



Publication date May 27, 2025

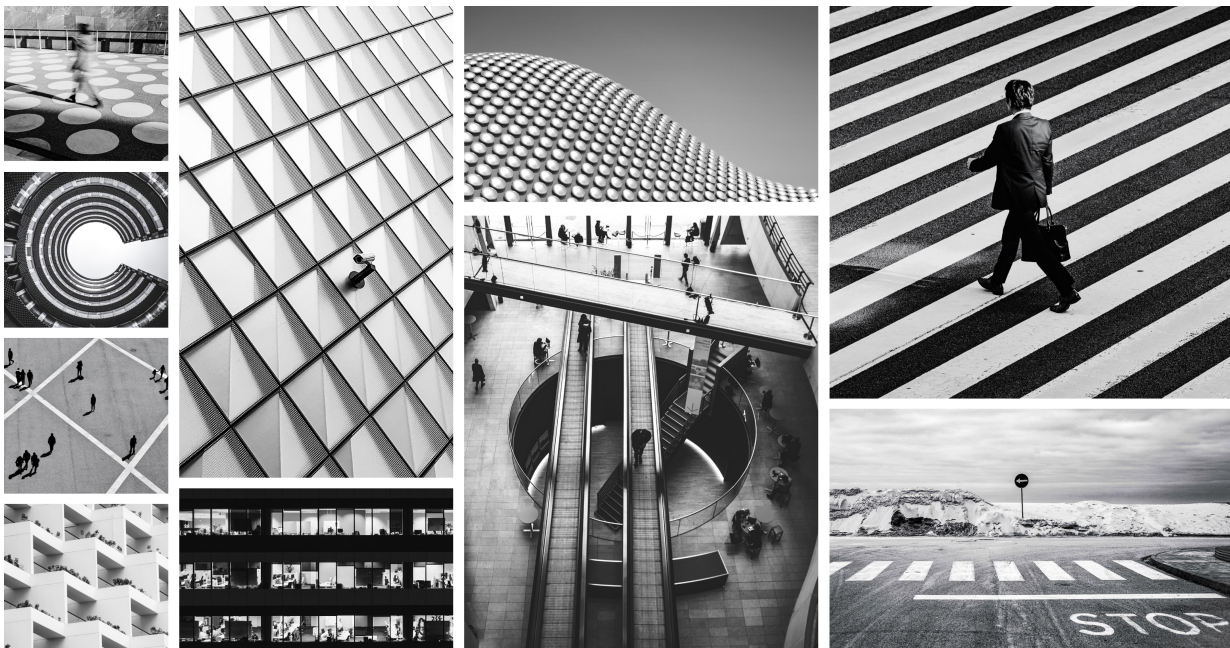


Table of Contents

About the Wiz Connector for Illumio	3
Add a Wiz Service Account	4
Set Up Wiz Connector for Illumio	6
View Wiz Vulnerability and Risk Information	7
Known Issues for Wiz Connector for Illumio	9

About the Wiz Connector for Illumio

The Wiz Connector for Illumio uses security events from Wiz Cloud to augment cloud resources and cloud flow data in Illumio to help you understand potential vulnerabilities and exposures to security breaches in your cloud environment. By enabling Wiz Connector for Illumio, you can view cloud inventory, vulnerabilities, and issues within Illumio Console.

The Wiz integration provides the following benefits:

- **Enhanced visibility:** The Wiz integration provides enhanced visibility into cloud environments and gives security teams the necessary insights to apply segmentation policies.
- **Improved vulnerability management:** This integration improves vulnerability management by not only detecting misconfigurations and vulnerabilities, but also by adding application deployment and traffic-flow telemetry data between workloads.
- **Faster breach containment:** With this integration, you can implement granular access controls based on real-time threat intelligence to minimize your organization's attack surface and automatically contain potential breaches.

With this integration, you can see detailed vulnerability information for Cloud resources in the Illumio Console.

For more information, see [Wiz](#).

Add a Wiz Service Account



NOTE

You must have created a Wiz service account before you can set up the Wiz Connector for Illumio. Service accounts are required for machine interfaces to be able to authenticate with the Wiz API.

1. Log into the Wiz application, navigate to **Settings > Access Management > Service Accounts**, and click **Add Service Account**.
2. Name the account and select the Custom Integration (GraphQL API) type of service account.
3. Select the projects that you want to limit access to if you do not want to grant access to all projects. Note that you cannot change the projects after you have created the service account. You must create a new service account.



NOTE

If you create a new service account, you must also edit the Client ID and Client Secret and save the values to a secure location on your machine.

The screenshot shows the Wiz application interface. On the left is a sidebar with a navigation menu. The 'Settings' section is expanded, and 'Service Accounts' is selected. The main content area displays the 'New Service Account' form. The form includes the following fields and options:

- Name:** A text input field.
- Type:** A dropdown menu set to 'Custom Integration (GraphQL API)'. Below it, a note says 'Select which type of software component will use this Service Account'.
- Description:** An optional text input field.
- Projects:** An optional dropdown menu set to '2 selected'. Below it, a note says 'Limit access to selected projects only' and 'Select up to 50 projects. Leave empty to grant access to all projects'.
- Expiration Date:** An optional dropdown menu set to 'No date selected'. Below it, a note says 'Set an optional expiration date for this service account. After this date, the service account will no longer be able to access the Wiz API.'

4. Under API Scopes, grant the following permissions:
 - read: issues
 - read: vulnerabilities
 - read: threat_issues
 - read: projects
 - read: reports

- create: reports
5. Click **Add Service Account**. The dialog box shows the **Client ID** and **Client Secret** for the service account. Your application uses this information to request a new API token. Tokens last for 24 hours, and after one expires, your system asks for a new one.
 6. Copy the **Client ID** and **Client Secret** to a secure location. Note that this information only displays once, so make sure to copy it.
 7. Click **Finish**.

**NOTE**

Note the following recommendations for service accounts:

- Restrict service accounts to the minimal permissions possible.
- Rotate the Client Secret on a scheduled basis. When you do this, remember to update the value in the Wiz Connector and save the secret in a secure location.
- Remove unused service accounts.
- Securely store Client IDs and Client Secrets.

Set Up Wiz Connector for Illumio



NOTE

Before you set up the Wiz Connector, create a Wiz service account within the Wiz application. See [Add a Wiz Service Account \[4\]](#).

1. Log into Illumio Console, navigate to the **Connector** page, and click the **Wiz** tile.
2. Click the **+Add Wiz Connector** button. The button only displays if Wiz has not been onboarded yet.
3. Fill in the following fields:
 - **Authentication URL** (obtain this value from the Tenant Info page within Wiz)
 - **API URL** (obtain this value from the Tenant Info page within Wiz)
 - **Client ID** (obtain this value from the Wiz service account)
 - **Client Secret** (obtain this value from the Wiz service account)
4. Click **Save**.

After you click **Save**, Illumio Console starts ingesting data immediately. While Illumio Console is ingesting data, the **Connection Status** field shows **Onboarding**. After it has ingested the vulnerability data from Wiz, the status changes to **Success**.

If adding the Wiz Connector fails, the **Connector** page displays a red warning banner above the **Connection Status** pane and lists the reason for the connection failure.

The connection may have failed for the following reasons:

- The Authentication URL or API URL has changed. If so, obtain the correct URL from the Tenant Info page within Wiz.
- The Client ID or Client Secret was incorrect.

View Wiz Vulnerability and Risk Information

After you have onboarded Wiz, navigate to the **Inventory** page and search for a virtual machine resource.



NOTE

Risks are only visible for virtual machines.

Home / Cloud / Inventory / Cloud Resources

aws Data-Warehouse

Q Search K EF

Summary Attached Resources Traffic **Risks** Resource Graph [PREVIEW](#)

Wiz Issues Vulnerabilities

Vulnerability Description	Severity	CVE #	Vulnerability Score	Component of Services
Issue summary: Checking excessively long DSA keys ...	MEDIUM	CVE-2024-4603	5.3	OpenSSL
Issue summary: A timing side-channel which could p...	MEDIUM	CVE-2024-13176	4.1	OpenSSL
Issue summary: Use of the low-level GF(2^m) ellipt...	MEDIUM	CVE-2024-9143	4.3	OpenSSL
Issue summary: Some non-default TLS server configu...	MEDIUM	CVE-2024-2511	5.9	OpenSSL
Issue summary: Calling the OpenSSL API function SS...	MEDIUM	CVE-2024-5535	9.1	OpenSSL
Use after free in Windows Digital Media allows an ...	HIGH	CVE-2025-27476	7.8	Windows Server 2019
Use after free in Windows Remote Desktop Services ...	HIGH	CVE-2025-26671	8.1	Windows Server 2019
Heap-based buffer overflow in Windows Telephony Se...	HIGH	CVE-2025-21222	8.8	Windows Server 2019
Improper input validation in Windows DWM Core Libr...	HIGH	CVE-2025-24060	7.8	Windows Server 2019
Improper access control in Windows Defender Applic...	HIGH	CVE-2025-26678	8.4	Windows Server 2019

Page Size: 10 1 to 10 of 123 Page 1 of 13

Note the following information:

- Only accounts and subscriptions that have been onboarded to Illumio CloudSecure and Wiz will be able to view the issues and vulnerabilities in Illumio.
- You will only see risks for workloads that are in subscriptions that have been onboarded to Illumio CloudSecure and that are part of the Wiz projects that the onboarded service account has access to.

Drill down on the resource and then click the **Risks** tab to display more information about the detected vulnerability.

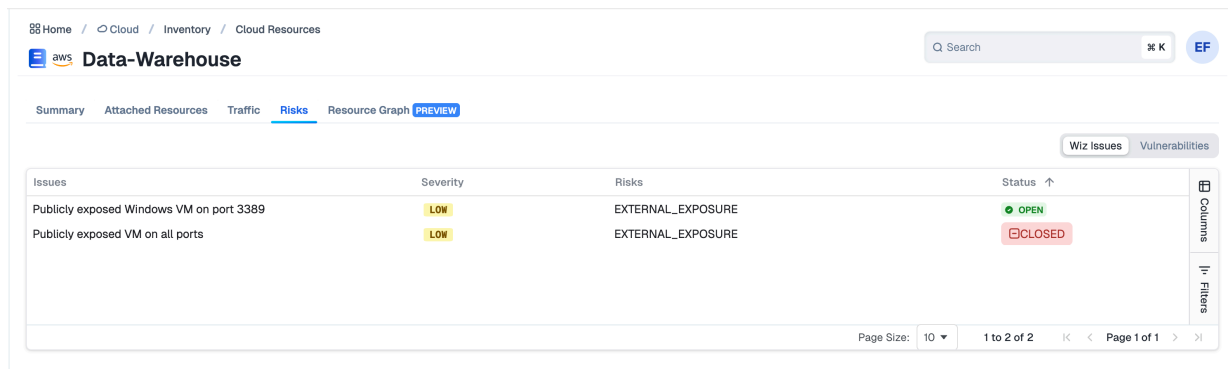
Click the CVE number to view more information about the vulnerability. This information comes from the National Institute of Standards and Technology (NIST)'s Common Vulnerability Scoring System (CVSS). The risks are scored as follows:

Risk Score	Risk Level
0.1 to 3.9	Low
4.0 to 6.9	Medium
7.0 to 8.9	High
9.0 to 10.0	Critical

The Wiz application detects the vulnerability and the component or resource that it affects and then associates the issue with the CVSS number.

For more information about NIST vulnerability scores, see [NVD Dashboard](#).

Click the **Wiz Issues** tab to view vulnerability issues that have been detected for resources in your network.



The screenshot shows the Wiz application interface for a resource named 'Data-Warehouse'. The 'Risks' tab is selected, displaying a table of detected issues. The table has columns for 'Issues', 'Severity', 'Risks', and 'Status'. Two issues are listed: 'Publicly exposed Windows VM on port 3389' with a 'LOW' severity and 'EXTERNAL_EXPOSURE' risk, and 'Publicly exposed VM on all ports' with a 'LOW' severity and 'EXTERNAL_EXPOSURE' risk. The status for the first issue is 'OPEN' (green circle) and for the second is 'CLOSED' (red square). The interface includes a search bar, navigation tabs, and a sidebar with 'Columns' and 'Filters' options.

Issues	Severity	Risks	Status
Publicly exposed Windows VM on port 3389	LOW	EXTERNAL_EXPOSURE	OPEN
Publicly exposed VM on all ports	LOW	EXTERNAL_EXPOSURE	CLOSED

After you have viewed the information in the **Vulnerabilities** and **Risks** tabs, you have visibility into workload vulnerabilities and you can also write policies to secure your vulnerable resources.

Known Issues for Wiz Connector for Illumio

The following known issue applies to Wiz Connector for Illumio:

Vulnerabilities that reflect N/A as the vulnerability score do not have scores within the National Vulnerability Database.

See National Vulnerability Database: <https://nvd.nist.gov/>