - Basic - Anonymous <p>This chart also displays the total number of unique users.</p>
Top 5 Users/Top 10 Users	Identify the top users, top 5 or top 10, who have invoked the highest number of APIs and transferred maximum data within a specific time frame.
Top 5 APIs/Top 10 APIs	<p>Identify the top APIs invoked, top 5 or top 10, including their invocation count, name, context, and version.</p> <p>Note: This chart displays the names of the APIs created after you upgraded to the April 2025 version of API Center. All existing APIs created before April 2025 are deactivated. Activate the deactivated APIs.</p>

Activity logs tab

You can view and download API activity logs of the API invocations from the **Activity Logs** tab on the **API Monitor** page. You can download log entries as a text file from the last one through four hours.

The following image provides you a glimpse of the activity log:

Overview

Activity Log

Time range: Last 4 hours

Activity Log

Timestamp	API Context	Provider	Method	API Endpoint URL	IP Address	Applied Policies	Status	Consumer	Short Log	Duration
Oct 3, 2025, 08:24...	ManQLccN	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	113
Oct 3, 2025, 08:34...	ManPm24x	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	6
Oct 3, 2025, 08:34...	ManPm24x	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	152
Oct 3, 2025, 08:26...	ManQpE9o	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	80
Oct 3, 2025, 08:26...	ManQpE9o	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	74
Oct 3, 2025, 08:26...	ManQpE9o	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	110
Oct 3, 2025, 08:30...	ManDGwnO	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	12
Oct 3, 2025, 08:30...	ManDGwnO	Application Integr...	POST	https://api.com/...	192.168.1.1	5	200 OK	...	IP Address : 192...	221
Oct 3, 2025, 08:38...	ManvHHVQ	Application Integr...	POST	https://api.com/...	192.168.1.1	1	401 Unauthorized	...	OAUTH_2 not sup...	144
Oct 3, 2025, 08:38...	ManDrNS	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	154
Oct 3, 2025, 08:24...	ManeXvY	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	100
Oct 3, 2025, 08:33...	Man7MkXh	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	70
Oct 3, 2025, 08:33...	Man7MkXh	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	109
Oct 3, 2025, 08:29...	ManA4O6	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	103
Oct 3, 2025, 08:26...	ManFEns5	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	139
Oct 3, 2025, 08:21...	ManR3K7h	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	137
Oct 3, 2025, 08:38...	ManXj28b_Edited...	Application Integr...	POST	https://api.com/...	192.168.1.1	2	403 Forbidden	...	IP Address : 192...	12
Oct 3, 2025, 08:38...	ManXj28b_Edited...	Application Integr...	POST	https://api.com/...	192.168.1.1	5	200 OK	...	IP Address : 192...	75

You can filter and view the following details for each API invocation:

- The timestamp when the API was invoked
- The context that API Center adds to the API URL
- The service provider of the API
- The HTTP method of the API
- The API endpoint URL that was invoked
- The IP address of the incoming API request
- The policies that were applied to the API
- The status code of the API response
- The consumer or the users who invoked the API
- The short log of the error message if the API invocation failed
- The total duration, in milliseconds, when the gateway receives a request, processes it, delegates to implementation, and responds back

Using the **Consumer** column, you can get insights into the users who invoked the APIs. It displays one of the following values based on the authentication method that the API uses:

Authentication method	Consumer value
Anonymous	Anonymous
Basic	Name of the user who invoked the API using an IDMC user name and password.
JSON web token (JWT)	Name of the user who generated the JWT token.
Session ID	Name of the user who generated the IDMC session ID.
OAuth 2.0	ID of the OAuth 2.0 client that invoked the API followed by the user name within parentheses.
Third-party authentication	Name of the user who invoked the API using an external identity provider.

Note: The **Consumer** column does not display any value for custom APIs.

Define time frame for activity logs

You can select the time frame for which you want to view the API invocation details. You can select one of the following time frames:

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

You can use **CUSTOM** to customize the time frame for which to view the API invocation details.

Download API activity logs

To download a log file, select a time frame from the time frame menu and click **Download**.

Activity logs display a maximum of the first 500 invocations in a selected time range. You can also download activity logs for a maximum of 30 days. Use the **CUSTOM** option from the time frame menu to download activity logs for a customized time period. Use the **Select Date Range** time picker to set the customized time period.

Consider the following guidelines when you customize a time period:

- The time interval between the start time and end time can't exceed 4 hours.
- The start time must not be less than 30 days.
- You can view a maximum of 500 records. If your current date and time range exceeds this value, narrow down the date and time range to view holistic data.

Filter search results

You can filter the search results based on the following fields:

- API Context
- Provider
- Method
- IP Address
- Status
- Duration