

Table of Contents

About the Illumio and Claroty Integration	3
Before You Onboard the Illumio and Claroty Integration	3
Generate an API Token from Claroty xDome	3
Create a New User and Generate an API Token in Claroty xDome	4
Onboard the Illumio - Claroty Integration	6
View Traffic from Claroty Devices	6
View Device Traffic in the Devices Tab	7
View Device Traffic in the Map Screen	8

About the Illumio and Claroty Integration

The Illumio and Claroty integration allows you to view traffic from OT devices, between OT devices, and between OT and IT devices. You can drill down on these flows to view details and use the information to enforce policies.

[Watch the video](#)

Before You Onboard the Illumio and Claroty Integration



IMPORTANT

To be able to view traffic for Claroty devices, you must set up Flowlink. See [Flowlink](#).



IMPORTANT

You must generate the API token in Claroty xDome before you onboard the API Connector.

Use one of the following procedures depending whether or not you already have an API User user in xDome:

Generate an API Token from Claroty xDome



IMPORTANT

Use this procedure if you already have a user in xDome with the API User role.

1. Log into Claroty xDome and navigate to **Home > Settings > Admin Settings**.
2. On the **User Management** page, select a user with the **API User** role.
3. Click the key icon at the end of the row for the API User to generate the API token.
4. In the **Generate API Token** modal, select an expiration date for the token from the **Token Expiration** drop-down list.



NOTE

Claroty recommends that you set tokens to expire after 90 days.

5. Click **Generate**.
Make sure to copy the API token because it only displays once.
6. Click **Finish**.

Create a New User and Generate an API Token in Claroty xDome



IMPORTANT

Use this procedure only if you do not already have a user in xDome with the API User role.

1. Log into Claroty xDome and navigate to **Home > Settings > Admin Settings**.
2. On the **User Management** page, click **+ Add User** and set the following values in the **Create User** modal:
 - a. Select the **API User** role.
 - b. Click **Edit Site Permissions** and set the following values in the Add Site Permissions modal:
 - i. Select the **Group** values, select **Including future sites and groups**, and click **Apply**.
 - ii. Select **Read-Only User** from the Roles drop-down list.
 - iii. Click **Create User**.
The **Pending Token Generation** badge displays while the token is generating.
3. After you create the new user, click the key icon at the end of the row for that user.

4. In the **Generate API Token** modal, select an expiration date for the token from the **Token Expiration** drop-down list.



NOTE

Claroty recommends that you set tokens to expire after 90 days.

5. Click **Generate**.
Make sure to copy the API token because it only displays once.
6. Click **Finish**.

Onboard the Illumio - Claroty Integration

1. Log into the Illumio Console and go to **Settings > Connector**.
2. Find the Claroty connector and click **+ Add**.
3. On the **Connection Configuration** page, enter the required values:



NOTE

See [Before You Onboard the Illumio and Claroty Integration \[3\]](#) to obtain the required values.

- a. Enter the API URL, such as `https://<your-claroty-console>/api`.
 - b. Enter your API token in the **Client Secret** field.
4. Click **Test Connection** to verify that you have entered your credentials correctly.
 5. Under **Category**, select the device category that you want to import. You can select all categories or specify certain categories.
 6. Click **Save**.
 7. Check the **Last Updated Status** and **Devices Updated** information to verify that your devices imported successfully.



NOTE

If you are importing a large number of devices, it might take some time for the confirmation message to display.

View Traffic from Claroty Devices

After you complete onboarding, your Claroty devices display. However, if you want to view traffic for those devices, you must install Flowlink. See [Configure Flowlink](#).

View Device Traffic in the Devices Tab

The screenshot displays the 'Devices' tab in the Illumio console. At the top, there is a browser tab titled 'speedway-r220-xxnsnn' with a close button. Below the tab, the device name 'speedway-r220-xxnsnn' is shown next to an 'OT Device' icon. The main content area is titled 'Device Information' and lists various attributes for the device:

Name	speedway-r220-xxnsnn
IP Address	10.18.28.171
MAC Address	00:16:25:4a:80:74
Device Category	General IoT
Device Type	RTLS
Site	NY-BR-770
Boundary	
Purdue Model	L4
Risk Score	CRITICAL Medium
Source	CLAROTY
Tags	Tier-01 Unsupported_OS
Labels	

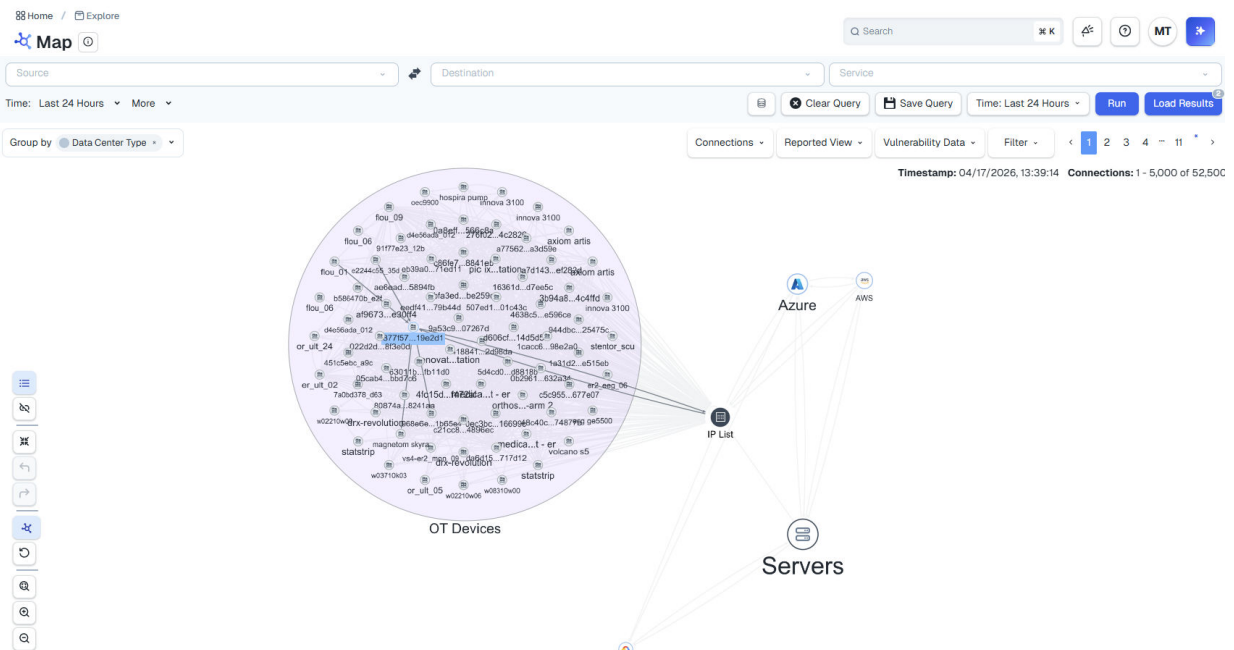
1. Within Illumio Console, navigate to **Servers & Endpoints > Workloads > Devices**.

Illumio and Clarity Integration Guide

Name	IP Address	MAC Address	Device Category	Device Type	Site	Purdue Model	Risk Score	Source
speedway-r220-xxnsmn OT Device	10.18.28.171	00:16:25:4a:80:74	General IoT	RTLS	NY-BR-770	L4	CRITICAL Medium	CLAROTY
10.10.9.157 OT Device	10.10.9.157	00:05:12:f4:9d:df	General IoT	Mobile Printer	Clinton	L3	CRITICAL High	CLAROTY
10.10.9.155 OT Device	10.10.9.155	00:05:12:c6:32:ce	General IoT	Mobile Printer	Clinton	L3	CRITICAL High	CLAROTY
speedway-r220-jmgmsf OT Device	10.179.192	00:16:25:6a:3b:cd	General IoT	RTLS	Houston_Line_1	L4	CRITICAL Medium	CLAROTY
10.6.99.31 OT Device	10.6.99.31	10:2b:05:c8:7a:ec	General IoT	Printer	Washington	L4	CRITICAL Medium	CLAROTY
10.18.29.1 OT Device	10.18.29.1	00:07:4d:c1:06:20	General IoT	Mobile Printer	SV_2	L3	CRITICAL Low	CLAROTY
10.6.99.8 OT Device	10.6.99.8	10:2b:05:5f:a6:98	General IoT	Printer	Washington	L4	CRITICAL High	CLAROTY
speedway-r420-udkicx OT Device	10.11.53.123	00:16:25:da:01:5c	General IoT	RTLS	Albany	L4	CRITICAL Medium	CLAROTY
10.18.28.243 OT Device	10.18.28.243	00:05:12:e7:76:b8	General IoT	Mobile Printer	Albany	L3	CRITICAL High	CLAROTY

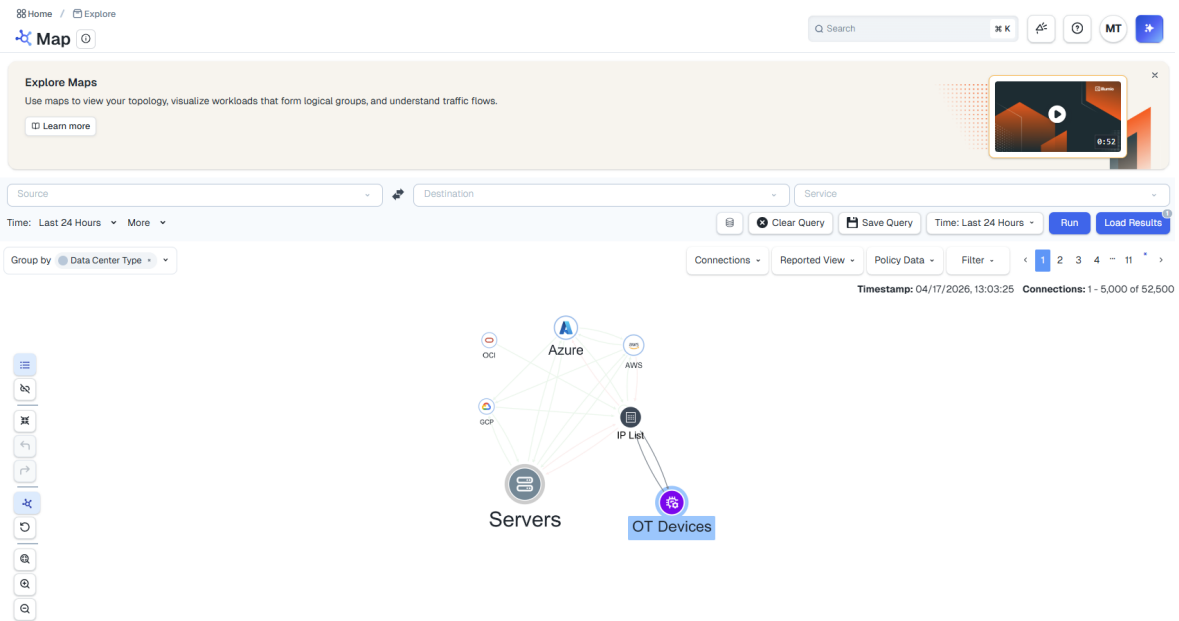
2. To view details, hover over a device and click **Details** in the tooltip or click any column in the device row to view the detail pane.

View Device Traffic in the Map Screen



1. Navigate to **Explore > Map** and group by **Data Center Type**.

Illumio and Claroty Integration Guide



2. Click the **OT Devices** group to view the traffic between your resources.

Include additional filters to refine the results. For example, to display only Production devices that are located in Canada, add the Environment and Location filters.



NOTE

Filtering is context-sensitive. If you click a group, the details pane displays information about the group, and if you click a device, the details pane displays information about the device.

The following figure displays a summary of all OT Devices:

Summary Traffic Workloads

Data Center Type

OT Devices

Private Data Centers

OT Devices

74 Devices